SECURITY AND USABILITY IN A HYBRID PROPERTY BASED GRAPHICAL AUTHENTICATION SYSTEM

PhD Thesis

HASSAN UMAR SURU

School of Computing Science and Engineering

University of Salford

August 2018

Declaration

I hereby declare that the research contained in this thesis is original work conducted and composed by me except where explicitly stated otherwise.

Hassan Umar Suru

Acknowledgement

First of all I will like to express my gratitude to God Almighty for seeing me through this program successfully. I will also like to express my utmost gratitude to my main supervisor Dr. Pietro Murano for the immense support, motivation and encouragement he has given me throughout the duration of this course. He has painstakingly read every line of my work and offered useful suggestions that have helped in the conduct and compilation of this work. My gratitude also goes to my supervisor at Salford, Prof. Apostolos Antonacopoulos for his support, guidance and immense contributions to my work. I also extend my profound gratitude to Prof. Sahalu Junaidu of Ahmadu Bello University, Zaria, for offering to work as my advisor and giving me all the help and support I need for the success of the programme.

On a special note, I sincerely thank and appreciate the efforts of my brother, Hussaini Umar Suru, for his support financially and morally, without which the programme would not have been possible. I humbly appreciate the support of my mother and my family, Shafaatu, Nafisa and the children, whom had to continuously cope with my long absences. I thank everyone for their support.

There are so many people to whom I am greatly indebted, my friends in Salford, and the UK, Mal. Murtala Muhammad of the school of computing, science and engineering, university of Salford, his friend Mal. Umar, Mal. Abdul and others that have made my life worth living while on campus. I also appreciate the support of my great friend in Sutton, London, Muhd Kabir Batsari that has been of the greatest help to me throughout the time of my studies. Friends and family members in Nigeria, including Dr. Salihu Suru, Alh. Haruna Suru, Dr. Maihankali, Mal. Usmanu, Mal Aliyu, Alh. Abdullahi A. U. Suru and the host of others, too numerous to mention, have all provided the much needed help support that saw to the completion of this work. I thank all of you very much for your support and numerous contributions to my work.

I also like to express my utmost gratitude to Abubakar Isah AbdulMalik (Baba) with whom I have worked tirelessly to put together hundreds of lines of code that ensured the development and smooth running of all system prototypes. I also use this medium to thank the hundreds of university staff and students that have supported or participated in my user trials, notable among whom are AbdulRahman Aliero, AbdulHakeem Ibrahim, Zainab Sani, Sunday Chintama, and many others whose names I'm not able to remember here. Thank you very much for your tremendous efforts.

Table of Contents

List of Figures

List of Tables

Abstract

Alphanumeric text and PINs continue to be the dominant authentication methods in spite of the numerous concerns by security researchers of their inability to properly address usability and security flaws and to effectively combine usability and security. These flaws have, however, contributed to the growing research interest in the development and use of graphical authentication systems as alternatives to text based systems. Graphical passwords or graphical authentication systems are password systems that use images rather than characters or numbers in user authentication. The picture superiority effect, a belief that humans are better able to memorise images than text, has very much influenced the proliferation of and support for graphical authentication systems.

In spite of their growing acceptance, however, empirical studies have shown that graphical authentication systems have also inherited some of the flaws of text based passwords. These flaws include predictability, vulnerability to observational attacks and the inability of systems to efficiently combine security with usability. Hence there is a continued quest among usable security researchers to find that hypothetical system that has both strong usability and strong security.

In this research, a novel concept for hybrid graphical authentication systems is developed. This consists of a class of systems that are called 'property based authentication systems' which adopt the use of image properties for user authentication, rather than specific images as used in existing systems. Image properties are specified contents of images which gives the image a set of characteristics. Several implementations of these systems have been developed and evaluated. Significant empirical performance studies have been conducted to evaluate these systems in terms of usability and security. The usability evaluations conducted evaluate the systems in terms effectiveness, efficiency and user satisfaction, while security evaluations measure their susceptibility to common attacks. The results from these studies suggests that property based systems have better usability and security when compared to commonly known and well researched graphical authentication systems.

Chapter One - Introduction

1.1 Introduction

Human Computer Interaction (HCI) is that branch of computer science involved with the study of how computing systems can best be designed to the satisfaction of human users. HCI thus encourages what is often termed as a "Human centred" approach to systems design and development [1,2]. HCI emerged in the early 1980s and has brought together professionals from diverse fields and aggregated many semi-autonomous areas of research in human centred computing [3]. Usable security is a branch of computer system security and human computer interaction that studies the role of human factors in system security. This is particularly important as humans are often considered the weakest link in the system security chain due to vulnerabilities infused by human attributes. According to Patrick, et al. [4], there are three main areas in which human computer interaction is most important. These areas are: (1) authentication, (2) security operations, and (3) the development of secure systems. The focus of this research is in the area of authentication which is the act of allowing system access to legitimate users and denying same to illegitimate users, and is a vibrant field open to ongoing research. Several authentication systems have been developed and evaluated [4]. Biometric systems use human traits and physical characteristics for user authentication, token based systems use hardware tokens and smart cards, while knowledge based systems make use of some secret information only known to the legitimate user in user authentication. Each of these systems has its inherent problems [4].

Over the years, the main method of authentication has been the use of alphanumeric text, which has either been predictable or difficult to remember [5]. The use of graphical images to complement text based passwords so as to improve their usability and security have also been suggested [6]. The fact that users need to keep track of several accounts has made them resort to insecure behaviour such as the use of the same password for several accounts, use of common names, as well as writing down and sharing of passwords [7,8]. In order to address these problems, alternative password schemes have been suggested [7,9,10]. Among such schemes are graphical (or image based) passwords, as researchers believed that humans are better able to remember pictures than text [11,12]. Several graphical systems have been developed and evaluated. These have been divided into a number of categories. Recognition based systems utilise the human ability to remember images that have been previously seen, recall based systems utilise the ability to recall activities previously undertaken, while cued recall based systems utilise the ability to recall activities previously undertaken on locations previously identified. Research shows recall based systems to be more secure, and recognition based systems to be more usable [12].

This research focuses on a system that combines recall and recognition, in which properties are assigned to images and used in user authentication instead of subsets of large image sets as used in existing recognition based systems. Properties are like cloths on a human, they do not tell you who a person is, but what he is putting on. When sales or students representatives are asked to meet potential clients or new students at train stations or airports, the clients or new students normally do not know the person they will meet and may only recognise the person through some sort of 'uniform'. In traditional recognition based graphical authentication systems, specific images are selected and used for authentication. In property based systems, a set of 'contents' or 'characteristics' are defined for an image set and are designated as properties that are used in a user's authentication process. During authentication, any image bearing that 'property' is selected as the authentication or pass image. In this research, a number of prototypes of systems representing the various implementations of this concept have been developed and the underlying usability and security issues and ideas investigated. Based on the prototypes' simplicity in use and understanding, as well as their strong security, it is believed that this novel system effectively mitigates current usability and security contention in existing systems through combining the strengths of recognition and recall. The work is aimed at establishing the following:

- The strengths and weaknesses of existing graphical authentication systems.
- The feasibility and applicability of the use of image properties in graphical user authentication.
- The ability of the system to provide better security and usability as compared to existing graphical authentication systems.
- The ability of the system to mutually combine strong usability and strong security in one system.
- An understanding of the various possible implementation of this concept.
- An evaluation of the strengths and weaknesses of various implementations of this system.
- An understanding of underlying issues that may be brought forward in the course of the research.
- The ability to suggest or provide further enhancements to the system.

1.2 Aim and Objectives of Research

The aim of the research is to develop a more efficient hybrid graphical authentication technique that utilizes both recognition and recall as an effective means of combining usability and security as well as to build a concise conceptual model of the system. This aim shall be achieved through the following objectives:

1. To investigate usability and security issues in relation to currently developed (existing) graphical authentication systems.
2. To develop an alternative novel system towards improving usability and security.
3. To identify the various possible approaches towards the implementation of the new system.
4. To empirically evaluate the performances of the new system.
5. To evaluate novel ideas developed in the course of objective 2 so as to determine their effects on system performance
6. To develop a concise conceptual model for the implementation of the system.

1.3 Research Question

Graphical (picture based) authentication has been proposed as an alternative to conventional (text based) authentication systems (passwords and PINs) due to their vulnerabilities. These vulnerabilities include predictability and observability (especially shoulder surfing). Shoulder surfing is the tendency that a keen observer is able to acquire a user's password by simply looking over his shoulder during password entry. Several graphical authentication models have been implemented and tested. In spite of their promise in addressing the security and usability challenges of text based passwords, they also inherit some of their vulnerabilities. Most graphical passwords have predictable patterns and are prone to observational attacks. They have also failed in merging the required usability with the required security. The quest for a system that is both highly usable and highly secure has remained elusive.

The focus of this work has therefore been to develop and evaluate a novel "property based" graphical authentication system that combines the basic ideas of recognition and recall to provide a hybrid scheme with the hope that the new approach effectively mitigates the security and usability contention inherent in graphical passwords. The new method explores the use of image properties as bases for user authentication instead of predefined subsets of large image sets as used in existing systems. The system is demonstrated and evaluated using appropriate software prototypes. The work seeks to answer the following question:

"Can images, assigned properties and associated variants, be used in user authentication as hybrid graphical authentication systems to effectively combine usability and security?"

1.4 Motivation for the Research

Graphical authentication systems are a new form of authentication systems introduced to mitigate the usability and security challenges associated with the use of alphanumeric texts. These challenges include usability issues such as memorability and ease of use, and security issues such as predictability and observability. Although many graphical authentication systems attempt to address some of these issues, none has been able to effectively combine usability with security. Secure systems have mostly not been usable and usable systems have not been secure [14]. The quest to find a system that is both usable and secure has remained elusive. This research aims at providing the long awaited solution to the security/usability contention problem in graphical authentication systems through a novel scheme that has never been considered previously in usability and security research. The motivation for the research work and the proposed approach have been driven by the following:

- To develop and test novel systems that are both usable and secure and that could be usable across all system user groups.
- To develop authentication systems that are efficiently applicable across small and large computing devices.
- To develop a graphical system that can help tackle the growing trend of online and offline electronic data theft.
- To present and investigate a new concept that will form the foundation for new and continued research.

1.5 Research Approach and Methodology

The research approach is geared towards achieving the research aims based on three distinct steps. The approach and the steps are illustrated in figure 1.1. The first step is focused on an extensive literature search and detailed review of existing graphical authentication models. This provides a forum for an analysis and comparison of these schemes with a view to identifying their strengths and weaknesses. The second step deals with the suggestion of a solution to issues discovered in existing systems as identified in step 1. This involves the identification, classification and implementation of the various models of the proposed graphical authentication model. The third step deals with a detailed analysis and evaluation of the proposed authentication model. This is capped with a comprehensive report on the research findings.

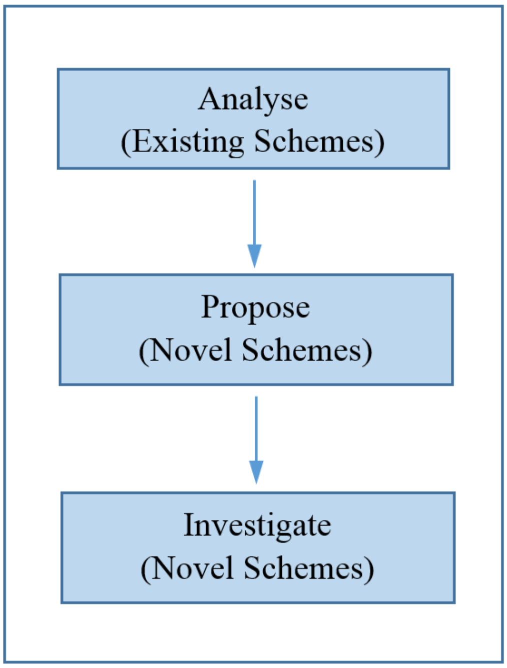


Fig. 1.1: The Research Approach

For each of the research studies, software prototypes have been developed to reflect the underlying concept of the proposed model and the purpose of the study. The methodology is presented in figure 1.2, a modification of the methodology in [15, 16, 17, 18, 19]. All system prototypes are first subjected to a preliminary tests before extensive user trials. These tests help identify inconsistencies in system design as well as provide a glimpse into user observations and opinions.

Although the research suggests both long term and short term usability trials for each of the proposed models so as to more efficiently analyse system performance, as well as user choice and satisfaction, due to the rigour and timing demands for longitudinal (long term) trials, only a number of prototypes are tested in the long term user studies. Hence participants were mostly tested for short term recognition and recall. In order to reflect a mixed user population in a one-to-one user study, the participants are drawn from the university community (mainly students) obtained through open call for volunteers.

Based on the usability metrics of effectiveness, efficiency, memorability, knowledge/user skill, and user satisfaction stated in section 5.2, usability performance evaluation conducted in the studies are based on the three elements of success rate, timing and user feedback. The success rate indicates the number of login success or failure of participants as they try to authenticate, the timing reflects the amount of time taken by a participant in both the registration and authentication phases of the various user sessions, while the user feedback provides quantitative or qualitative feedback on user choices and perceptions on system use and performance through research questionnaires. The security evaluations were designed to analyse the vulnerability of the various system implementations to observational attacks, guessing attacks as well as vulnerability to verbal and written descriptions. The metrics for all security evaluations are based on the number of successful login attempts.

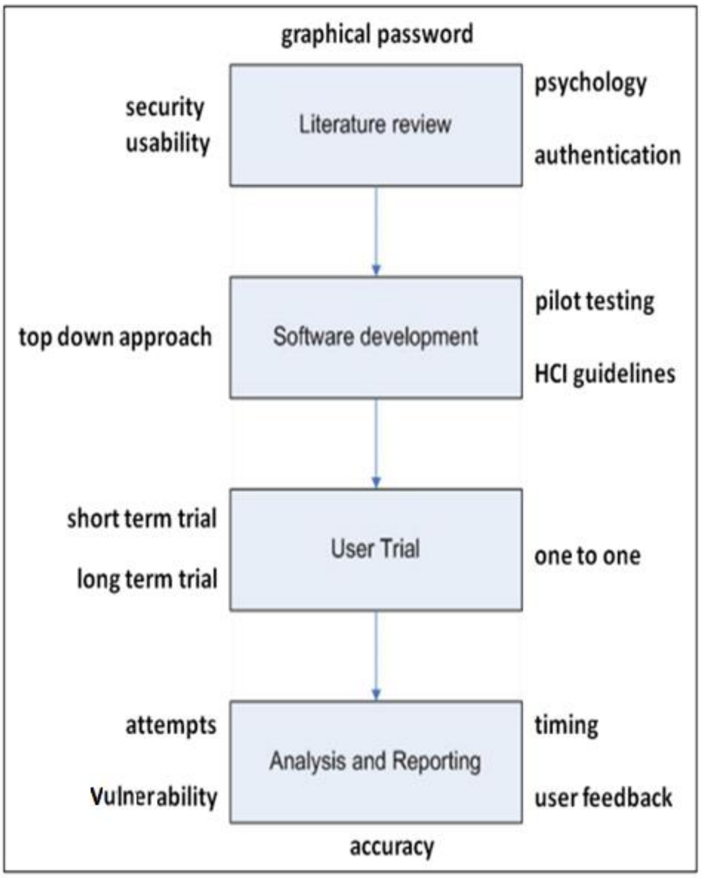


Fig. 1.2: Research methodology

1.6 Contributions to Knowledge

The inability to eradicate or even significantly reduce the disparity between usability and security in existing password systems has remained a challenge for usable security researchers. Usable systems have normally been weak in security, while secure systems have poor usability, and bridging this gap has remained almost impossible [20]. Moreover, some security challenges, such as shoulder surfing, have become a recurring problem in graphical authentication.

This work is aimed at the development and evaluation a novel system that integrates the recognition and recall based concepts in order to harness the benefits of both systems. From the literature studied in the course of this work, no research has been uncovered that has exploited the tendency for user authentication based on the use of characteristics of images (properties) instead of a selected subset of images that has been used consistently in the design of existing systems. Software prototypes of several models have been developed and evaluated. Hence, this novel method is believed to be as close to the "ideal" authentication system as possible. According to [21], "an ideal authentication system should provide strong security while maintaining high usability". Hence, an ideal system should be able eliminate the usability/security contention that has constituted a major challenge in the design of authentication systems. Specifically, there are ten (10) significant contributions to the body of academic knowledge that have been achieved from this research:

1. Property based systems combine recognition and recall in a picture style grid based presentation. Since it is assumed that recall based systems are more secure, while recognition based systems are more usable, a system that can effectively combine them will guarantee good usability as well as good security. This ensures that the system provides better usability and security than other grid based schemes such as the passfaces scheme or the déjà vu scheme that are purely recognition based.

2. Property based authentication sees the introduction of a new authentication factor that has not been discovered and used in previous studies. Authentication factors play a significant role, if not the most significant, in ensuring the usability and security of authentication systems.

3. The use of image properties is a novel concept in graphical authentication that relieves the user of the memory burden of having to remember many images. Most grid based authentication systems such as the passfaces scheme are designed such that every user goes through four or more authentication steps. In property based systems, the system allows a user to select the number of authentication steps he desires, thereby reducing the memory burden of remembering multiple images. With few steps, the system still provides better security than similar existing models deploying many steps.

4. Through the concept of property based authentication, a new class of authentication systems is born with numerous implementation and design options. This multiplicity of design options provides users with a multiplicity of choices. For these studies, a variety of designs were implemented, and system users had many models to choose from. No authentication model is known to provide as much freedom of choice. In most existing systems, a user only has a single system or design to work with.

5. Property based systems offer flexibility. All existing graphical authentication systems are rigid. That is, there is normally a fixed grid size and a fixed number of authentication steps. In property based systems, however, the size of the authentication grid as well as the number of authentication steps are appropriately selected by the user.

6. The system is highly adaptable. Unlike in the implementation of existing systems, every implementation of the property based concept could be redesigned to accommodate more properties. In doing this, the complexity of the system is increased with a proportional increase in the security of the system without compromise to the system's usability.

7. One important issue that has hindered the development of graphical passwords is the issue of image selection. This is an issue which many systems, even commercialized systems such as the passfaces scheme have to contend with. System supplied images are more secure, while user chosen images are more usable. The tradeoff between that two has remained a topic of discussion. In property based systems, however, a user selects his 'properties' during registration, but the system supplies the images for authentication, thus eliminating the contention between user-chosen and system-supplied images.

8. Novel concepts and ideas have been developed and evaluated as part of this work alongside and apart from basic research into the various subdivisions of property based systems. Ideas such as the mixing of models, property based ordering and organised image selection styles have all been implemented and investigated in the course of the research work.

9. The development of this novel approach to user authentication is one of the contributions to knowledge as presented in chapter three.

10. Several usability and security evaluations have been conducted as part of the contributions to knowledge. The results for these studies are presented in chapters five and six.

1.7 Cognitive Theories and Information Retrieval

One of the most important issues relating to the development and use of authentication systems is the ability of users to use and retain passwords over long periods of time. Hence there is a very close relationship between the design of authentication systems and how they are stored in and subsequently retrieved from user memory. Recognition and recall are the main design concepts in authentication systems and also determine the way information is both stored and retrieved.

1.7.1 Basic Components of Human Memory

To understand the ideas of recognition and recall, one also has to understand the underlying psychological principles governing human memory. Several models have been proposed to depict the relationship between memory structure and processes and how they interrelate. A model proposed by [22] is discussed in this section. To better understand the workings of the system, the following definitions need to be understood:

Sensory Register: Information collected by various sensory organs from the external environment are stored in the sensory register. The information stays there for a very short time.

Short-term memory (STM): If the individual is paying attention when the information is obtained, then the information is transferred from the sensory memory to the STM. The STM holds the information as memory codes, that is, mental representations of the selected parts of the information.

Long term memory (LTM): Through rehearsals and other control processes from the user, information contained in the short term memory is transferred to the long term memory where it is further processed and encoded. The encoding is, however, most effective if the information can be attributed to something meaningful.

Control processes: Control processes are those processes that are undertaken by the user. These processes help encode information into the registers. The ability to store and retrieve a piece of information depends on the particular encoding. A superior encoding helps to remember and retrieve processed information easily over extended periods of time. Encoded information is retained by the long term memory as it is rehearsed and practiced over long periods of time.

1.7.2 Human Memory and Information Processing

This section provides a detailed overview of the workings of the various structural features of the human memory and how these components are interrelated. The discussions shall focus on the sensory register, the short term memory, the long term memory and the processes that pass information between these components. To aid in the understanding of the workings of the system, a diagrammatic representation of the model is presented in fig. 1.3.

When and external sensory stimulus is received, there is an immediate registration of the stimulus within the appropriate sensory dimensions. This registration is particularly significant in terms of a visual stimulus (as is the case with authentication systems) as it is understood to form a distinct component of memory unlike the registration of other forms of external stimulus.

The second basic component of the system is the short term memory which is also referred to as a person’s working memory. Information in the short term memory may decay and eventually get lost completely. This memory loss is, however, much slower than the one that takes place in the sensory register. The duration of him within which information is retained in the short term register is independent of the information source. It is, however, dependent on the type of memory process invoked upon by the user. If the user engages in rehearsal process, information in the short term memory takes longer to be lost.

The third and last major component of the system is the long term memory. Information stored in the long term memory does not decay or get lost in a similar way like as does in the sensory register or the short term memory. All information is eventually lost in the sensory register and short term memory, but information in the long term register is relatively permanent.

The process by which information flows or is being transferred from one memory component to another is entirely dependent of the system user who generates the processes. During such transfers, part of the information in the memory is copied into the memory to which it needs to be transferred without deleting it from the memory from which it is transferred. It remains in the memory from which it is transferred and decays according to the characteristics of the memory component.

Information flow into the system first resides in the sensory register. From this register, the user initiates a scan to locate the long term register as a result of which the needed information is transferred to the short term register. Information flow from the short term register to the long term register is a continuous process governed by user generated control processes. There also exist transfers from the long term register back to the short term register, also due to processes under user control such as problem solving and other processes that normally involve considerable amounts of thinking. There is also the tendency (as can be seen in fig. 1.3) that information stored in the long term memory is gradually lost due to interference with other information learned. The phenomenon is part of a concept known as interference theory.

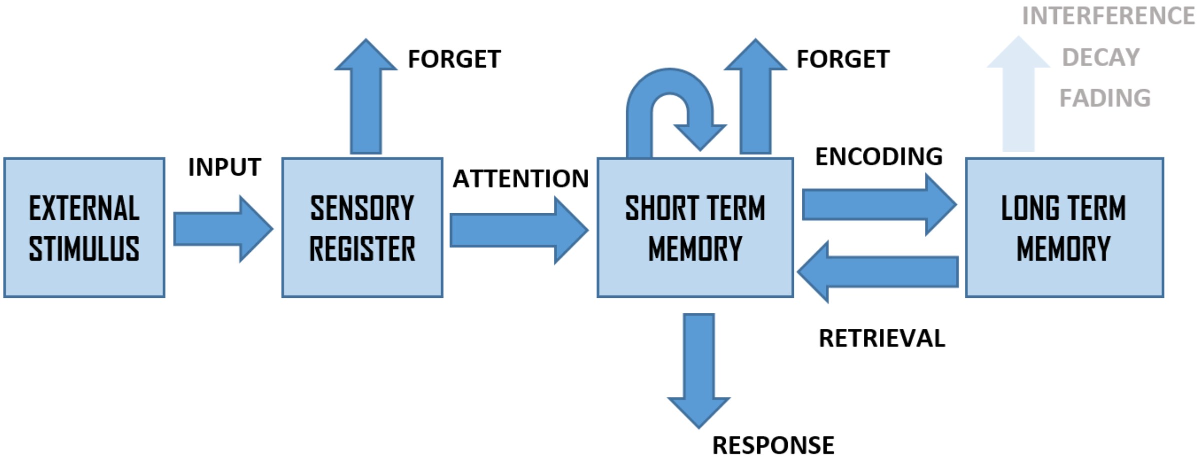


Fig. 1.3: Human memory and information processing [22].

1.7.3 Password Memorability Problem

The tendency of users to resort to insecure behaviour in the handling of passwords arises primary due to limitations the long term memory (LTM) as they experience difficulty in the remembrance of complex pseudo-random password over time. The power law of forgetting [23] is associated with rapid forgetting immediately after learning, which is then followed by a gradual decay over a long period of time. Psychological studies have proven that decay and interference with other information in the long term memory are the main causes of forgetting [24]. While information that is not constantly refreshed or rehearsed often enough is easily lost, information that is jumbled up with other information in the long term memory such that happens with the use of multiple passwords for multiple accounts, separating the contents of the various passwords or identifying which password belongs to which account becomes an issue. Strong passwords normally adhere to password policies demanding the mixing of characters and may be only learnt by rote memorization [25], a repetitive and weak way of remembering. To cope with password memorability issues, users resort to the use of weak passwords or to series of insecure behaviour. Memorability, however, is not the only reason for users' poor password practices, many users are simply unaware of the strengths of modern password cracking techniques.

1.7 Thesis Structure

The report presents a comprehensive study of a novel hybrid graphical authentication algorithm that is able to combine usability and security in graphical authentication through the association of images with properties and using the properties as means of user identification rather than specific images as used in existing systems.

The first chapter (the introduction) provides a generalized overview of the research study. It gives a statement of the research problem, the motivation for the research, the research question, the research aim and objectives, as well as the research methodology and its contributions to existing body of knowledge.

Chapter Two (literature review) provides a review related literature. In this chapter, a number of existing recall and recognition based graphical authentication systems are discussed and their usability and security strengths and weakness analysed based on data from available literature. The chapter also explains the significance of predictability and shoulder surfing as significant security issues in the design and implementation of authentication systems.

Chapter Three provides a conceptual overview of the property based graphical authentication approach. It provides simplistic explanation of the idea of image properties and their corresponding variants, the classification of property based schemes and models, as well as underlying concepts, ideas and terminologies.

Chapter Four (operational procedures for property based authentication systems) provides detailed explanation on the metrics used in the security and usability evaluation of property based authentication models. It also provides details of the design and operational procedures of the various system prototypes used in the conduct of the research work.

Chapter Five provides detailed discussion on the experimental design, methodology and procedures used in all usability experiments conducted in the research. It provides insight into the analysis tools used in the research, the motivation for the use of such tools as well as discussion of the results of data analysis for all usability experiments conducted as part of the research work. These includes results from user registration (sign-up), authentication (login) and memorability (failure rate) data obtained from system logs, and user experience data obtained from survey questionnaires.

Chapter Six, as Chapter Five, provides details of the experimental design, procedures and results of all security experiments conducted in the research. This includes results for various vulnerability tests conducted as part of the security evaluation of the various prototypes used in the research

Chapter Seven provides discussion of comparative usability and security evaluations in relation to existing graphical authentication systems. The existing systems include representative models from the recognition based, recall based and cued recall based systems compared to the performance of a fill based property based model.

Chapter Eight presents the conclusion. This chapter includes the summary, conclusion, recommendations, constraints and limitations faced during the work and the work's future direction. It is followed by the research's list of references.

Chapter Two – Literature Review

SECTION I – Review of Existing Authentication Systems

2.1 Introduction

This chapter provides a literature based review on the evolution and evaluation of existing authentication systems. The chapter is divided into the two sections. The first section provides a general overview of the developmental trends in the design and proliferation of authentication systems focusing on the security and usability issues in relation to these systems. The section also looks more closely into some of the most common user-related security issues which include guessability, shoulder surfing (observability) and vulnerability to description that have all been investigated in the course of this work. The second section takes a closer examination of three of the existing graphical authentication systems; the passpoints scheme, the passfaces scheme and déjà vu, a system that uses pictures and random art (abstract) images. Random art (abstract) images are coloured computer generated images that do not have a definite form. The section provides insight into important research finding related to the usability and security of these systems.

2.2 Overview of Existing Authentication Methods

In the literature, authentication methods have been developed and classified based on what is required of a systems user in the process of authentication. These methods include:

Something you have (Token based authentication) [26,27]

Something you are (Biometric authentication)

Something you know (Knowledge based authentication)

Token based authentication involves the use of additional devices such as key fobs, bank cards and tokens provided to the user for the process of authentication. Token based systems, such as in ATM machines, however, are often combined with a knowledge based component.

Biometric systems utilise human traits and characteristics in user authentication. Human fingerprints, palm scan, iris scan, facial scan and DNA are all used in biometric authentication. Gait and gaze based biometric systems have also been developed. Although biometric systems provide the highest level of security, they mostly have usability issues such as being slow and sometimes unreliable as human physiology may change due to old age or ill health. Other problems with biometric systems include ‘spoof attacks’ [28] and ‘template database leakage’ [29]. They also mostly require the attachment of additional components to traditional computing systems and handheld devices, which are often very expensive.

The most widely used systems today are knowledge based systems which utilise something known only to the user for authentication. The most common of these techniques is the text based system that uses alphanumeric text and numeric PINs [30, 31, 32]. Considerable research has been conducted on the usage and performance of text based passwords including that on people’s attitudes towards the selection of passwords, the strength and memorability of user chosen passwords, the number of passwords users have, as well as the use of passwords by corporations [30]. Graphical passwords were developed as an alternative to text based systems and are subdivided into recognition based, recall based and cued recall based systems [33, 34].

2.3 Overview of Recognition Based Systems

Recognition based graphical authentication systems are graphical systems that depend on the user's ability to recognise images that he had selected earlier from a large collection of images. In each round of authentication, the user is presented with many images from which he is expected to recognise and correctly select the images that represent his chosen password.

Several recognition based schemes have been developed and evaluated. Among these is the déjà vu scheme developed by Dhamija and Perrig [7] which used Harsh Visualisation Technique [35] to generate a set of abstract images using a computer algorithm (fig. 2.1). The déjà vu scheme is an example of a grid based type of recognition based graphical authentication system. To study the déjà vu scheme, the researchers developed system prototypes that were implemented and analysed in a study that involved interviews and web-based user studies. Two user studies were conducted using déjà vu systems that used photographs and random art images in which twenty research participants were recruited (11 males and 9 females) to compare the déjà vu system to traditional password based systems (passwords and PINs). A within user study was used with each user testing each of the four system prototypes presented, two for the déjà vu systems and another two of each of the textual and PIN based password systems. The tests were conducted in two sessions, one week apart. Although relatively slower in password creation and login time, memorability of the déjà vu system was better than in text based passwords ad PINs. No login failure was recorded for the déjà vu system during the first session, unlike the passwords and PINs that recorded 1 failure (5%) each. After a week, the login failure had increased to 7 (35%) for PIN and 6 (30%) for passwords while the déjà vu systems recorded 2 (10%) and 1 (5%) for the random art and photo based schemes. In spite of the improved memorability, a usability issue with the déjà vu system is that the seeds of each of the algorithms had to be stored separately to ensure that the exact image could be reproduced in the future. Another basic flaw of this work is the very low sample size. An improved version of this scheme was developed in [36]. Their Image Based Registration and Authentication System (IBRAS) used a function called a SHA-1 harsh function. It was more secure and used less memory than the earlier version. Although similar in their storage of initial seeds, the main difference between the implementation of the IBRAS and the déjà vu system is that in the IBRAS, a user chooses and uses a single graphical authentication image. Although the déjà vu scheme performed well with its use of abstract images, researchers believe it is easier to remember images that have some meaning attached to them [33].

Researchers in [38] introduced and evaluated the Convex Hull Click (CHC) scheme. In this scheme, a participant selects a set of icons from a large set of icons during the registration stage. In each authentication round, the participant is expected to identify his pass-icons in every challenge set. An authentication round consists of several challenge sets. A challenge set is a set of images presented in an image grid containing some of the user's pass-icons and many decoy icons. The participant is expected to click inside any triangle (convex hull) formed by any subset of his pass-icons. The researchers conducted a usability study comprising of two sessions, one week apart in a between user study with 15 participants (6 males and 9 females), mean age 37 (StdDev = 13.6) using a software prototype. The first session took about 15 minutes to collect data on the number of correct and incorrect logins, the number of correct and incorrect challenges, and the total time for each correct and incorrect login and challenge. Each participant was asked to authenticate himself onto the system until he/she is able to get up to ten successful logins. Experimental results indicated the mean penetrance correctness of entries was 90.35%, the mean correctness of the challenge sets was 97.95%, while the mean time for correct password inputs was 71.66 seconds. Statistical evaluation of the results shown a statistically significant smooth reduction in authentication times between the ten correct logins collected from participants. The results also indicated that participants whose challenge sets comprised of 5 pass-icons were faster in login times that those with 3 and 4 pass-icons in their challenge sets. No statistically significant correlation was identified between the login times of those with 3 and 4 pass-icons in their challenge sets. In the follow up session one week later, the participants were shown a list of 112 icons and told to identify the 5 pass-icons they had used in the previous experiment. Only 1 of the participants was unable to identify all the 5 pass-icons, the participant was only able to identify 4.

In order to compare with other recognition based systems, the researchers detailed a number of experiments to compare the usability of the passfaces, déjà vu and the VIP schemes with alphanumeric PINs and passwords. The VIP scheme is a graphical PIN authentication system that is meant for use with both a PIN and an ATM card. The researchers discovered that although déjà vu compared better to the alphanumeric PINs and passwords in terms of memorability, the efficiency of déjà vu was lower due to the longer times it took to authenticate. Weinshall and Kirkpatrick proposed a number of graphical schemes in [35]. Their methods used picture, object and pseudo word recognition schemes with a considerably large number of images. With the aid of prototypes, they ran user trials that lasted for three months. They realized that for the picture based model three aspects of their procedure made the largest influence on the accuracy and retention. These were: choosing picture groups with a clear theme but individual distinctions, the number of training sessions, and the frequency of testing. Overall, the systems had good memorability as users could recognise their chosen images even after several weeks. The picture based implementation, however, proved to be more effective than the others. While the pseudo-word model had a 70% success rate at the end of the three months period, the picture based model recorded about 90%.

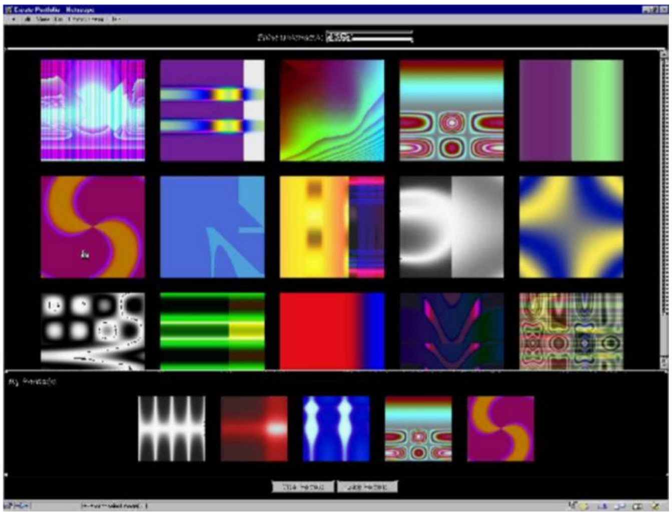


Fig. 2.1: Abstract images (Déjà vu)

Sobrado and Birget [40] proposed a number of shoulder surfing resistant schemes. Shoulder surfing is the ability to observe a user's password by simply looking over their shoulders [41]. Their models were an extension of the Convex Hull Scheme (CHC) proposed by Wiedenbeck et al. [38]. In their first approach a user had to locate any three of his chosen password images and click inside the convex hull formed by those images (fig. 2.2). In the second approach, the user needed to position one of his chosen images in a movable frame, and then move the frame to align with any other two of the user's chosen images to authenticate. The researchers also introduced a third scheme in which the a user had to locate any four of his chosen images and then click on the point of intersection of invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. No details of experimentation with these schemes has been reported in the literature. To decrease guessability, the researchers suggested the use of thousands of images. According to the researchers, the number of possible passwords is a "Binomial Coefficient" $\binom{N}{K}$ (choose any K object among N). Hence when N = 100 and K = 10, the number of possible passwords becomes $\binom{1000}{10} \approx 2.6 * 10^{23}$, which is a little more than the number of alphanumeric passwords of length 15. However, a large number of images on a small computer screen makes the screen highly compacted thereby creating usability issues. In fact researchers in [43] discussed two significant drawbacks of this scheme. The first was a technical drawback in which the researchers developed a system prototype using 1000 icons as suggested in [40]. However due to the size of a standard computer screen, it became impossible to distinguish one icon from the other. The second drawback was a "theoretical complication". Let K denote the number of user chosen pass-images, N the total number of images displayed on the screen and h the number of authentication screens for an authentication round. They argued that 10 pass icons (K) were suggested on [40] and that from a theoretical assumption: *"There is a constant c > 1, which depends only on the size of the screen used such that the probability of the center of the screen being in the convex hull of the K randomly placed pass-objects is greater than* 1 - $\frac{1}{C^{k-1}}$ ". This meant that if K objects are randomly placed on computer screen, an attacker can play a wait-and-hunt. For each image (screen), the attacker may just click in the center of the screen and the probability of a successful login is *q* = (1 - $\frac{1}{C^{k-1}}$)^{h}. For a standard sized screen, c ≈ 1.5, and thus, we have q ≈ 0.77 when K = 10 and h = 10 and q ≈ 0.45 when K = 10 and h = 30. Therefore, the K pass icons will have to be moved as a group all over a screen. This complicates analysis of the scheme, since a mouse click always gives an attacker some hint. Another drawback is that authentication in this systems may be considerably slow due to the time it may take in locating the images, lowering the efficiency of the system.

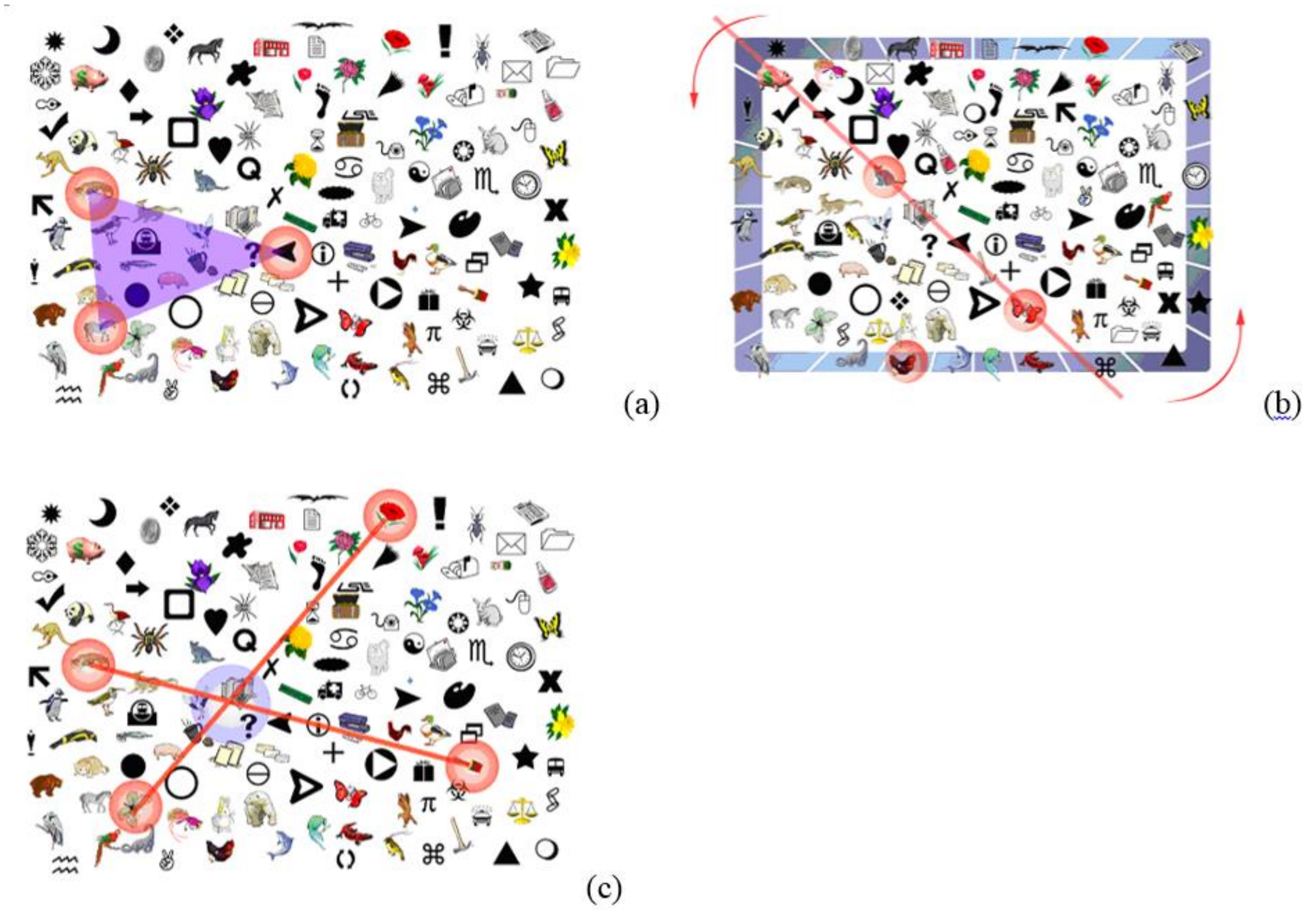


Fig. 2.2: Sobrado and Birget schemes [40]: a – Convex hull, b – Movable frame, c – Intersection.

An algorithm for filtering distractor (doodle) images was suggested in [42]. The algorithm was used to filter out images due to their similarities based on the number of black and white regions as well as the number of joints possessed by each image. The aim of the algorithm was to identify similarities in distractor images to be presented as decoy images in the course of authentication. The assurance that simple doodle distractor images do not possess obvious similarities with the users pass images improves usability by reducing user input errors.

Man, et al. proposed a system [43] called WIW (where is Waldo?) which borrows its name form a popular puzzle game. In this scheme the graphical interface is made up of several login images (called a scene). Each scene is made up of several many objects from which a user selects his pass-objects and a set of perturbation. Each authentication round is performed such that a user is presented with several scenes depending on his exact selection. Each scene represents a challenge set in which a user presented with his pass-objects and many decoy or non-pass-objects. He is expected to identify and select his pass objects from a mixture of pass and non-pass-objects contained in the scene. The perturbations are a number of variants developed for both the pass and non-pass objects such that during authentication the user can select any of the various perturbations (or variants) of his chosen images. A monitor’s screen can be viewed as a rectangle with width a, and height b. Each scene is displayed on such a screen. For each scene, WIW renders two small icons of eye shape at $(\frac{a}{3}, \frac{b}{2})$ and $(\frac{2a}{3}, \frac{b}{2})$, respectively. These icons are designated as the left and the right eye. In the process of authentication, as the pass and non-pass objects are shuffled across each scene, the user has to relate the position of each of the designated eyes to the various positions of his pass objects within the scene. Although a prototype of the system was developed and experimentation was performed using a number of research participants, the methodology adopted for the experiment as well as the details of its results were not provided in the paper.

The system in [43] was improved upon by Hong et al. [44] in which every image had several variants and each variant was associated with a unique code. System users are presented with a scene during authentication, the scene containing pass object variants randomly selected and presented among many decoy images. To authenticate, a user types the code associated with his pass image variants and the relative position of his pass image among decoy images as observed on the computer screen. According to the researchers, the system proved resistant to shoulder surfing, although users had to both recognise their images as well as memorise the codes for the various image variants which may affect the memorability and overall usability of the system. Although an experiment was reported to have been conducted by the researchers, the details of the experiment as well as its results were not reported. An improvement was also proposed in which a system user assigns his own codes to his preselected images (fig. 2.3). The need to memorise such code, however, meant that it suffered the same fundamental usability flaws as the previous scheme.

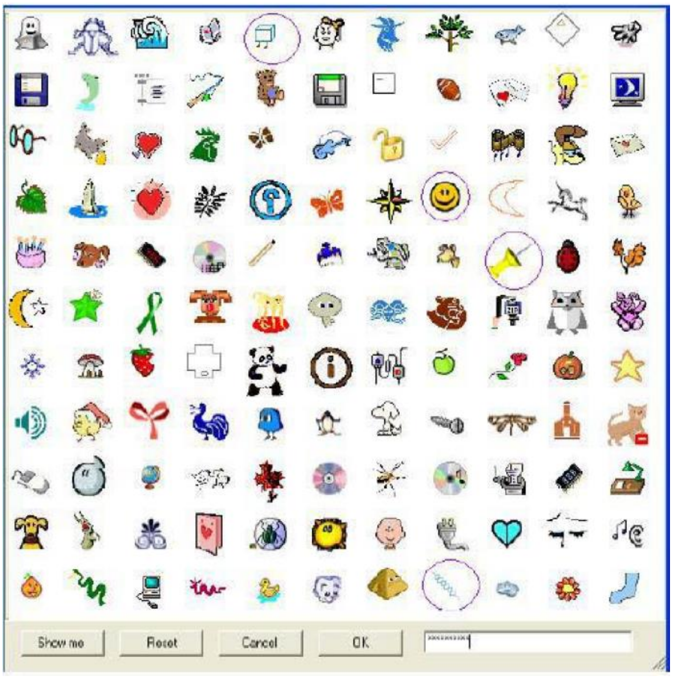


Fig. 2.3: Shoulder surfing resistant scheme by Hong et al. [44]

The *passfaces* technique was developed by the Real User Corporation [45]. The idea came from the belief that humans find it extremely easy to remember the faces of other people even after prolonged periods of time. In the implementation of this scheme, a user is presented with a large database of human faces from which he is expected to select any four random faces. During authentication, the user is presented with four successive grids, and is expected to recognise and select his chosen faces among eight distractor face images (fig. 2.4). Considerable research has been done on the usability and security of the passfaces scheme.

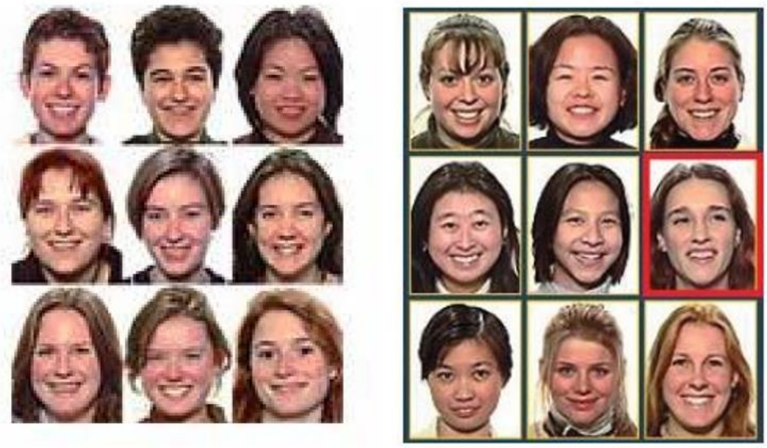


Fig. 2.4: The Passfaces Scheme [45]

Studies into the effectiveness of the passfaces scheme conducted by [46, 47] indicated that passfaces could easily be remembered even after a prolonged period of time. One of these was a within user study conducted by T. Valentine [46] involving 77 staff and students of Goldsmith's College to test the memorability of the passfaces scheme. All participants used the passfaces scheme to test 3 conditions. For the first condition, 29 participants were asked to login to the system every working day for a period of 2 weeks. The participants remembered their passwords in 99.98% of logins. The second condition used 29 participants to login after about 7 days of initial enrolment. Most (83%) of the participants were able to login on their first attempt. Everyone was, however, able to login on the third attempt. For the third condition, 19 participants were asked to login once after about 30 days of initial enrolment. In this condition too, 84% of participants were able to login on their first attempt, while all others were able to login by their third attempts. The passfaces scheme is also believed to withstand long term recall as the study participants were asked to login to the systems after more than five months of their last use [47]. While 56 participants were able to participate in the follow up trial, 72% were able to login on their first attempt and 84% by the third attempt. It was also reported that the participants that used the everyday login condition could remember their passwords the best, with 87% remembering the passwords in the first attempt and 100% remembering them in the third attempt.

Other studies in [48] revealed that the login failure rate of passfaces was less than that of text based passwords, but login time was longer. Davis et al. [45], however, discovered predictable patterns in the passfaces scheme as users were attracted to beautiful faces, faces of the opposite sex and members of their own race. In this study, the researchers analyzed observations collected during a roughly four month semester period of two universities in which two graphical password systems were used by 154 research participants. One of the schemes was a face based password systems modelled after the passfaces scheme [45], while the other was a story scheme developed by the researchers. Each participant was randomly assigned one of the two graphical schemes. Each of the students used his graphical password to access published content that included his or her grades, class assignments, assignment solutions and reading materials through the use of Java enabled browsers. In total, 174 passwords were created during the semester, indicating that a number of students changed their passwords at least once during the study. A total of 2648 login attempts were recorded, out of which 2271 (85.76%) were successful logins. At the end of the semester, an exit questionnaire was used to both capture the demographics of the participants as well as the reasons why they each selected their faces (for the face scheme) or their chosen stories (for the story scheme). The results of the experiment revealed that in the face scheme, both males and females chose the faces of females significantly more often than the faces of males. In fact, over 68% for females and over 75% for males selected female faces. It was also observed that when males chose the faces of females, they almost always chose the faces of models. This accounted for roughly about 80% of male selection of female faces. This fact was also supported by participants' remarks in the research questionnaire. The researchers also recorded a significant correlation among members of the same race. Asian and Caucasian females selected faces of people from within their own race about 50% of the time, Caucasian males chose the faces of Caucasians over 60% of the time, while black males chose the faces of blacks about 90% of the time. With these results, the researchers refuted the argument that user-chosen graphical passwords of the face and story schemes are likely to offer additional security over text passwords without users being trained to select better passwords. System assigned passwords was suggested as possible solution to the predictability problem. This, however, may render the system less memorable, hence negatively affecting its usability. Vulnerability of the passfaces scheme to descriptions was analysed in [50]. The study was aimed at understanding the possibility of verbal descriptions on passfaces and how such vulnerabilities could be reduced. The study was conducted using images from the passfaces online demo using 45 face images (18 males and 27 females). The experiment evaluated three test conditions: random groups (the base condition) in which decoy face images for a target face image were selected randomly, visual groups in which decoy images for a target face image were selected based on visual similarities with a target face image and verbal groups in which decoy face images were selected based on verbal similarities with a target face image. The researchers recruited 56 participants (31 male and 25 female) with an average age of 22 Standard dev. = 7 that conducted lab based trials during a computer science practical sessions. Five face grids were provided for each test condition out of which each participant was expected to identify a target face among decoy images assembled based on the criteria for the test condition in a within users study. A group of 18 contributors (9 males and 9 females) were recruited for the decoy image selection process. The results indicated that of all the 158 login attempts collectively made in the entirety of the experiment, only 13 (8%) were successful. That is, only 8% identified all five target face images in the five face grids of any particular test condition. The random groups had the highest login success rate and the verbal groups had the lowest. The average login success (out of 5) for the random groups was 3.57 (standard deviation = 0.91), for the visual groups was 2.87 (standard deviation = 1.07). The mean variation was statistically significant (t=3.63 p< 0.0). The average login success rate for the verbal group condition was 2.81 (standard deviation = 1.14). The mean variation between the verbal and he random conditions was also statistically significant (t=3.64 p < 0.01). The study concluded that passfaces could effectively be described and suggested the presentation of similar faces in a grid as an effective way of reducing facial disparity, and hence description. It is observed in [41] that keyboard entry was a better alternative in the implementation of the passfaces scheme in a study that compared the security of keyboard based versus mouse based data entry in the passfaces scheme.

A theme based set of graphical passwords [51-53] were proposed by Jansen et al. for mobile devices. In this systems, a user selects images which represent themes (such as the sea, the forest, group of animals, etc.). Some themes comprise thumbnails of pictures which when put together will form a particular image, others comprise a set of similar images. A user selects a number of images in a sequence within this theme as his password (fig. 2.5). During authentication, the user needs to select his images within the theme in a definite order. The system also allowed users to submit and use their own set of images [52]. A method called “salting” was proposed to increase the security of the system against observational and specialized dictionary attacks. Salting is the process whereby the clear text value of an image password is prepended with a random numerical value *R* called a salt. Through salting, the search space of an attacker is increased by a factor $2^{|R|}$ if the attacker does not know the salt. Although details of the system implementation were provided in [52], the researchers did not publish any details of any experiments or experimental results. The main limitation of this system was the fixed size of the mobile screen, which limited the number of thumbnails used, a great hindrance to the efficiency and usability of the system.

Another graphical scheme was proposed by Takada and Koike [54] which allowed a user to submit his favourite images to the server as his password. In each round of authentication, the user only needs to recognise the images he had submitted among other decoy images. If none of the user's images are presented on the screen, the user selects nothing. The idea of an online registration for every image submitted by the user as well as the use of image notifications as provided by the system greatly improve security. No experimental or design details were, however, reported for the system. Submitting one's own images greatly improves memorability, but also makes it easier for an intruder who knows the user to easily guess the password [48, 55], a great setback on security.

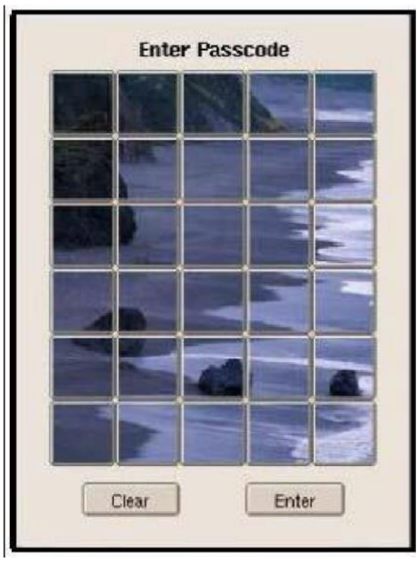


Fig. 2.5: Theme based graphical technique

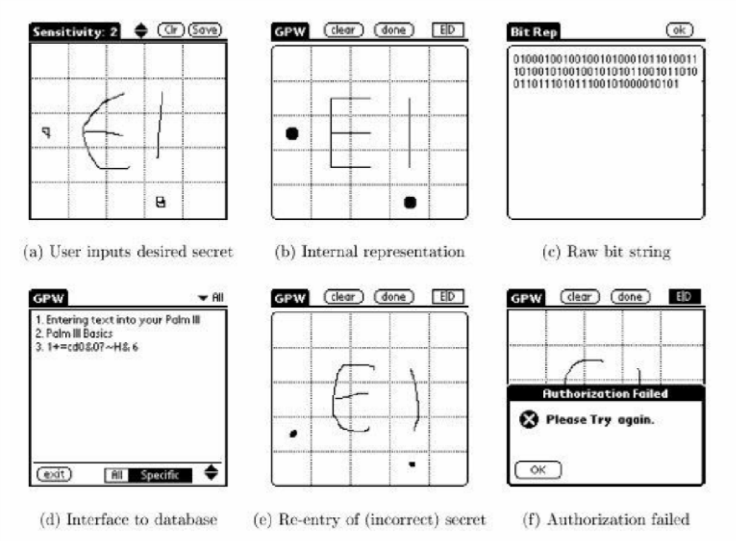
2.4 Overview of Recall Based Systems

Recall based systems are systems in which a user performs a series of actions during registration and is expected to repeat the actions, in the same order, during each authentication round. They are mainly divided into two subgroups: (1) Pure recall based systems (2) Cued recall based systems.

2.4.1 Pure Recall Based Systems

Pure recall based systems are systems in which a user is expected to fully recall a piece of action from past memory to authenticate. Majority of these systems present a blank touch sensitive screen during each authentication round upon which a user is expected to reproduce an image he had drawn earlier during registration.

A technique called *Draw a Secret* (or DAS) was proposed by Jermyn et al [56] which allowed users to draw their own pass images on a 2D grid using a touch sensitive screen. The coordinates of the drawn image on the grid are stored on the system in the order in which the drawing occurred. The user has to repeat the drawing in exactly the same order each time he wants to authenticate. The password space for the DAS system is larger than the text password space. Another advantage of the DAS scheme is that since it is independent of any alphanumeric strings, it can well be used by speakers of any language.



```
010001001001001010001011010011
101001010010010101011001011010
0110111010111001010000010101
```

(a) User inputs desired secret (b) Internal representation (c) Raw bit string

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&07~H& 6

Authorization Failed

Please Try again.

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 2.6: The "Draw-a-Secret" (DAS) system by Jermyn, et al. [56]

A number of researchers have investigated the usability and security of the DAS password scheme. One of such was presented in [57]. In an analysis of the memorable password space of DAS, the researchers developed the concept of graphical dictionaries which was used to study the susceptibility of the DAS scheme to brute force attacks. They postulated that since mirror symmetry had a significant position in human cognitive memory, it was possible to develop an attack dictionary based on symmetric patterns. A performance comparison of mirror symmetric and asymmetric images was also performed, which led to the conclusion that symmetric images were more preferred by system users, but were also less secure. Another study [58] investigated the impact of stroke count on DAS password strength and observed that the higher the stroke count the stronger the password. The study was aimed at investigating the relationship between the number of composite strokes, the dimensions of the grid and the length of the DAS password in the DAS password space. In doing this, the researchers introduced DAS password complexity properties based on pattern complexity factors which included password length, number of composite strokes (or the stroke count), symmetry, or the number of turns in each stroke. The study was to understand if any of these factors could have an effect of the DAS password space such that it was possible to perform a brute force attack on a DAS password using a graphical dictionary. The study proved that when users choose with less than 5 strokes with a password of length less than 13 on a 5 × 5 grid, instead of the maximum of 12 strokes, the password space of the DAS password is reduced from 58 bits to 40 bits. To further strengthen the DAS password, the researchers proposed the grid selection technique (fig. 2.7) in which a user selects a small rectangular section of the grid as his drawing grid, which is then zoomed into before the password is created. This method significantly increased the password strength of the DAS system with an increase of up to 16 more bits. The researchers, however, did not report any user study. Dunphy et al. [59] also tried to improve the security of the DAS password through the introduction of background images in a method called Background DAS (or BDAS). In this method, a user first had to select a background image, and while the chosen image appears faintly at the background of his DAS grid, the user draws an image on the grid as is done in a normal DAS password (fig. 2.8). In two laboratory studies with paper based prototypes, the researchers investigated the effects of background images on the memorability of the DAS password as well as the effects of background image choice on user performance in the BDAS password scheme. A total of 21 subjects were recruited for the first experiment, 15 male and 6 female aged between 18 and 50+ that cut across technical and non-technical disciplines. Participants were split into two groups, the control group that used a prototype representing the original DAS system and the BDAS group that used BDAS prototype. Five (5) picture images were used for the background and participants were allowed to use images of their choice. The results of the first study (the pilot study) revealed that 90% of the DAS group employed global symmetry as opposed to 50% in the BDAS group. Also, 90% of the passwords used in the DAS scheme used were centred within the grid as opposed 70% in the BDAS scheme. The lengths of the passwords created by the BDAS user was significantly greater than that created by the DAS users. The t-test results showed $t=2.377$, $p < .0$. These results imply that the users of the DAS scheme employed centralization and symmetry as means to aid recall and that the BDAS users created longer passwords. In the second study, 46 participants were recruited, 32 male and 14 female with most participants between the ages of 18 and 25. While 20 participants had technical backgrounds, 26 were from non-technical disciplines. Participants were equally split into two groups as in the first stud. The results from this study indicated that 43% of the BDAS group exhibited global symmetry as compared to 57% for the DAS group. In terms of image centering, 43% of the BDAS passwords exhibited image centering as against 87% for the DAS group. While the recall rate was better for the DAS password after the first five minutes (96% and 100%), the recall rates were same at the end of the first week (95% for both). The study also indicated that the complexity of the passwords selected by the BDAS users was significantly higher than that for the DAS users with t-test indicating t=2.78 p < 0.01. In spite of the increased complexity and length of the BDAS passwords over the DAS passwords, user performances in both systems were similar. Hence the researchers concluded that in spite of its apparent increased complexity, the implementation of BDAS helped improve the memorability of DAS passwords.

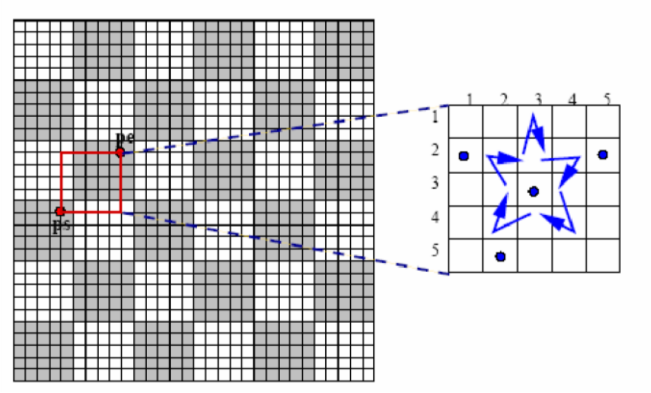


Fig. 2.7: Grid based techniques developed by Thorpe and Van Oorschot [58]

Goldberg et al [60] proposed the *passdoodle* technique in which the user produces a small design or text on a touch screen. The researchers used a between-user design with 13 participants using paper prototypes to investigate the viability of the passdoodle scheme in user authentication through an understanding of the memorability and user preferences in comparing the passdoodle scheme to alphanumeric passwords. The study was divided into two login sessions one week apart to create and recall a username and one alphanumeric and one doodle password. Their studies observed that users could accurately remember how they drew complete graphical images, yet mostly forget the sequence in which the various components of the image were initially produced. Hence the researchers observed that if the restriction of ordered login is removed for subsequent implementations of the passdoodle scheme, it will greatly enhance the usability and memorability of the system.

A further study to analyse the predictability of the DAS password was conducted in [61]. In spite of lacking any predictable patterns, it was discovered that at both the beginning and the end points of the password strokes, some characteristics such as rectangles, letters, numbers and crosses were common and that users generally preferred passwords that were predictable, hence insecure, in favour of memorability. In a paper based study with 16 participants, 10 male and 6 female, aimed at understanding if predictable patterns will appear in the implementation of the DAS password scheme, the researchers discovered that approximately 45% of the users chose symmetric passwords, 2/3 of which were mirror symmetric (reflective). Approximately 80% of users chose passwords composed of 1-3 strokes, 10% chose passwords composed of 4-6 strokes, and 10% of the users chose 6 or more strokes. With regards to the centering of passwords within grids, 56% of the passwords were centered, an additional 30% more were approximately centered, that is, centered on a set of cells adjacent to the central grid lines.

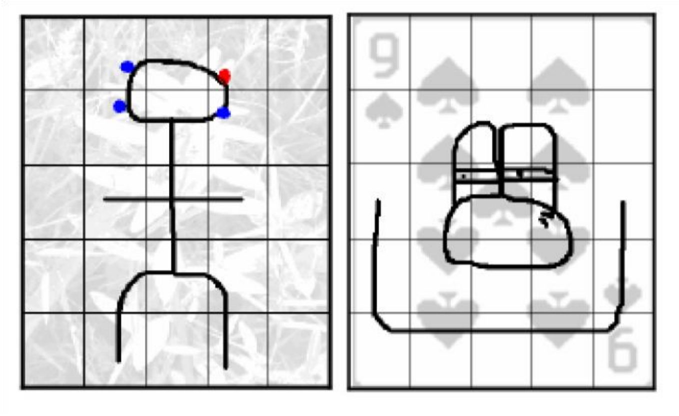
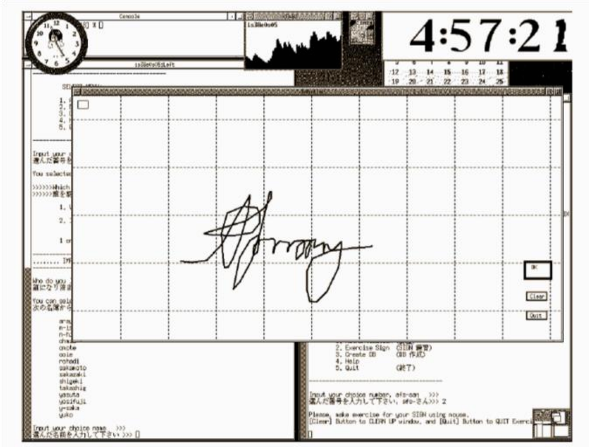


Fig. 2.8: The Background DAS (BDAS) scheme [59]



```
2. Exercise Sign  (SIGN 練習)
3. Create DB      (DB 作成)
4. Help
5. Quit           (終了)

Input your choice number, afs-san  >>>
選んだ番号を入力して下さい, afs-さん>>> 2

Please, make exercise for your SIGN using mouse.
[Clear] Button to CLEAN UP window, and [Quit] Button to QUIT Exerci
```

Fig. 2.9: The signature scheme

The signature scheme was proposed in [62]. The scheme is presented in figure 2.9. In this scheme, a user is asked to draw his signature on a grid during the registration stage. The coordinates of this signature are immediately stored on the system and confirmed by a further verification stage before any round of authentication. The success of the scheme was satisfactory as the users did not have to memorize their signatures. Users could also replicate their signatures with almost exact precision. To understand the distinguishing factors between user and imposter signatures, the researchers developed a set of signature writing parameters such as number of signature points, coordinates of points, signature writing time, velocity and acceleration and used these parameters against user and imposter signatures. The greatest variation was observed in the use of the acceleration parameter. This was then used in the experiments to differentiate user and imposter signatures. The researchers evaluated the system using two experiments; one with a static signature database in which signature data is registered into the system and kept in the system's database during the registration phase. The data is kept and used for user authentication until a new copy of the signature data is again registered onto the system and used to replace previous data. It was however discovered by the researchers that users become more efficient in the use of the scheme as the number of authentication cycles increased. The signatures became more accurate and took less time to write. Hence, in the second experiment, the researchers used a dynamic database in which the signature data in the system's database was changed occasionally and automatically by new signatures written by the users. In the static DB experiment, the successful verification rate was 91%, while the successful rejection rate was 92%, while in the dynamic DB experiment, the successful verification rate was 93% and the successful rejection rate was 96%. The signature scheme, however, needed proficiency with the stylus as well as the need for additional devices. Moreover, some tolerance threshold had to be set as the password is captured. This allows for better usability, while compromising security.

2.4.2 Cued Recall Based Systems

In cued recall based systems, a user is required to locate and click on a number of click points chosen earlier on an image. The image itself serves a *cue* and assists a user to recollect the series of actions carried out, since these actions were all carried out on the image. In pure recall based schemes activities are done on an empty grid. The idea of click points was first proposed by Blonder [59]. In his design, an image was displayed on the screen which had predefined click points. The user had to click on these points to register and do so in the same order anytime he intends to authenticate (fig. 2.10). Some tolerance threshold is, however, provided for each click point. No experimental prototype of Blonder's scheme was every developed. Hence, no user studies have ever been conducted.

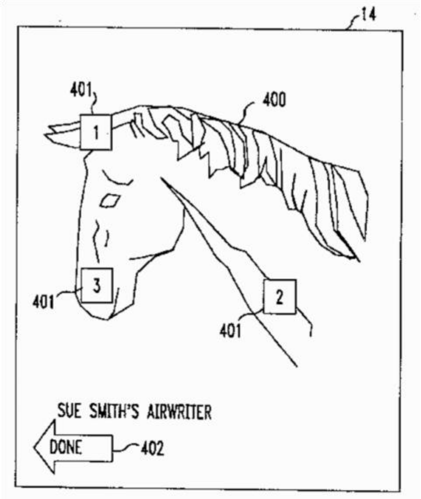


Fig.2.10: Blonder's scheme

Passlogix [64] developed a scheme based on repetitive actions (fig. 2.11) which a user had to choose such as preparing a meal or picking of cards as his password. Researchers have also proposed the variation of grid sizes [65] for grid based systems during each authentication round. Through a web based prototype, the researchers reported that the system was 92% resistant to shoulder surfing attacks. No details of experimentation and or analysis were, however, reported. It was also reported in [66] that Microsoft proposed a graphical scheme in which users click on predefined areas on an image to register and authenticate. The details of the system was not, however, published.

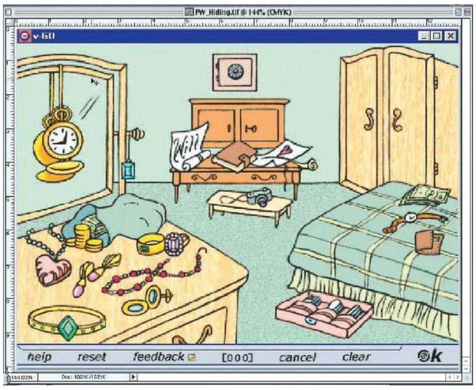


Fig. 2.11: The Passlogix scheme

The ideas of Blonder were further improved through the elimination of fixed boundaries and use of different images by Weidenbeck et al [67-69]. In their models, a user was allowed to click on any part of an image in any order to form his password (fig. 2.12) with some tolerance allowed for each click point. The system adopted the quantization method proposed in [70] and with hundreds of click points to click from, it is believed to possess a large password space. The researchers reported an empirical study comparing the use of the PassPoints scheme to alphanumeric passwords. The participants were split into two groups that created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over a period of 6 weeks. The results showed that the graphical password users created valid passwords with fewer difficulties than the alphanumeric users. However, the graphical password users also took longer and made more invalid password inputs than the alphanumeric password users during the practice sessions. In the longitudinal trials, the two groups performed similarly in the memorability of their passwords, but the graphical group took more time to input their passwords. The researchers also observed that an increase in the size of the image increased the number of available click points within the image thereby increasing both the security and usability of the image. The system of cued click points was also developed and studied in [71] as an optimized version of the click based password scheme. In this system, multiple click-based images are used with one click point per image. The next image is based on the previous click point. The system was tested with 24 participants in a lab study which revealed that the system had considerable promise in both usability and security. From the results, the performance was very good in terms of speed, accuracy, and the error rate. Participants also preferred CCP to PassPoints [69], claiming that selecting and remembering only one point per image was easier, and that seeing each of the images triggered their memory of where the corresponding click point was located. The researchers believed that CCP will provide greater security than PassPoints because the number of images involved increases the workload for attackers. The study, however, suggested further investigation into the memorability (usability) of this systems and the problem of hotspots (security) through more elaborate and longitudinal trials. The effect of tolerance and image choice was studied in [68]. The tolerance study was conducted with 32 participants (undergraduate students), 22 males and 10 females. The mean age was 22.7 (SD = 1.33). The participants were divided into two groups with varying tolerance regions (error margins) of 10x10 pixels (.26cm^2) and 14x14 pixels (.37cm^2). The results showed that accurate memory of the password was greatly reduced when the tolerance was reduced from 14x14 to 10x10. It was observed that small tolerances can greatly increase the space of possible passwords and therefore make the passwords more secure. The nature of the images used in the system may also have a large effect on people’s ability to remember their click points. It was observed that allowing users to choose their own images may lead to high memorability for the user, but may also result in images with poor security characteristics such few click points or high guessability. The study revealed that countless images could be used in the implementation of the passpoints scheme. Further studies conducted in [69] showed that click-based graphical passwords had better security than text passwords, although user training may also take longer. The problem of hotspots in picture based passwords was studied in [72]. The aim of the study was to explore popular points (hotspots) in click based passwords and examine the strategies to predict and exploit them in guessing attacks. The researchers reported both short-term and long-term studies. The first was lab controlled test 43 participants and 17 diverse images and the second was a field trial involving 223 user accounts. The research discovered that hotspots existed in varying degrees from one image to another. The researchers explored the use of 'human computation' to predict hotspots from images and to generate two 'human seeded' attacks. The first was based on a first-order Markov model while the second was based on an independent probability model. Within 100 guesses, the first-order Markov model based attack reveals 4% of passwords in one image's data set and 10% of passwords in a second image's data set. The independent model based attack reveals 20% of passwords within 233 guesses in one image's data set and 36% passwords within 231 guesses in a second image's data set. The researchers also evaluated the first-order Markov model based attack with cross-validation of the field study data, which revealed an average of 7-10% of user passwords within 3 guesses. The research concluded that all click based graphical passwords were predictable and hence vulnerable to online and offline attacks.

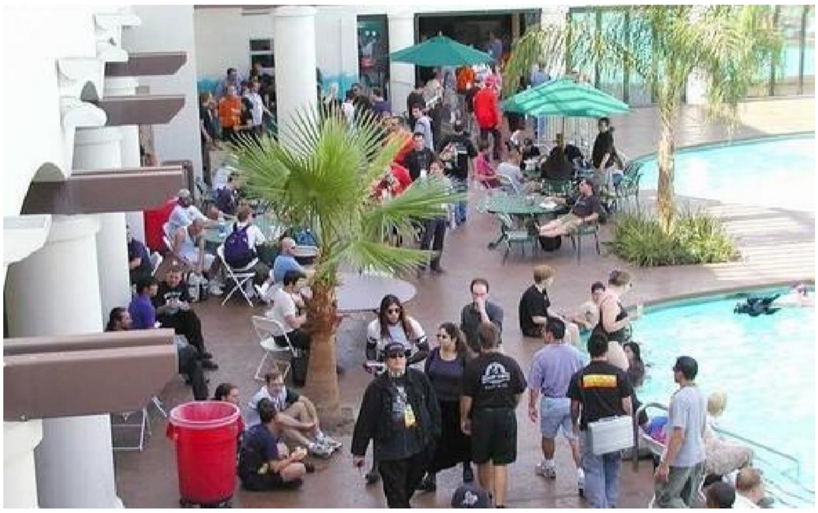


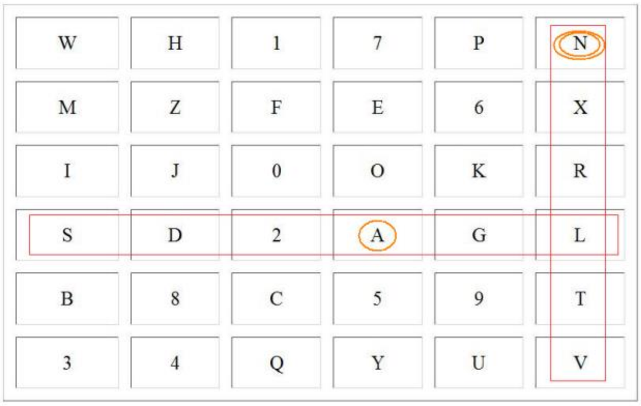
Fig. 2.12: The Passpoints scheme by Weidenbeck et al.

According to [66], a system of navigation through a virtual world for authentication was proposed by a man named Adrian Perrig by which users could randomly create virtual environments and be authenticated by navigating through these virtual spaces. Although it is believed to have the potentials of creating strong passwords, there is, however, no documentation for this system. The use of mnemonics to aid recall have also been studied in [17, 73], where the use of mnemonics was incorporated into a number of graphical systems. In [73], a between-users retention test was conducted for multiple passwords for a control group (Group 0) using PIN based password entry, a graphical password group (Group 1), a group with graphical passwords with signature color background for graphical images to augment memorability (Group 2), a group with graphical passwords with mnemonic strategy to augment memorability (Group 3) and a groups with graphical passwords with mnemonic strategy and colour background to augment memorability (Group 4) where each participant was randomly allocated one of the groups. The study was conducted over a period of four weeks and each participant was allocated 5 passwords. A total of 172 participants participated in the user study. Due to the high dropout rate, however, only 61 participants completed the study. The dropout rate was highest in group 0 in which some participants thought it was impossible to retain multiple PIN based passwords over a relatively long period of time. Their study results proved the superiority of retention of multiple graphical passwords over multiple PINs and that mnemonics could aid even the recall of multiple graphical passwords. The use of mnemonics and degraded images in a recognition based system was also studied in [74]. This scheme, which borrowed its ideas from the story scheme, used a trace line across both the user's pass-images and the distractor images, to safeguard against the shoulder-surfing problem. In a between-user study with 20 participants (10 males and 10 females) with an age range of 20 to 30 years, the researchers compared the new scheme called CDS (meaning "Come from DAS and Story" scheme), with the story scheme in two login sessions, an initial session and a follow up session one week later. The mean password creation time was 42.9 seconds for the story scheme and 49.5 seconds for the CDS scheme. The mean login time was 9.2 seconds for the story scheme in the first session and 23.1 seconds in the second session, while it was 13.7 seconds for the CDS scheme in the first session and 19.8 seconds in the second session. The success rate for the CDS was 80% as compared to 60% for the story scheme. A comparison of the new scheme with the story scheme in terms of observational attacks, was, however, not conducted in the research.

In several studies, the combination of several graphical passwords has been explored. In [75], the researchers deployed the use of a recognition based system in the first stage and a recall based system in the second stage of user authentication. A set of questions (three, specifically) were associated with the recall based phase. The questions help the user in knowing his click points as the click sequence is randomized in each authentication round. No user study was reported for this scheme.

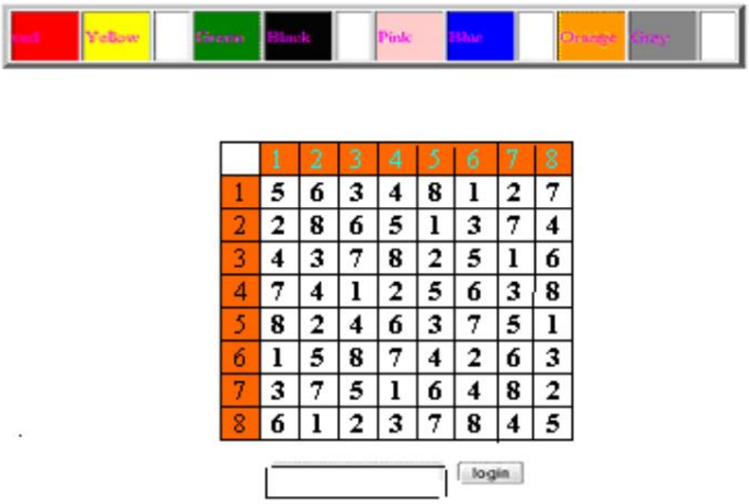
2.5 Hybrid Authentication Schemes

A number of hybrid authentication systems have also been developed. These are systems that combine the elements of recall and recognition based authentication systems or text and graphical authentication systems in order to benefit from the usability and security advantages of both systems [76, 77]. A hybrid system for the generation of session based passwords was presented in [76] and [78], and extended in [79]. The system combines graphical and text based authentication schemes, and during registration, a user needs to select both a graphical and a text based password. To authenticate, the user has to correctly enter both the graphical and text based passwords. Two implementations of the system were proposed. In the first implementation, the user is presented with a text grid (figure 2.13) from which he chooses his password from an intersection of the various rows and columns of the grid which represent his password, while the second implementation suggested the ranking of colours, both of which the user has to remember accurately. The mixing of upper and lower case letters and augmentation with special characters was suggested for the text-based password. The registration phase for this model is presented in figure 2.14. Although the system is believed to be resistant to most common password security attacks, there is high likelihood that the system will suffer from usability issues. A usability evaluation has, however, not been conducted.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 2.13: Intersection letter for the passwords pair ‘AN’.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig. 2.14: Authentication grid and associated colour pairs [76]

Another hybrid graphical scheme is presented in [77] which incorporates a recognition based scheme with dynamic graphics. In this scheme, during the registration process, a user is presented with a 4x4 grid of images from which he selects his chosen password images. Below each image, however, is a random three digit number, and at the bottom of the image grid is a text box. On selecting an image, the user needs to enter the three digit code for his chosen image in the text box. At the end of the selection of all password images, the textbox contains a string of digits which represent the user's password that is saved by the system. The user thus has to remember the exact order in which the password images were chosen.

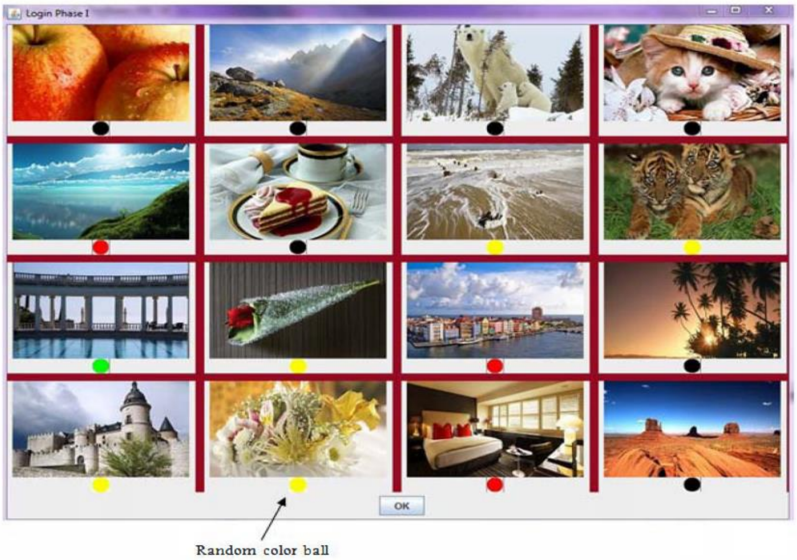


Fig. 2.15: The first authentication phase, 4x4 grid and associated colour balls

The authentication phase for this system is divided into two phases for each of the chosen password images. In the first phase, the user is presented with a 4x4 grid (fig. 2.15) to select his password images. Associated with each of the images and below each image is, however, a colour ball. The user has to both recognise each of his chosen images in the grid as well as remember their associated colour balls. The colour balls associated with each image are randomly assigned per session. In the second authentication phase (fig. 2.16), the user is presented with a 16x1 grid also with a colour ball associated with each of the images. The colour ball associated with each image in this grid is, however, randomly reassigned according to a specific timeframe. The user has to recognise his first selected image and its associated colour ball in phase one and click on this image in phase two only at the time when the colour ball bears the same colour as that associated with it in phase one. The user then repeats phase two for all of his remaining images.

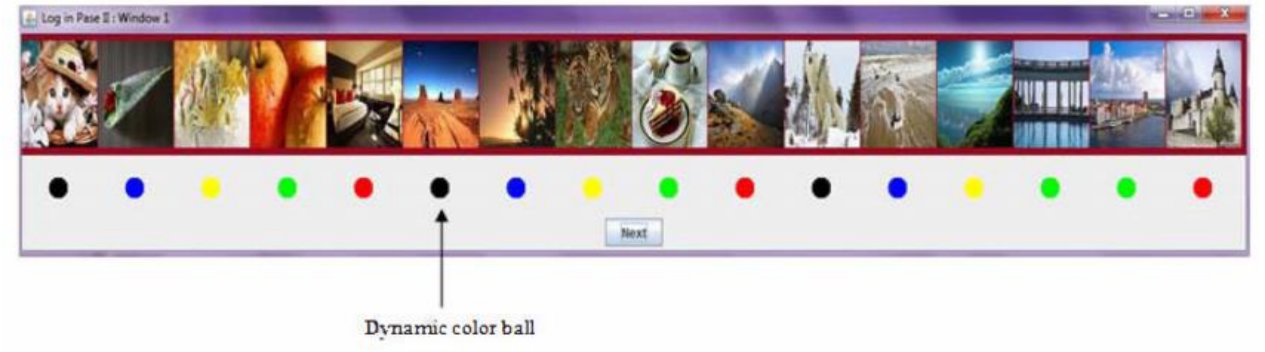


Fig. 2.16: The second authentication phase, 16x1 grid and associated colour balls

In this scheme, when images are presented in the grid for authentication in the first phase, a user is not expected to select any image, but to only observe the colour of the ball below the images. The actual image selection is done in the second phase. This provides extra security to the system as an onlooker may not even understand that the first phase is actually a part of the authentication process. According to the researchers, the system has a large password space, high entropy and is resistant to most common password intruder attacks. Another parameter that enhances the security of this system is the time window within which a user has to select the image in the second phase when the coloured ball for the image seen in the first phase appears.

According to the researchers, the system had both good usability as well as good security as it was both easy to use and to remember as well as being resistant common security attacks. One would expect, however, that the need to memorize a set of images selected by the user in the registration phase as well as the colour balls allocated to each of the images in the first authentication phase, and the need to interact with two separate grids in the system's authentication phase creates additional burden for the usability of the system.

Many other hybrid graphical authentication systems have also been proposed. In [80], a system that uses shape and text is proposed. The system combines a traditional text based password with a shape drawn on a grid as in the DAS scheme. Although the system is believed to be strong against shoulder surfing and brute force attacks, the researchers themselves agree that the system suffers from several usability flaws. Another hybrid model is presented in [81] which combines a traditional password based authentication system with a recognition based graphical authentication system. The registration phase for the text and graphical passwords are done normally. A user enters his text based password which consists of alphanumeric and special characters and then selects a number of images from an image grid. In the authentication phase, the user enters his alphanumeric password and then selects his chosen images from an image grid provided for the selection of the images. The image grid is, however, slightly different from the traditional image grid in which a user needs to click on his password images to select them. In the image grid for this system, below each image is assigned a unique number (fig. 2.17). This number is randomly assigned and changes in each authentication round. A selection panel is provided at the bottom of the image grid in which the numbers are arranged in ascending order from the smallest to the largest. A user selects an image by clicking on its corresponding digit in the selection panel. Hence a user does not need to click directly on an image to select it, but to click on the digit that represents it in the selection panel. This is a strong mechanism against shoulder surfing attacks. The selection panel also helps a user keep track of the various pass images he has already selected as the selected digits in the selection panel remain highlighted till the end of the authentication process. Although the system is believed to be strong against common password security threats, actual user studies to verify and analyse its security and usability potentials had not been conducted.

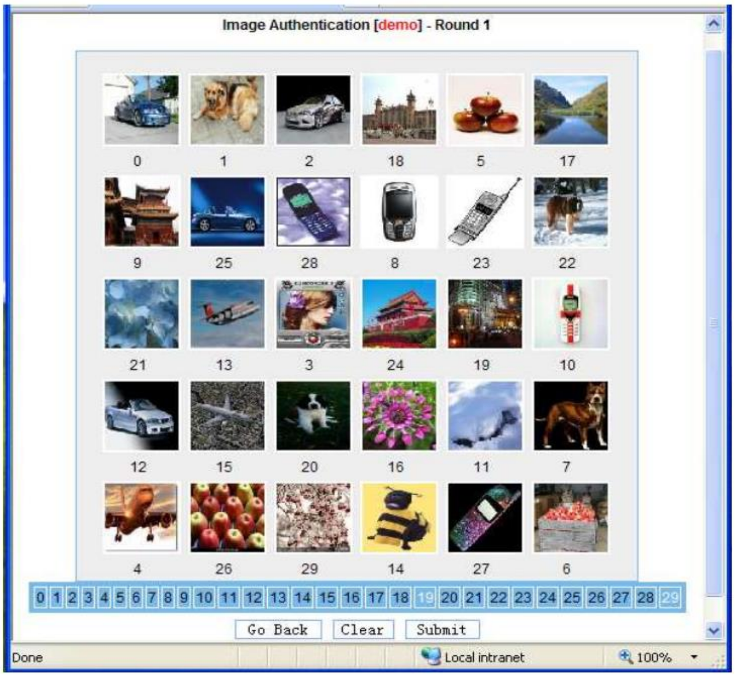


Fig. 2.17: Selection panel for graphical authentication

2.6 Two Factor Authentication

Section 2.2 discussed the various authentication methods through which a legitimate user can authenticate onto a computing device. These include; token based authentication, biometric authentication and knowledge based authentication. Two factor authentication involves the use of any two of these methods in a single authentication system. A typical example is in the use of the bank ATM machine. The ATM smart card serves to provide the user ID and helps the machine understand which account(s) are being accessed. The user then enters his PIN (Personal Identification Number) to show that he/she is the legitimate owner of the designated account. Several authentication systems have been developed that adopt the two factor paradigm for user authentication. The most common of these systems include the use of smart cards [82] for physical access mechanisms, hardware tokens and OTP (One Time Password) for mobile and online applications. The most common security problem with smart-card based systems is the *offline guessing attack* [82]. The greatest usability problem associated with multifactor authentication systems is the need to carry additional device. Systems that combine biometric authentication such as fingerprint recognition with tokenised devices have also been proposed [83]. In [84], however, a gait based two factor system for mobile devices was proposed. Other researchers have proposed the use of three factor [85] and four factor [86] authentication systems as a means of improving upon the security of two factor authentication techniques. This increased complexity may, however, add increased constraints on the usability of the systems.

2.7 Password Security Threats

A number of threats have significantly affected the use of text-based passwords. The exact extent of the effects of these threats on graphical passwords is not fully understood as the deployment of graphical passwords in real user environments is still undergoing research and is in its infancy. Some of these threats are the following:

Brute Force Attack: Brute force attack is the use of the brute force search algorithm to try all possible combinations of user passwords to gain access to a user's account. Since passwords are a combination of letters, numbers and special symbols, brute force attacks take a considerably long period of time. Hence, having a considerably large password space is a good defense strategy against brute force attacks. Graphical passwords are believed to be more difficult to compromise than text based techniques as they are believed to possess a similar or sometimes even larger [56, 59, 62, 70] password spaces. Recall based techniques normally have larger password spaces than both the text and recognition based techniques. The dependency on mouse movements makes graphical passwords more resilient to brute force attacks than text based methods.

Dictionary Attack: A dictionary attack is a password security threat in which the attacker repetitively tries a list of words, called a dictionary to gain access to a computing system. Unlike a brute force attack that uses all possible combinations, a dictionary attacked uses a list of weak passwords that are insecurely used as passwords by system users. Although it is believed that dictionary attacks could be used against some recall based graphical passwords [62], it is definitely more complex to execute especially as they mostly involve the use of the mouse and not the keyboard.

Guessing Attacks: The ability to guess a user’s password is common in text passwords and is further simplified by having some information about the user. Forming passwords with the names of family members or pets and known places or dates is therefore highly discouraged. Guessing is also possible in user defined passwords and password systems with predictable patterns such as the passfaces scheme [45] in which users select beautiful faces, faces of the opposite sex and of members of their own race. The DAS system [56] also showed predictability especially in symmetric and non-symmetric images, according to [61].

Spyware Attack: Spyware are mischievous programs or devices intended to "spy" or gather sensitive information from any system to which they are attached. They are normally used to spy on persons or organisations and may retransmit the information gathered to a third party. Keyloggers are hardware and software designed to keep track of and automatically log user keystrokes onto external media, while mouse trackers are software and hardware designed to capture and store mouse or cursor movement on the screen. Although, it is believed that keyloggers cannot be used against graphical passwords [43, 44], mouse trackers are seen as a potential risk.

Shoulder Surfing Attack: Shoulder surfing is the ability of an intruder to obtain useful password information by simply observing the user's actions from across the user's shoulder. Shoulder surfing is a potential risk in most graphical schemes [43, 44].

Smudge Attack: Most android phones and other mobile devices today use a form of authentication called a pattern lock [97 in which a user tracks a set of dots on the screen. The use of this system may sometimes lead to the pattern becoming traceable due the formation oily deposits on the face of the phone over time. This pattern ‘smudge’ can be used by attackers as investigated by [87].

Social Engineering Attack: Social engineering is the ability to fraudulently obtain useful information from a person through pretext. Social engineers exploit human attributes of love, fear, respect, trust and pity to deceive system users into divulging sensitive information which they later use to gain access into applications or devices. Phishing is the ability to impersonate an entity such as a bank to obtain personal security details from users. For password systems, however, social engineering is effective only if a user password could be described.

Vulnerability to Description: Vulnerability to description is the ability to clearly describe, verbally or in writing, the characteristic features of a user password. Text based passwords can mostly be effectively described, and it is a main concern that many graphical passwords can also be described. Vulnerability to verbal and written descriptions of various image types used as authenticators was studied in [50,88].

2.8 The Evaluation of System Security

A visit to any bank, bank related website or ATM machine and one will be overwhelmed with messages asking bank customers to “protect” their accounts, card and token-based information and “not to disclose” any part of it to anyone. They are warned that the bank “will never ask” for sensitive information via telephone and that they should “beware” of persons or websites demanding sensitive banking information from them. Probably the only other message that is communicated along with these is the demand that the customer complies with the banks *password policy*. These are all messages that are seen every day and are meant for just one goal: to ensure that the bank account user "takes adequate care" of *his own part* of the security chain. The protection of password entry from keen observers is a counter-measure against observational attacks, the refusal to divulge sensitive account, card or token-based information is a counter-measure against social engineering attacks, while the use of "strong passwords" or password policies is a counter-measure against guessing attacks.

This section provides an overview of the main security concerns highlighted and investigated in this research work. Three main issues have been the focus of the security based evaluation and analysis in this work due to their relevance in ensuring the security and applicability of authentication systems, especially as they are directly related to important roles played by system users in the use of authentication systems.

The security concerns include guessing attacks, shoulder surfing attacks and vulnerability to descriptions. Guessing attacks can be performed either randomly (normally called blind guess) or based upon some valid information known to the intruder about the legitimate user (herein called hinted guess). Shoulder surfing or observational attack is the ability of an intruder to steal a user's authentication information by mere observation of the user's login session. Vulnerability to verbal and written description is the susceptibility of an authentication system to be breached by intruders for its reason of being easy to verbally describe or to write down [88]. All the intruder needs to do is to obtain a verbal or written description of a user's password and he uses the descriptions to break the password. Vulnerability to description is itself a factor that reflects the vulnerability of an authentication system to social engineering attacks. Social engineering attacks are efforts made by crafty intruders to convince unsuspecting legitimate system users to divulge sensitive security information to allow the intruder gain access to the system. Studies have considered the evaluation of these three security dimensions to be of equal significance in the design and implementation of authentication systems [89].

According to [4], users are the weakest link in the system security chain. Hence, this work takes a more user centric approach to security by providing a system that can effectively mitigate the security issues that relate to user behaviour, while still providing good usability [90, 91, 92]. The success of such systems will guarantee that organisations do not have to worry about what legitimate system users might do to jeopardize the security of their accounts or the entire system.

In fact, some researchers argue [5, 93] that the idea of users selecting weak passwords is normally due to a lack of motivation in the use of the security systems provided. They believe that the bulk of the problem arises from the way security systems are designed and the lack of proper user orientation on their use.

2.8.1 Analysing the Guessing Attack

This section provides an insight into the need to provide algorithms that can effectively safeguard against guessing attacks in the design of authentication systems. In most security related literature, system users are always advised on the use of strong passwords to counter online and offline guessing attacks. However, guessing attacks are only possible when password systems are predictable, that is, when predictable patterns exist in password application by system users [94]. In a study in 2010, Zhang et al. found out that 41% of passwords from a university system could be cracked in just under three seconds each, when the cracker has some knowledge of expired passwords from the same account [95]. Predictable patterns in password use arise when users choose passwords that can be easily guessed [96]. Many organisations thus impose password policies to make passwords less predictable [97]. A study was conducted by Rainbow Technologies Inc. on the use of insecure passwords in a sample population of 3000 computing professionals, and it was discovered that most system users used insecure passwords. The need to maintain multiple passwords as well as the need to constantly change passwords had intensified the situation as more than 50% of the surveyed population reported having more than five passwords and more than 80% reported that their organisations had imposed policies forcing them to use ‘nonwords’ as passwords or combinations of numbers and letters. This, in turn had forced the users to write down their passwords. Hence 51% of the surveyed user population have reported that they need IT support help to gain access to their accounts and applications as they had forgotten their passwords. This trend essentially underscores the contention that has existed between usability and security in authentication systems in which the need to improve one has consistently diminished the other. A study conducted in [98] on the vulnerability of ATM PINs discovered that the mere knowledge of a user’s birthday is enough to compromise from 1 out of every 11 to 1 out of every 18 ATM cards. In spite of this, researchers have continued to strive for more efficient password systems and better password policies. According to [99] “One weak spot is all it takes to open secured digital doors and online accounts causing untold damage and consequences”. Poorly assigned and poorly used passwords remain the most important causes of password guessing attacks [100] which are among the greatest issues facing authentication systems today [101]. Several graphical based authentication systems have been developed to counter the guessing attack [102, 103, 104].

Since the use of passwords for the maintenance of online accounts is ubiquitous [100] and they are often the first and only line of defense [97], the continued search for a solution to the password guessing problem has become of paramount significance to system security researchers. Since online and offline guessing attacks have utilised various algorithms for text-based searchers, researchers have confronted the problem through the use of complex cryptography and other security protocols [104, 105]. The idea of using brute force or dictionary attacks may, however, not be applicable in graphical authentication schemes. Nonetheless, the appearance of predicable patterns in the use of most graphical authentication schemes makes them also vulnerable to guessing attacks. Graphical implementations such as the passfaces scheme, the passpoints scheme and even the DAS scheme have been found to have predictable patterns that render them susceptible to guessing attacks [106, 107, 108]. This research presents the ideas and implementation of a novel hybrid graphical authentication alternative that efficiently eliminates the problem of predictable patterns and susceptibility to online and offline guessing attacks.

2.8.2 Analysing the Shoulder Surfing Problem

Shoulder surfing is the act of looking over the shoulders of a system user while he/she is in the process of authentication so as to use the information obtained at a later time to gain access to the user’s private resources [13]. This situation can occur typically in an office or busy public places such as shopping malls, bus stations, coffee shops, airports and train stations especially in crowded areas where the attacker places himself in an advantaged position in order to have a good view of the user’s login session to be able to capture his/her required login details [38]. While keying in alphanumeric passwords on a computer system, a typical attacker can observe the user’s keyboard input from a vantage point. The same applies to PIN entries on ATM machines. In a typical graphical password, however, all the attacker needs to do is to observe the screen, and the user’s only defense is to shield the screen during password entry. More complex forms of shoulder surfing include the use of additional devices like binoculars and low power telescopes or video camera to capture or record user login entry. Apart from advising password users to be conscious of the threat and to shield their systems during password entry, little help can be rendered against shoulder surfing in most authentication systems [109]. Many organisations counter the problem of shoulder surfing through the use of ‘two-factor authentication’ in which password entry is complemented with the use of hardware tokens [109] that generate random digits to be used alongside traditional authentication methods. Since only the legitimate user possesses the hardware token, attempts toward shoulder surfing become a futile idea. Other systems incorporate mobile technology [110] with traditional password systems such that One-Time-PINs (OTPs), a set of digits, are sent to the user's phone via the user's registered telephone number, and the OTP is used alongside normal authentication procedures. Shoulder surfing is regarded as one of the greatest concerns of information and computer security researchers since the evolution of text based passwords, it has been researched rigorously [13, 14, 38, 41, 43] and has been the impetus for the development of graphical authentication systems as alternatives to text based passwords [12, 43]. Most graphical authentication systems, however, are still prone to the shoulder surfing attack and this has led to the proliferation of different graphical authentication schemes to curb shoulder surfing as well as the development of various mechanisms to mitigate the shoulder surfing attack. A lot of effort has been put into the search for a promising solution to the shoulder surfing problem over the years, yet truly satisfactory solutions have not been found [38].This is because the search for the solution has opened up other salient issues. One of these is the fact that it is difficult combine security and usability on one system. The quest for more secure systems has rendered systems less usable while the quest for more usable systems has rendered systems less secure. Bridging this gap has continued to elude system security researchers over the years. In this work, the researchers have developed a novel graphical password system that is both able to provide the needed resilience against the shoulder surfing attack as well as bridge the gap between usability and security absent in existing authentication systems.

2.8.3 Description Vulnerabilities and Social Engineering Attacks

Vulnerability to verbal and written descriptions denote the ability of a system user to verbally describe his password to someone else, or to write a description of his password on paper for later use or for the use of another person. The storage of passwords has constituted a serious security issue in the applicability of text based passwords for the following reasons: 1) It renders the password vulnerable to being stolen and used illegally. 2) It provides fertile grounds for social engineering attacks. Social engineering is the act exploiting human factors to persuade or convince a system user to divulge sensitive security information. Social engineering is considered one of the most serious and effective online attacks [111] and has gained significant academic importance [112]. In social engineering, an attacker pretends to be someone that can be trusted by the user such as his employer, or a staff from his bank to maliciously obtain sensitive information. Social engineering is a common threat in online or web applications. People engaged in social engineering technically rely on knowledge of human psychology to exploit human psychological weakness commonly known as *human factors.* One of the most common forms of social engineering attacks on the internet is called *phishing*. Phishing is a situation whereby an attacker uses malicious email or website to pose as a trustworthy organisation. Phishing is a mighty threat on the internet and costs internet users and organisations millions of dollars each year [113]. It is estimated that for the year 2007 alone, the global cost of phishing attacks was about three hundred and twenty million dollars ($320m) [114]. Perpetrators of phishing attacks have consistently used malicious applications to pose as banks and financial institutions and use these applications to demand sensitive details from unsuspecting users [115]. This has continued to pose severe threat to banking applications and institutions. The main problem with phishing attacks, which probably guarantees its success, it that it directly targets the human user, hence it is not hindered by all system security protocols [116]. In a study conducted in [117] to evaluate the trends in global phishing attacks in 2006, the researchers discovered that it was becoming a global issue with up to 31 regions being targeted in up to 16 different languages. Gartner [118] conducted a research survey in 2004 that included about 5,000 adult respondents to determine the trend of phishing attacks on US citizens. Extrapolating from the results, Gartner concluded that about 30 million people were absolutely sure they had been victims of a phishing attack, 27 million believed they had received what "looked like" a phishing attack, 35 million were unsure of an attack, 49 million were sure they had no such experience. Based on the statistics, nearly 11 million adults, which represented about 19% of those attacked had actually clicked on the phishing e-mail, and, more shockingly, about 1.78 million remember providing sensitive personal or financial information to the phishing sites. In fact, the study concluded that U. S. banks and bank card issuers had lost about $1.2 billion in 2003. Gartner acknowledged that phishing attacks were causing a gradual erosion in consumer trust and may slow down U. S. commerce growth by 10% by 2007. Gartner then suggested the use of phishing antidotes which include the use of digitally signed emails and the provision of antiphishing services.

In spite of their seriousness, phishing attacks are not possible if user passwords cannot be described. Hence, [119] suggests that to work against phishing attacks, systems must be developed that take human factors into consideration and be designed to preclude all vulnerability to phishing attacks. Other researchers [120, 121, 122] suggest that since social engineering is a user centered threat, its prevention should include security awareness and alert programs focused directly towards the system users that take into consideration the main security weaknesses that are continuously exploited by the social engineers.

2.9 Combining Usability and Security

Quite significant research effort has been made in recent years in the area of graphical authentication systems. Most of this effort has, however, not been put in the development of novel and more secure and usable systems, or in bridging the gap between usability and security in existing systems, but on trying to make existing systems either more usable or more secure [123, 124]. Some researchers have, however made the effort to look into the security/usability contention and have come up with a number of suggestions.

The Convex Hull Click (CHC) [38] was designed as a remedy against shoulder surfing attacks which are prevalent in grid based models of recognition based graphical authentications schemes. The system worked by the use of small icons from which a user clicks inside an imaginary triangle formed by any three of the user's pass images. The system could allow a user to authenticate even in the presence of onlookers, hence the system greatly improved upon the security of traditional grid based systems. Since the system used many small icons, however, a user had to spend more time to authenticate and this was a usability problem.

In the passfaces scheme [45], a suggested solution to the predictability problem [48,124], was the use of system assigned passwords. This improved the security, but reduced memorability, hence making the system less usable. Another enhancement to the passfaces scheme was proposed by [125] in which alphabetic letters were assigned to each of the passfaces images to allow for the replacement of the mouse with the keyboard. To increase usability, passwords were also composed with face images from separate grids of males and females or clowns and kids [126].

Image categorisation has been suggested in [127] where images are subdivided into groups and users select only the groups containing the images they will like to use to authenticate. A user only has to remember the category to which his chosen images belong and not the images themselves. Although the idea sounds plausible, the system is still not very secure. This is because if an intruder knows the image category selected by a user, he can easily recognise any image presented from that category.

The use of image synonyms was proposed in [128]. Image synonyms are varying images of the same object or class of objects. For example, there are different designs and models of a standing fan, and each can represent an image synonym of that object. Although not the same concept, image categorisation and image synonyms suffer the same problems. Anyone who knows that a user's pass image is a flower will likely select any flower presented to him if it is the only flower within the image set. It will still work, however, for an observer who observes the dimensions of an image during a user's authentication and will only accept the particular image he had observed.

Since graphical authentication is a new and evolving field [129], new models are being developed continuously with the hope of bridging the gap between usability and security. The target is a system that effectively combines usability and security as illustrated in figure 2.18. For now, no single method can claim to have bridged security and usability to a satisfactory level [68]. It is the belief of these researchers that the novel concept of property based authentication presented in this work, being a hybrid scheme, is able to provide the needed balance between usability and security as well as to generate research interests in this direction. With this work, the researchers have tried to approach the implementation of the *ideal authentication system*. According to [21] "An ideal authentication system should provide strong security while maintaining high usability – it should be usable everywhere, by everyone, without the need for any specific training".

Figure 2.18 presents a modified version of the diagram presented in [130] that depicts the tradeoff between usability and security. The diagram shows the tradeoff between usability and security in existing systems such that improving the security aspects of systems often renders the systems unusable, while improving the usability aspects normally renders the systems unsecure. The target is to design and implement systems that are both highly usable and highly secure, which has been the drive of research effort in this field. The target is at some intersection of usability and security where both usability and security are considerably high.

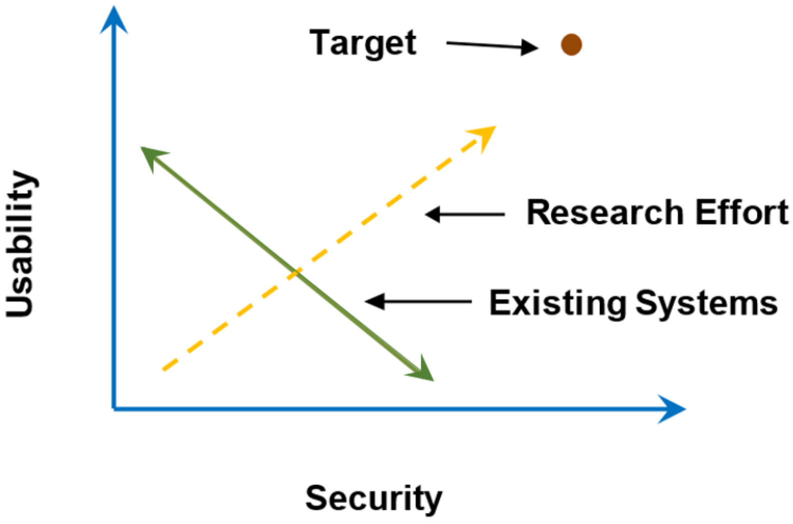


Fig. 2.18: Usability and Security (Modified from [130])

SECTION II – A Closer Look at Some Existing Graphical Models

This section provides an overview of the implementation and analysis of some of the graphical authentication algorithms discussed in the literature. Research in the field of graphical authentication systems has consistently focused on identifying the various usability and security challenges of various implementations through field and lab based experiments using sample user populations. While usability ascertains system strengths and weaknesses in relation to a number of usability metrics which include effectiveness, efficiency and user satisfaction, security has been evaluated through the study of vulnerability parameters such as vulnerability to guessing attacks, vulnerability to shoulder surfing attacks, vulnerability to description, etc. Hence, in this section, some of the most researched graphical authentication models are cross examined on security and usability in the context of existing literature.

2.10 The Passpoints Scheme

The passpoints graphical authentication system is a click based graphical authentication system. The system extended the ideas proposed and developed by Blonder [63] which was the pioneering model in the design and implementation of graphical authentication systems. In this system, a user is presented with an image on the computer screen during registration and is expected to select a number of 'click points' from the image in a definite order as his password. The user is then expected to click on these click points in exactly the same order as he did during registration in order to authenticate. The click points scheme is considered a *cued recall based* system and is one of the most studied graphical authentication systems today [74]. The difference between the new system and the system proposed by Blonder is that this system does not impose any restrictions on click points. The Blonder model provided fixed regions within an image within which a user had to click to select his password. Clicking anywhere outside the regions provided, even though still within the body of the image, is not recognised or recorded by the system. The new model, however, allowed users to click freely from any location within the image to select their passwords.

A study conducted in [68] examined the extent to which tolerance and image choice could affect user performance. Tolerance means the area (in pixels) surrounding a given point selected as password, within which user selection could be accepted as valid. Results of the study revealed that accurate memory of the password was strongly reduced when a small tolerance (10x10 pixels) was used around a user's password points. This happens due to the fact that memory of the precise location of the user's passpoint reduces as time elapses. Hence, from the usability perspective, it is safe to say that increased tolerance meant increased usability for users. In the study on image choice, four images of everyday objects were used. The study revealed few significant differences in user performance between the images used. The study also revealed that many images may support memorability in click based graphical passwords systems.

The performance of the passpoints based system in comparison to other authentication systems has also been studied. In a study conducted in [69], the usability of the passpoints scheme was compared to that of alphanumeric passwords. Study participants were divided into two groups and asked to create and use passwords with passpoints and alphanumeric text over a period of six weeks. Study results indicated that users created their passwords with less difficulty while using graphical passwords. During the practice stage, however, users of the passpoints scheme took longer to login to their systems and made more errors than those with the text based passwords. The two groups performed similarly in terms of memorability in the longitudinal trials, although the graphical system users took more time to login. Although the study results indicate the tendency for improved usability in the use of the passpoints scheme over alphanumeric passwords, this was in contrast to the results that compared the usability of both systems.

The best images suitable for click based passwords and the passpoint selection choices made by users was studied in [131]. The model predicts the probability of the likely click points of users to help predict the entropy of click points in the graphical password formed from a given image. The model also allows the evaluation of the suitability of an image for use in a click based graphical password helping to analyse the possibility of dictionary attacks on the system. In the study, predictions made using the model were compared to the choices made by actual human users. The study revealed that user choices could be modelled and were thus predictable. The study suggests further work along this direction to help improve the security of click based passwords. The study is further corroborated by another study in [124] that investigated the presence of predictable patterns in click based authentication systems. This study further confirmed that user interface design in graphical authentication systems could encourage secure or insecure behaviour among users and that user selected passwords varied considerably in their predictability. The analysis of user selected click points among various image types suggests that click points were predictable. The study also investigated the implementations of the Cued Click Points (CCP) [71] and Persuasive Cued Click Points (PCCP) [132] algorithms and realized that they were indistinguishable from those of a randomly generated simulated dataset. These results indicated that these extended models of the passpoints scheme were less susceptible to guessing attacks than the original model.

Research in [107] studied the effect of multiple password interference on the usability of textual and click based graphical passwords. In this one-hour (short term) laboratory study the researchers aimed at comparing the recall of multiple text based passwords with the recall of multiple click based passwords. The researchers concluded that users of the multiple click based passwords did significantly better than those with text based passwords. The users of the click based passwords made fewer errors than those with text passwords and did not engage in insecure behaviour such as the use of passwords directly related to account names and the use of same passwords across multiple accounts as found in those with text based passwords. After a period of two weeks, the researchers observed that the login success rates were not statistically different for both participant groups, yet the group with the graphical passwords made less recall errors than those with text passwords. The study confirmed that those with multiple click based passwords were less susceptible to password interference in the short term, but had similar usability with text based passwords in other respects.

2.11 The Passfaces scheme

The passfaces scheme is a recognition based graphical authentication scheme developed by real user Inc. [45] and commercialized in the year 2000. The system was developed as a form of two factor authentication to be used alongside traditional text based authentication systems. The system also offers two way authentication composed of user-to-site and site-to-user to mitigate against phishing attacks. While using the passfaces scheme, a system user first goes through the registration phase in which he is asked to select a number of face images from a large image pool. In each subsequent authentication round, he is presented with an image grid containing one of his chosen images and other decoy images. He is expected to recognise and select his pass-image for each step in the order in which he had selected them in the registration phase.

Significant body of research has been conducted on the passfaces scheme. A study reported in [48] compared the performance of the passfaces scheme with that of alphanumeric passwords. The study used 34 students in a three months field trial. The researchers recorded fewer login errors in the passfaces scheme than in the passwords, indicating that the Passfaces scheme had better memorability than the passwords. However, the researchers also reported that the passfaces system took a longer time to execute than the passwords, and hence users of the passfaces scheme took longer times to commence their jobs. This in turn created a motivational problem for users of the passfaces scheme as they logged in to the system less often than those that used the passwords.

The study also reported an earlier study by T. Valentine involving 77 staff and students of Goldsmith’s College to test the memorability of the passfaces scheme. All participants used the passfaces scheme to test 3 conditions. For the first condition, 29 participants were asked to login to the system every working day for a period of 2 weeks. The participants remembered their passwords in 99.98% of logins. The second condition used 29 participants to login after about 7 days of initial enrolment. Most (83%) of the participants were able to login on their first attempt. Everyone was, however, able to login on the third attempt. For the third condition, 19 participants were asked to login once after about 30 days of initial enrolment. In this condition too, 84% of participants were able to login on their first attempt, while all others were able to login by their third attempts. The passfaces scheme is also believed to withstand long term recall as the study participants were asked to login to the systems after more than five months of their last use. While 56 participants were able to participate in the follow up trial, 72% were able to login on their first attempt and 84% by the third attempt. It was also reported that the participants that used the everyday login condition could remember their passwords the best, with 87% remembering the passwords in the first attempt and 100% remembering them in the third attempt.

Researchers in [50] conducted a study to ascertain the susceptibility of images in the passfaces scheme to verbal and written descriptions. The study sought to evaluate approaches by which such vulnerabilities (if they existed) could be reduced as well as to understand if any predictable patterns did exist between how male and female participants described and interpreted the descriptions of facial images. In this study, 45 facial images were obtained from the passfaces website and grouped into three subgroups. The first group contained images that were placed at random, without any consideration. The second group contained images placed together due to visual similarities to a target face image and the third group contained images placed together due to written similarities to a target face image. The study discovered that the study participants did worse in distinguishing a target image where images were grouped based on visual and verbal similarities. The study suggested that the passfaces scheme could be further secured by grouping images due to verbal and written similarities. Subtle differences were also uncovered between male and female groups in relation to how they describe images and how they interpret the descriptions of others.

Researchers in [133] conducted a three week study to compare the usability of passfaces and PINs among older and younger adults. In the study, two test groups of older and younger adults were deployed to use a PIN based system for a time, and then use two face-based graphical authentication systems of young versus old faces. Although, as expected the younger study group performed better in all the authentication systems provided, the older user group did considerably better in recognizing the older faces in the graphical systems. The study suggested that an age-appropriate implementation of the passfaces scheme will yield better usability among different age-related user groups.

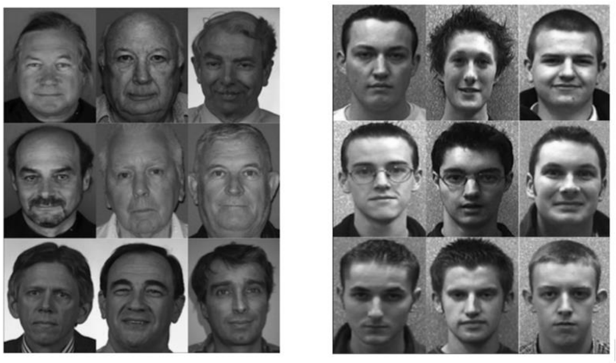


Fig. 2.19: Passfaces scheme: Older vs. Younger Adults [133]

2.12 Abstract Images (Déjà vu)

The déjà vu scheme used abstract images for user authentication and was proposed by Dhamija and Perrig [7]. It is another well researched recognition based graphical authentication system. Déjà vu was proposed to mitigate the issues of text based authentication systems especially in terms of memorability as it is believed that humans have an excellent ability to remember previously seen images. The researchers implemented the déjà vu scheme to conduct a user study that compares it to text based passwords.

In the déjà vu scheme, a user creates his image portfolio by selecting 5 images from a large set of images [38]. To authenticate, the system presents the user with a ‘challenge set’, an image grid, of 25 images, 5 of which are the user’s password images and the rest 20 are *decoy* images (Fig. 2.20). All the user needs to do to authenticate is to locate and click on his 5 pass images. In order to prevent the existence of predictable patterns in image selection, the researchers used Andrej Bauer’s *Random Art* to generate random art images. Given an initial seed, the system generates a mathematical formula which defines the colour value of each pixel in the image plane. The system does not store the images, but uses the stored seed to regenerate the image whenever needed. The researchers chose to use abstract images generated from the seeds to improve the security of the system as users are unable to describe their images to others.

The research findings indicated that 90% of the users were able to successfully authenticate with déjà vu throughout the user study as opposed to 70% for traditional passwords. The researchers outlined potential areas for the application of the déjà vu scheme on PDAs, ATM machines and websites. The main drawback of the system was the need for the server to store the seed for each of the images that form the user portfolio.

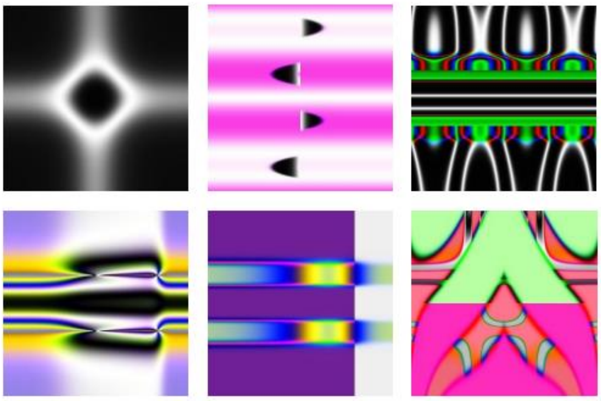


Fig. 2.20: Random Art Images for Déjà vu [7]

As reported in [38], a comparative evaluation was carried out between déjà vu, six character alphanumeric password and four digit PINs to compare the usability of each of these schemes. After initial training in password selection and the authentication procedure, participants using the déjà vu scheme using pictures and abstract images were all able to login successfully, while users of the alphanumeric passwords and PINs both realized 5% failure rates. In a follow-up trial a week later, déjà vu users with pictures and abstract images realized 5% and 10% failure rates respectively, while the users of PINs and alphanumeric text realized 30% and 35% failure rates respectively. In spite of the advantage in memorability, déjà vu had a relatively lower efficiency as it took approximate 30 seconds to login.

2.13 Conclusion

This chapter has done a considerable review of available literature on the design, implementation and research trends in graphical authentication. The chapter has also provided insight into existing security concerns brought about by either system design or user behaviour. It is important to note that from the facts presented in current literature, although some systems have done considerably better than others in terms of both security and usability, no existing system is devoid of either security or usability issues that need to be addressed.

The next chapter presents the ideas, concepts and principles that have evolved in the study and evaluation of property based authentication systems in the course of this research. The chapter serves as a platform to better understand the underlying concepts that serve as the building blocks of property based authentication systems. The chapter also helps to better understand the necessity for the numerous evaluations conducted as part of this research work.

Chapter Three – A Conceptual Model for PBASs

3.1 Introduction – Property Based Authentication

This research introduces a novel concept in Graphical Authentication Systems (GAS) developed in the course of this research work, which the researcher has named "**Property Based Authentication" (PBA).** It is the idea of using information *in* or *about* an image or a set of images as the *base* for user authentication. In existing recognition based graphical authentication techniques, users are asked to select specific images from large image sets during registration, and to identify and select *the same* images they had previously selected from among many other decoy images each time they want to authenticate. In property based authentication, however, a user is asked to choose from one or more *properties* (or characteristics) associated with each of a given set of images and then to select a *variant* (or option) from a list of variants assigned to each of the properties and to recall and recognise each of his chosen properties and their corresponding variants each time he wants to authenticate. Hence, the properties are actually *characteristics* or *contents* of an image from which the image can be identified. The user is made to choose the properties and their variants in the registration phase and is expected to recognise and select the images that possess the chosen properties and variants in the authentication phase. Here, the *base* of *factor* for authentication is a *quality* which determines which image actually *qualifies* as an authenticator within an image set.

From all literature studied as part of this work, the concept of authentication by image characteristics or features has not been uncovered in authentication systems research and looking in this direction provides newer options for consideration in the design, usability and security potentials of graphical authentication systems. Five basic schemes (implementations) of this system have been identified and are discussed in detail in subsequent sections. Property based authentication is basically a merger (hybrid) of the concepts of recognition and recall in one system. One may presume that in this system, as in cued recall based systems, the image itself serves as a *cue* and helps a user to remember the properties he had chosen as his password and their corresponding variants. This assumption, however, is open to investigation. Although other cued recall based systems have been implemented that merge the potentials of recognition and recall, this systems provides this advantage in a grid based format.

The contents of this chapter are the researcher's own ideas of the meaning, concepts and principles in property based authentication that have evolved in the course of this research and are among the contributions to existing knowledge presented by this project. Some of the ideas presented have been evaluated through experimentation while others are left for future work. None of the contents of the chapter was obtained from another source. The chapter is organised to help in understanding the concepts and contents of the property based graphical authentication paradigm.

3.2 A Simplistic Example

The basic idea of **Property Based Authentication** is the use of certain *characteristics* of an image as the means of user authentication in the basic form of a recognition based graphical authentication system. As this idea has not been considered in earlier studies, some novel concepts have been introduced in the course of the work, some of which have been well discussed and sometimes investigated in course of the research. In understanding the basic idea of property based authentication, it is essential to understand how properties are assigned among similar images and how the associated variants are related to these properties.

To provide a simplistic example, consider the image in fig. 3.1, which could be referred to as image x. Image x is one member of a given set of images that share similar features (properties), each of the properties is also associated with a number of variants. Images in the same implementation have the same number of properties with variants associated with each property. No two images have exactly the same variant for each of the properties. That is, each image is unique. Let us consider image x, the image has four main features (or properties): i) a background ii) a shape iii) an outline for the shape and iv) a colour (or fill) for the shape. These are the basic properties or features of the image. Each of these properties is further subdivided into variants and these are the various colours, patterns or forms associated with each property. They include: i) image background colour, ii) image shape, iii) shape outline colour, and iv) shape fill colour. Suppose five shapes variants are associated with the 'image shape' property, such as star, circle, square, triangle and hexagon and six colour-based variants associated to the colour based properties, such as black, white, blue, red, green and yellow. Each image in the collection will comprise of each of these properties and a variant for each of the properties. From mere observation, one can see that the image has three *regions*, and a shape. The regions are designated as the authentication properties and the 'image shape' as a mere distractor property. In the process of authentication, a user only considers the image properties and variants he had selected for his password and selects any image that fits his chosen property/variant combination. This example illustrates a typical fill based (colour) model.

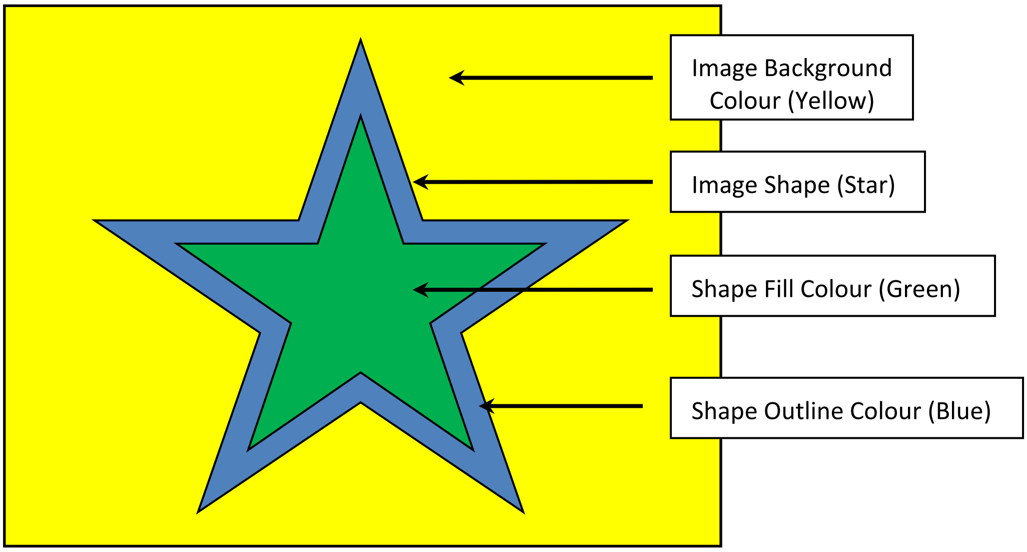


Image Background Colour (Yellow)
Image Shape (Star)
Shape Fill Colour (Green)
Shape Outline Colour (Blue)

Fig 3.1: Image from a simple model with four properties.

3.3 Presentation of the Grid

A typical grid in this simplistic implementation is represented by figure 3.2. The various properties in each image are represented by variants from among those provided for the system. Each image is obtained by the various permutations of the properties and their corresponding variants. A system user only needs to identify an image that contains his chosen variant for the property with which he had chosen to authenticate. Suppose a random user decides to use the *shape outline* (property) as part of his authentication choice and selects the *yellow* (variant) as his specific authenticator, this user then has a "*yellow shape outline*" as his password element for that particular step in each authentication round. Suppose in a particular login phase the user is presented with the grid in fig. 3.2, the only image in the grid that *satisfies* the "yellow shape outline" *condition* is the image in the second row and second column, and is the only one that can authenticate the user.

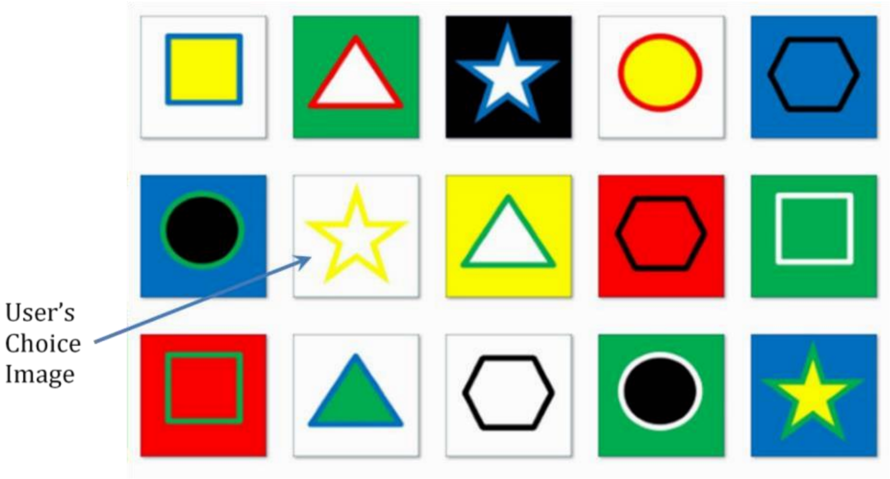


Fig. 3.2: Basic property based grid (1st login)

If the same user is again presented with the image in figure 3.3 in the same step of the *next* login session, the only image in the grid that *satisfies* the "yellow shape outline" *condition* is the image in the second row and fourth column. It is the only image that can authenticate the user. This particular model has been implemented and investigated in this research and is named the *basic shape model*. Of course, the user may not have chosen the image outline, he may have chosen the ‘image background’ or the ‘image fill’ as his chosen properties. All he needs to do to authenticate is to remember the part (property) of the image and the colour (variant) he had selected for that property in order to authenticate.

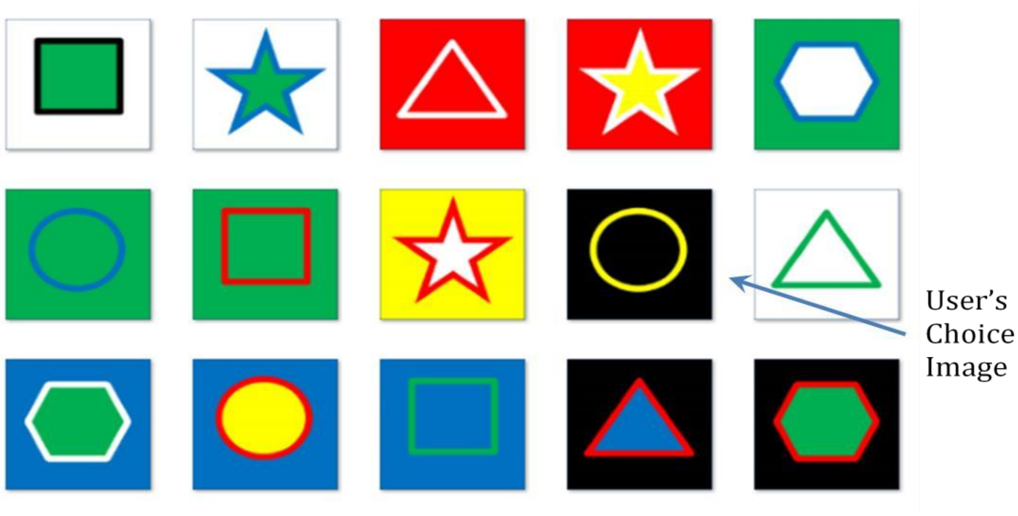


Fig. 3.3: Basic property based grid (2nd login)

3.4 Classification of Property Based Schemes

In the course of this work, several distinct ways in which the property based system of authentication could be implemented have been identified. These distinct implementations are referred to as *schemes*. Each scheme utilises an entirely different approach to the idea of Property Based Authentication. Individual implementations within a scheme are called *models*. Models from each of these five schemes have been developed and evaluated in the course of this work. The various schemes are depicted in fig. 3.4. They include the following:

1. **Fill Based Scheme:** This scheme consists of models in which the properties associated with images are determined by colours, patterns, or other fill types. Within this scheme the researcher has identified and implemented two classes of models, *colour based* and the *pattern based* models. Two colour based models have been implemented, a *basic shapes model* and a *butterfly model*. The scheme has also been used to implement the concept of ‘model mixing’. Thus a *mixed model* of patterns and colours has also been implemented and evaluated. Mixing is discussed in the next section.

2. **Number Based Scheme:** The number based scheme consists of models in which the properties associated with images are determined by numeric values. Two classes of this scheme have been identified and implemented, a *digit based* and a *number representation based* model. Properties in the digit based model are represented by numeric digits, while properties in the representation based model are represented by the physical representations of numeric values.

3. **Text Based Scheme:** The text based scheme consists of models in which the properties associated with images are determined by alphanumeric text and symbols. Two classes of this scheme have been identified, implemented and evaluated in this work. In the *character based model*, authentication is determined by the use of alphanumeric characters and symbols, while in the *word based model*, authentication is the determined by the relative positions of alphabetic letters within English words. A word based model may and may not include pictures that depict the images the words represent.

4. **Magnitude Based Scheme:** The magnitude based scheme consists of models in which the properties associated with images are determined by the relative sizes of objects within the images. A model implemented and evaluated in this scheme for this work is named *broken tiles.*

5. **Form Based Scheme:** The form based scheme consists of models in which image properties are based upon the visual appearances of objects within an image. Typical of form based models is the use of shape, posture, etc. The form based model implemented and evaluated as part of this work was named *animal farm*, a screenshot of which is presented in figure 4.17.

Terminology

- The term “fill-based” may also be used to apply to other models that are complemented with a fill based element.

- The term “position based” may be used to refer to any model associated with the spatial positions of left, right, top, down, center, etc., or the ordinal positions of 1st, 2nd, 3rd, etc.

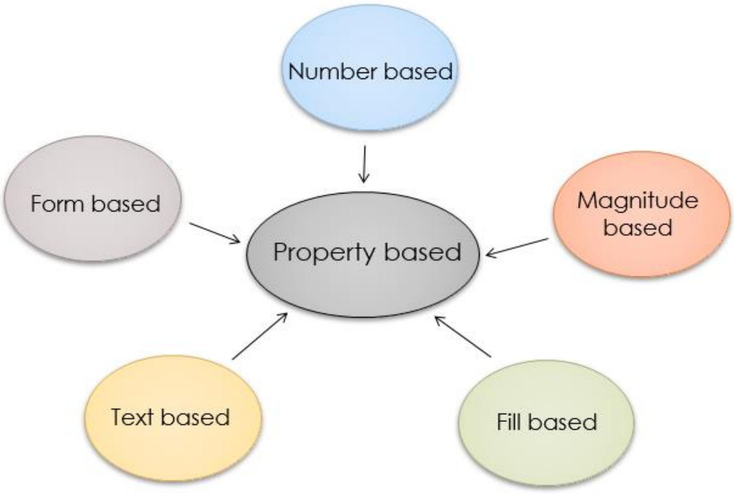


Fig. 3.4: Classification of Property Based Models

3.5 Mixing of Models

Mixing is the combination of two or more models especially within the same scheme to form a new authentication model. Two types of mixing have been identified. If the different models are independently placed between successive steps of a single authentication model, it is referred to as *stepwise mixing*, and if images from two or more models are mixed within the image grid of a new authentication system, it is referred to as *gridwise mixing*. Screenshot from a mixed model implemented and evaluated in this work is presented in figure 3.5. This is an example of gridwise mixing obtained from combining images from a colour based and pattern based models of the fill based scheme, both models have been implemented in this work. Image layout and authentication *factor* are important considerations in the design of mixed models.

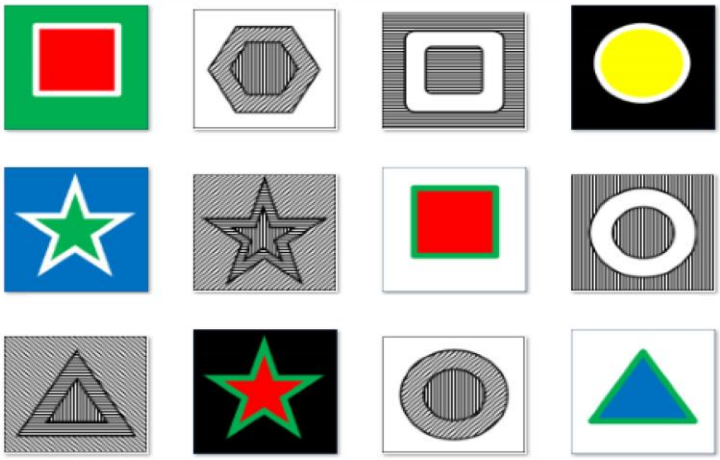


Fig. 3.5: Grid of a mixed model of colours and patterns.

3.6 Cardinality and Fragmentation in Fill Based Models

It is assumed that there are possible ways to make images appear complex to an attacker even though they are simple for a user to understand and use. One of these methods is by increasing the physical complexity of the image set. In doing this, any of two methods can be adopted. The first method is implemented in software. In this method, the properties of an image are divided into distinct sets, and during a user's registration he is made to select which set of properties he will use to authenticate himself onto the system. The numerical value that defines the number of distinct properties in an image that are deployed for authentication in such models is referred to as the *cardinality* of the image. The *pick value* is the number of properties in the image set from which the user selects his chosen password. Hence the term *redundancy* is used to denote the image cardinality minus the pick value. The relative cardinalities of images in a fill based model are depicted in figure 3.6. The second method of introducing complexity is done in the design of the image set, and one of the methods that may be employed is the use of *image fragmentation*.

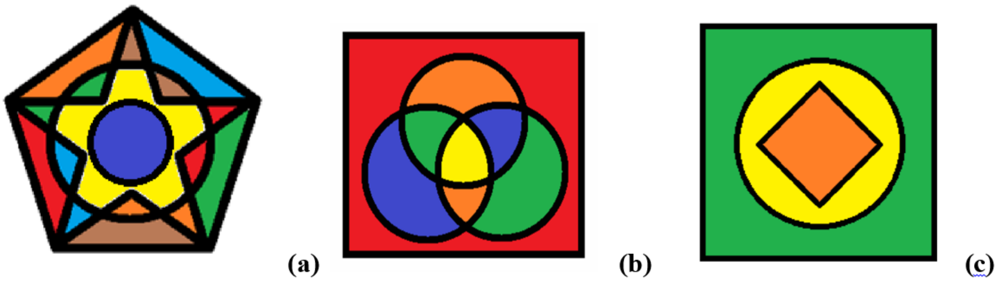


Fig. 3.6: Image cardinality; (a) High (b) Medium and (c) Low

Image fragmentation is considered as the art of breaking down the *layers* or *levels* of a position based concentric model into smaller *fragments*. This process helps to increase both the cardinality and complexity of an image. Position based models may present an image as *fragmented*, *centralised* or *mixed*. Different fragments on the same level can be designated as different properties and assigned different variants. A *centralised* or *concentric* image has its objects (properties) arranged in concentric circular order, while a *mixed* image comprises both concentric and fragmented components as illustrated in figure 3.7.

Position based models can also be identified by the *orientation* (arrangement) of their properties. Apart from the *concentric* models already mentioned, a *vertical* orientation means that the properties are arranged using the top, centre and bottom orientation, a *horizontal* orientation means that the properties are arranged using the left, right and center orientation, a *cross-radial* orientation means they are arranged using the top, bottom, left, right and center orientation, and *X-radial* orientation means they are arranged using the top left, top right, bottom left, bottom right and center orientation.

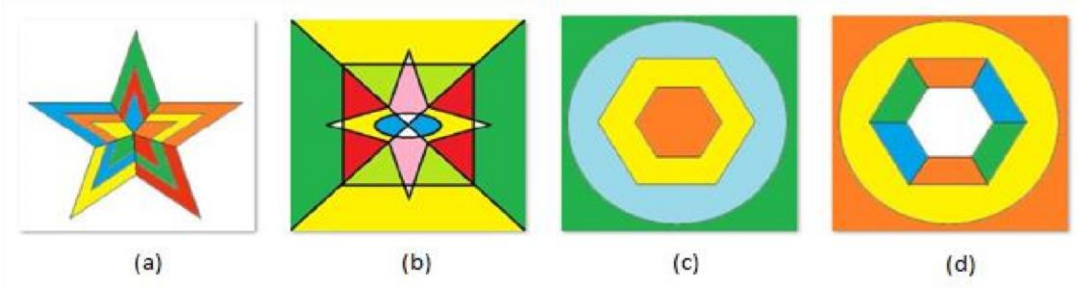


Fig. 3.7: Image fragmentation: (a) partly fragmented (b) fully fragmented (c) non-fragmented (d) mixed

3.7 Integrated Models

An *integrated model* is a model whose images are designed such that the system can successfully operate as a model in more than one scheme. During the registration, the system user selects which of the separate schemes he wishes to use for authentication and then proceeds to select the properties and variants associated that scheme. Images from a sample integrated model have been depicted in figure 3.8. It illustrates a model that may function either as a fill based or a number based model.

Blending, however, is the act of designing a model in a particular scheme such that it can function as more than one distinct model in the same scheme such that a user selects which model to use for registration and authentication.

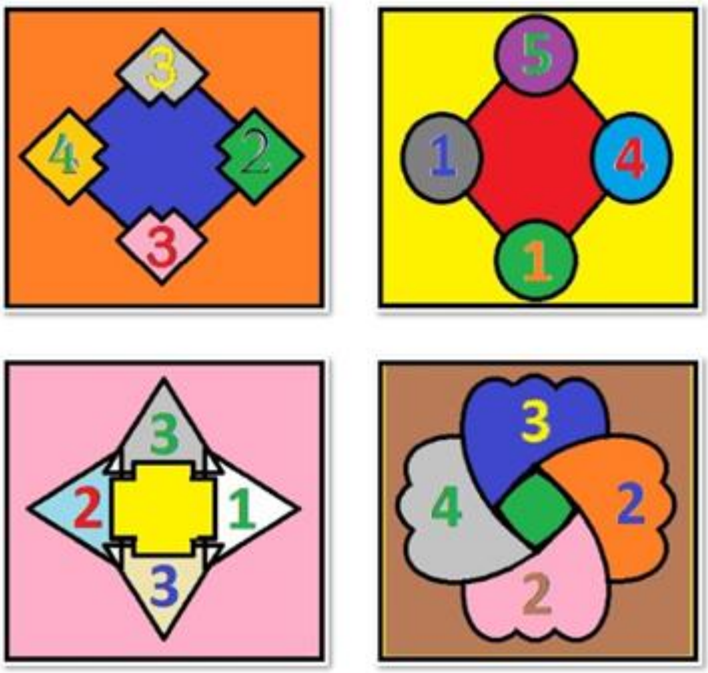


Fig. 3.8: An Integrated Model

The ideas of image cardinality, fragmentation, orientation and model integration are concepts that had gradually evolved and developed in the course of this work. They were borne out of the need for better understanding of the ideas presented herein as well as to improve upon the usability and security of the novel systems presented in this work. Actual investigations into the viabilities of these concepts has been left as part of the future dimensions of this work.

3.8 Multiplicity of Design Options

For every property based scheme, many models could be implemented. The limit depends only on the potentiality and prowess of the designer. In the fill based scheme, for example, there is the potentiality to develop many colour based models. Figures 3.9 and 3.10 depict two models that were suggested for implementation and evaluation, a butterfly model and a flower based model. Only the butterfly model has, however has been implemented and evaluated in this work.

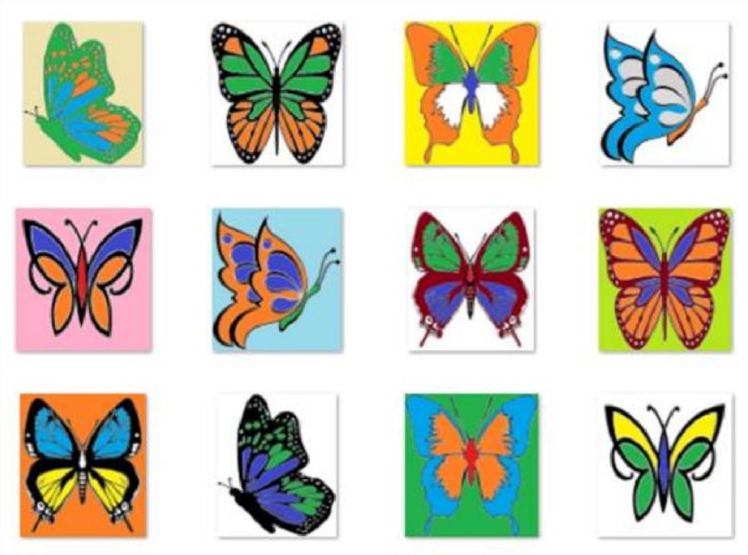


Fig 3.9: Fill Based Scheme - Sample butterfly model

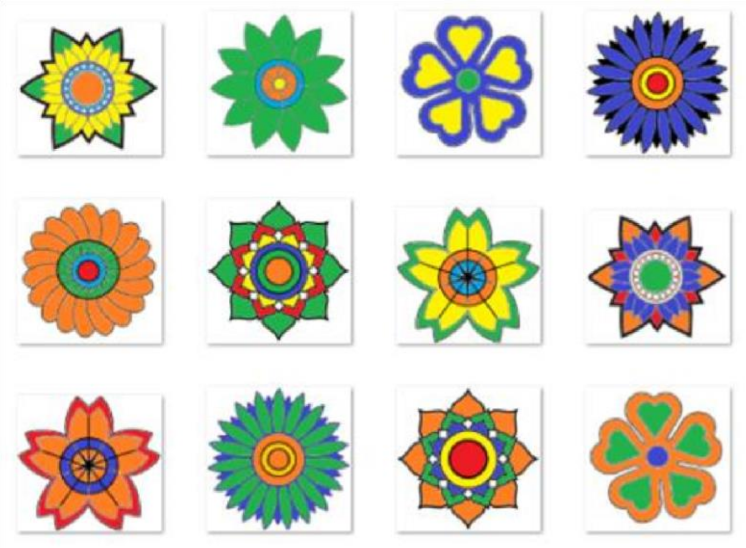


Fig. 3.10: Fill Based Scheme - Sample flower model

3.9 Order in the Magnitude Based Scheme:

In each scheme, the base for authentication is the main item (such as colour) with which user authentication is dependent. In magnitude based schemes, the base for authentication is the relative magnitude of objects (properties) within each image. A magnitude model is referred to as *ordered* if the properties in each image of the model are arranged sequentially in order of magnitude, and *unordered* if no sequential arrangement of this nature is implemented in the system. An example of ordered and unordered grids in a magnitude based system are presented in figure 3.11. It is believed that the concept of ordering could significantly make user authentication easier and faster as the number of image properties in a magnitude based system increase.

> *The impact of magnitude based ordering on user performance is one of the concepts that have been evaluated in the usability experiments as part of this project.*

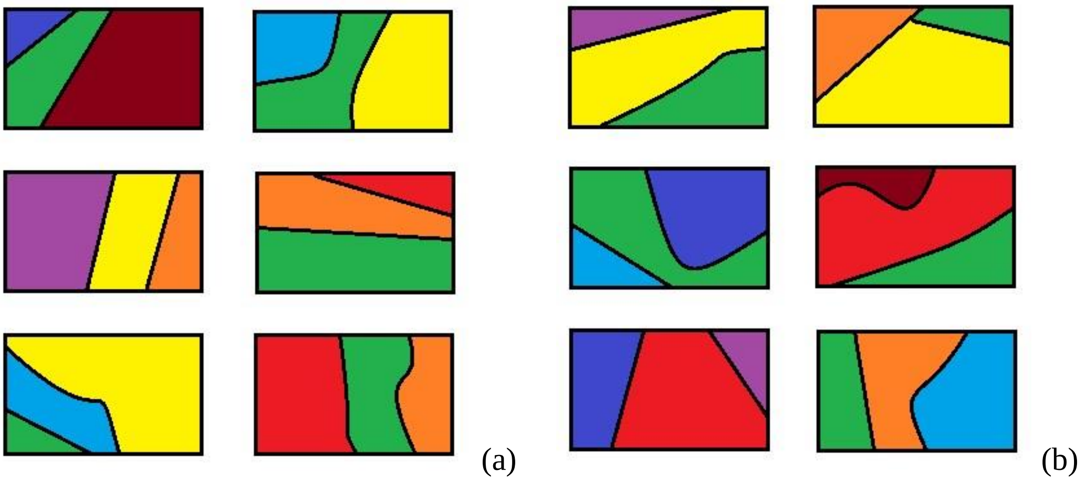


Fig 3.11: Magnitude based model: (a) Ordered (b) Unordered

3.10 Extensions to the Property Based Methods

Multifactor and multi-dimensional authentication have been suggested and studied in [134, 135, 136] in which a user incorporates various methods in order to authenticate onto a computing system. Such methods include the combination of graphical or text input with the use of hand held devices or tokens. This provides improved security over the use of a single authentication method (or factor). The main problem with this approach is the need to carry additional devices. In [137] sound signatures have also been suggested to complement graphical password schemes.

In this work, however, a number of extensions to the property based concept have been proposed. Since these extensions are intended to combine multiple implementations of graphical authentication systems, it would be more convenient to consider them as *multi-scheme*, rather than multifactor systems. In this study, two sets of extensions have been proposed for the property based authentication system. The first set is referred to as the *net based model* (figure 3.12). In this model, a user uses both a simple property based system and a numeric PIN. Numeric PIN values are allocated within a seemingly empty grid called a *net* and the actual positions of these digits within the net are determined by a *'key'* located below the empty net. First, the user needs to identify and select his property-based image in the normal way done in all property based schemes. In the second stage, the user clicks on the positions of his chosen PIN in the net.

The way and manner the digits are chosen and entered depends on the implementation of the model. The empty squares are numbered zero to nine and the spatial positions of these numbers are presented by a small numbered rectangle at the bottom of the net. This numbered rectangle is called the key. The key directs the user to the various locations of his chosen digits. Three versions of the net based system could be developed; drag based, click based and keyboard based.

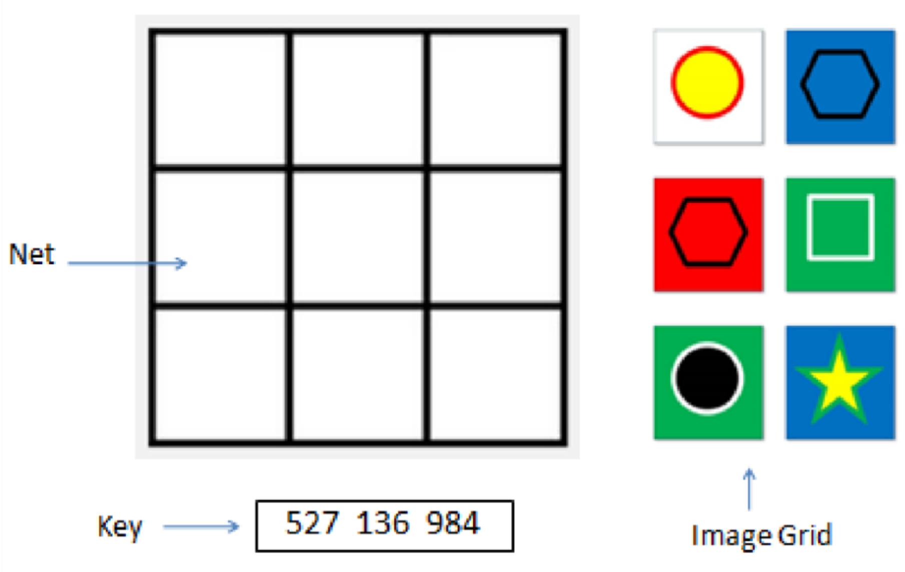


Fig. 3.12: System Enhancements: Sample net based model

The second extension is referred to as the *directional model* and also starts with the user locating his property based image in a normal way from an image grid. He then drags the image in a predefined direction. The drag direction is determined by four variously coloured arrows pointing in opposite directions that appear when the user touches his image. The user's drag direction is determined by the colour (or other factor) he had chosen for his arrow during registration (figure 3.13). The relative positions of the arrows is interchanged between sessions, such that the user's drag direction is not fixed.

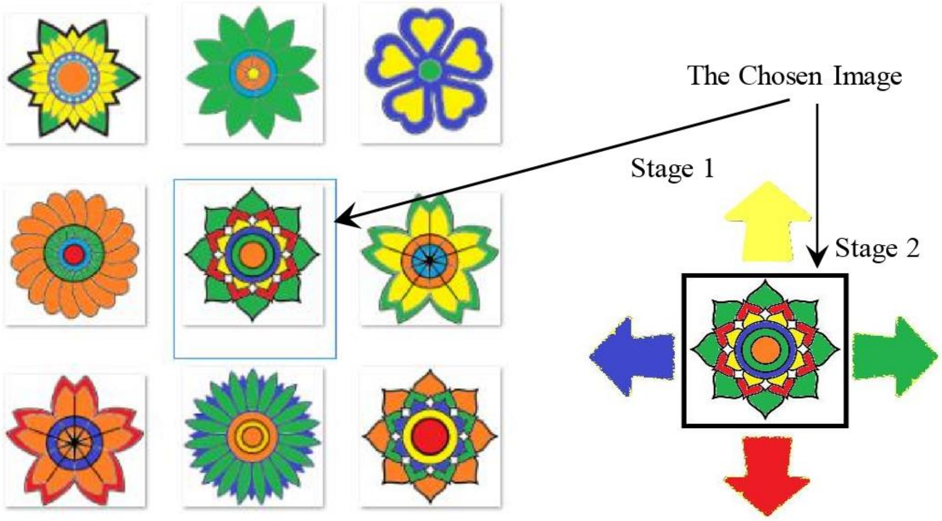


Fig. 3.13: System Enhancements: Sample directional model

3.11 Assistive and Organised Image Selection

Although a variation of choices across sessions in a multi-step model may be preferable for security reasons, the presence of a recall based component in every implementation may hinder memorability. Hence, the idea of *assistive or organised image selection* is introduced as a better option. It is the idea of having predefined selections in a predefined order in a position based system to support memorability. It comes in several flavours:

Stagnating: This is the use of the same variant in the same position (property) consistently across consecutive steps of authentication in a multistep property based model.

Inward Painting: This is the systematic use of the same image variant (fill) across successive levels of a concentric position based model across successive steps of a fill based model starting from the outermost levels.

Outward Painting: : This is the systematic use of the same image variant (fill) across successive levels of a concentric position based model across successive steps of a fill based model starting from the centre of the image formation.

Navigating: This is the use of the same variant across adjacent positions across consecutive steps in a multistep non-concentric position based model.

Hopping: This is the use of the same variant in a particular position for a fixed number of consecutive steps in a position based model, and then moving the variant to a new position and using it in the new position for another set of authentication steps.

Standard Spelling: This is the spelling of a particular English word in a fixed position along the successive steps of a word based model.

Ordinal Spelling: This is the spelling of a particular English word along successive steps of a word based model such that each letter is chosen at its natural position.

Fixed Lettering: This is the fixing of a particular letter of the alphabet in a fixed position along successive steps of a word based model.

Ordinal Lettering: This is the movement of a particular alphabet letter along successive steps of a word based model such that the letter moves inwards along ordinal positions in words.

Ordered Lettering: This is the use of successive letters of the alphabet in a fixed position along successive steps of a word based model.

Counting: This is the use of successive numbers in a fixed position of number based model.

> *The effects of assistive and organised image selection on user performance is one of the concepts evaluated as part of this research project. The concept was evaluated for the colour based and word based models in experiments 7 and 8 of the usability tests conducted as part of chapter 5.*

3.12 Conclusion

This chapter provides an overview of the basic concepts and ideas with regards to the development and implementation of property based authentication systems as they have evolved in course of this research. Some of the ideas outlined in the chapter have not been evaluated, while others have been implemented, evaluated and reported within the thesis. Those concepts that have not been evaluated are left as part of the future direction of this research work. Even among the ideas that have been evaluated, as is the culture of academic research, there are many potentials for expansion, enhancement and more elaborate studies. The idea of property based authentication is a spark that has just been ignited. Hopefully, when the idea is put forward to the research community other concepts and ideas are sure to come to light. Hence there is much optimism in the development of this concept into a stronger and more viable research field.

As stated previously, twelve prototypes of the property based paradigm have been implemented and evaluated. The next chapter discusses the implementations of the system prototypes presented in this research work. The chapter focuses on the details of how properties have been assigned, and how registration and authentication are conducted in each of the developed systems.

Chapter Four – Operational Procedure for PBASs

4.1 Introduction

This chapter contains details of the operational procedures for the main prototypes developed as part of this research project. In all, twelve prototypes of the property based implementation have been developed as part of this work. Two of the prototypes, however, have not been included in the presentations in this chapter. The two prototypes are the ordered and unordered implementations of the magnitude based model that were developed to evaluate the effects of magnitude based ordering on user performance. The reason why screenshots from the systems have not been included is due to their similarity in application and design with the standard magnitude based model which has been presented as part of this chapter.

4.2 Operational Procedures for Experimental Prototypes

This section provides a glimpse into the general operational procedures for property based systems as well as the specific implementation of each of the models. Throughout this section, actual screen shots from each of the models has been captured and utilised for demonstration. Five schemes of the property based authentication systems methodology have been identified, and in these schemes, twelve (12) prototypes have been developed as an implementation of various models for the evaluation of a number of significant security and usability parameters in the determination of the capabilities of the property based graphical implementation. Throughout the course of this work, for ease of understanding, except for the word based model, only three properties are provided for each model. Also, except for experimental purposes, a grid size of 9 has been used for all the usability and security experiments.

4.3 Registration and Authentication

In all software implementations for this research work, the first window displayed when a user runs the program is the user login window (fig. 4.1). From this window, a new user signs up (or registers) to use the system, while an existing user signs in (or logs in) to the system using an already existing user name.

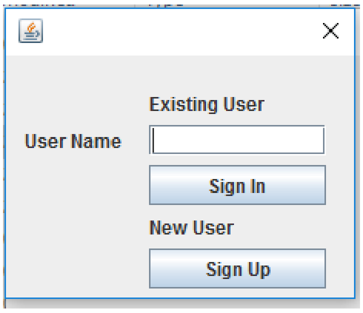
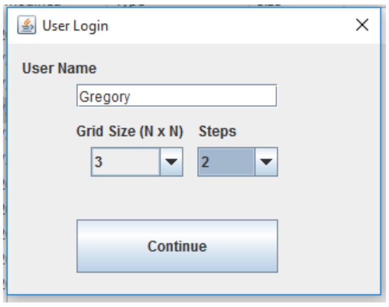


Fig. 4.2: Login window

For a new user, clicking on the 'Sign Up' button in the login window on figure 4.2 takes him to the grid and steps selection window (fig. 4.3), in which the user will enter a selected user name, select his preferred grid size and number of authentication steps from two drop down menus. The digit selected for the grid size (fig. 4.3) denotes N of an (NXN) matrix which indicates the number of images to be displayed in the image grid during each authentication round. The digit selected in the 'steps' drop down menu (fig. 4.3) indicates the number of authentication steps (i.e., the number of image grids to be displayed) to complete each authentication round for that user.


User Login

User Name: Gregory

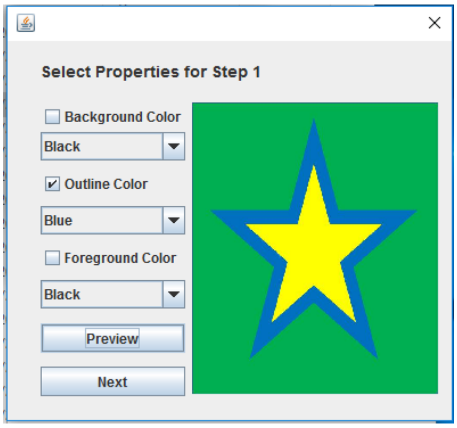
Grid Size (N x N): 3

Steps: 2

Fig. 4.3: Username, grid and steps selection window for new users.

4.3.1 The Colour Based Model

The basic shapes colour model is one of the members of the 'fill based scheme' developed in the conduct of this project. The fill based scheme is comprised of models in which fill types or elements (colours, patterns, gradients, etc.) are used as image properties to distinguish different sections of an image. In this implementation of the colour based model, after selecting the required grid size and number of steps for his login, as depicted in figure 4.3, the user clicks on the 'continue' button to go to the image properties window where he selects the properties he intends to use for each of his authentication steps. The user first selects the required properties for the first step and then clicks on the 'next' button to open the window for image properties selection for the second step and so on.



Select Properties for Step 1

□ Background Color

Black

☑ Outline Color

Blue

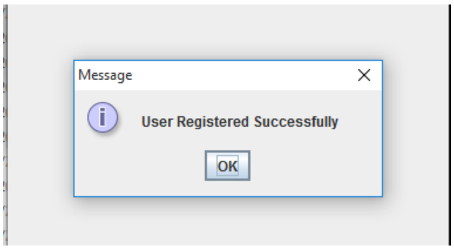
□ Foreground Color

Black

Fig. 4.4: image properties selection window (basic shapes colour)

Each image properties window has check boxes representing each of the properties provided by the authentication system (fig. 4.4). The properties for this system are: image background, image shape outline and image foreground (shape fill). The variants are the various colours to be chosen for each of these properties. Each property has a drop down menu with the list of variants for that property (fig. 4.4). The dropdown list of variants in this model shows the colours: black, white, blue, red, green and yellow for each of the properties used in the authentication model. The user first has to check the checkbox for each of the properties he intends to use for his password in the authentication step and then choose a variant of that property from the dropdown list of variants. The user may check any number of properties for his/her image in each step and select a variant for each property. For this work, the variants of adjacent properties cannot, however, be the same. If a user checks the checkbox for a given property but does not select a variant, the system assumes the default variant, which is 'black' in this model.

When the user completes the properties and variants selection consecutively for the desired number of steps and while in the properties and variants selection window for the last step, clicking on the 'next' button displays the message 'user registered successfully' as displayed in figure 4.5



Message

User Registered Successfully

Fig. 4.5: Registration success message

For demonstration, suppose the user here chose a blue outline colour as the property for his pass image in any of the authentication steps (as depicted in figure 4.4), he only needs to locate and select the image with a blue outline colour for his authentication in that step. The 'preview' button provides an image preview from one of the images that satisfies his pass condition (property choice).

On closing the successful registration message box displayed in figure 4.5, the user is returned to the login window (Figure 4.2) where he can now authenticate as an existing user. The user enters his chosen username and clicks on the 'sign in' button. He is the presented with the authentication grid for the first step (as displayed on figure 4.6)

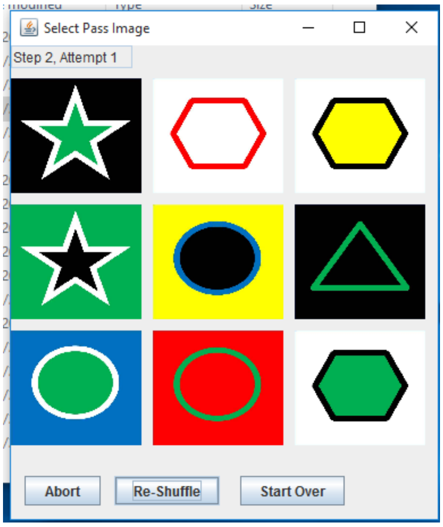
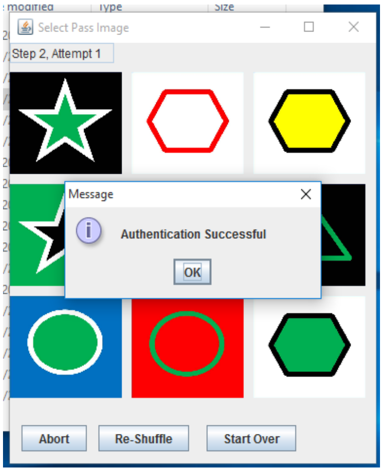


Fig. 4.6: Image selection grid for step 1 (basic shapes colour)

The authentication grid is a grid of size NxN depending on the grid size the user had selected in the registration phase. From the authentication grid, the user is expected to locate and click on the image containing the set of properties and variants (colours) he had selected in the registration phase. From the selection in figure 4.4, for this demonstration, the image the user needs to select for this step will need to have a 'blue outline colour'. The only image that fits this appearance from the images in figure 4.6 is the image of a circle with a black fill colour, blue outline colour and yellow background colour. On selecting this image, the user receives the massage 'Authentication Successful' (figure 4.7) if this is his last authentication step, else the system automatically displays a new image grid for the selection of the image for the next authentication step.

One can observe that the image selection window also contains the step and attempt numbers displayed on the top left hand corner of the window. These are important and are there to inform the user of the exact authentication step he is on and the number of attempts he has made to authenticate. In a typical implementation, the system suspends the user's account after three authentication attempts, to save the system from unauthorised access.

Three buttons are displayed on the lower side of each image selection window. The first button is the 'abort' button which allows the user to cancel the authentication process and return to the login window to re-enter his username and start the authentication afresh. The next button is the 'Reshuffle' button which allows the user to obtain a new image grid for that particular step. This is especially helpful when a user fails to identify the image with which to authenticate for that step. Ideally, the number of possible reshuffles per step is limited to one or two in each step. The last button is the 'start over' button. This button takes the user to the start of the authentication process. It allows him to start over the authentication with his current credentials by presenting him with the image grid for the first step of the authentication process and it allows him to start again from the first step. Unlike the 'abort' button that forces a user to re-enter his username, the 'start over' button allows him to start the authentication process from the first step. The essence of 'start over' button is to allow a user that remembers that he had been entering the wrong password go back and correct himself. The system does not regard a start over as a valid authentication since it has not been completed. However, since the system does not provide any clues to indicate that the user is on the right or wrong path to authentication, the button is not seen to pose any security risks.



Select Pass Image

Step 2, Attempt 1

Message

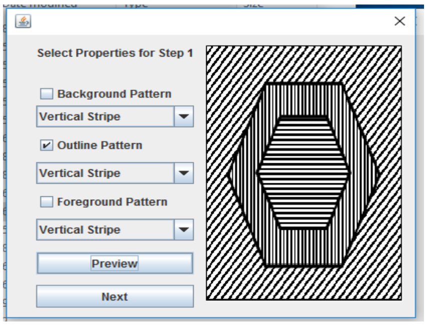
Authentication Successful

Fig. 4.7: Successful Authentication

4.3.2 The Pattern Based Model

The pattern based model is similar to the colour based model of the fill based scheme. The only difference is that in pattern based images, patterns are used in place of the colours used in the colour based scheme. The idea for a pattern based model was proposed out of the need to create fill-based models for people with visual difficulties (eyesight problems), most especially those with colour blindness or similar eyesight defects.

All registration procedure in the basic shapes pattern model is exactly the same as that demonstrated in the basic shapes colour model. The properties and variants selection for the pattern model is demonstrated in figure 4.8. The layout of the window is also the same as that presented in the colour based model and the properties are also similar. The properties are: Background pattern, outline pattern and foreground pattern. The variants for each of these properties are vertical stripes, horizontal stripes, slanting stripes and so on.



Select Properties for Step 1

□ Background Pattern
Vertical Stripe

☑ Outline Pattern
Vertical Stripe

□ Foreground Pattern
Vertical Stripe

Fig. 4.8: Image properties selection and preview (basic shapes pattern)

As in the registration phase, authentication in the basic shapes pattern model is similar to that of the basic shapes colour model. For each authentication step, the system user is presented with an image grid from which to select the image that matches the patterns for properties he had selected in the registration phase. Suppose the choice demonstrated in figure 4.8 represents the user's chosen image for a given authentication step. When later presented with the image in figure 4.9 during authentication, the user needs to identify the image that satisfies his chosen properties and variants in the registration phase, which is the 'vertical stripes outline pattern'. The only image within the grid that satisfies this condition is the image in the 3rd row and 2nd column. On selecting this image, the user either authenticates or is presented with the grid for the next authentication step.

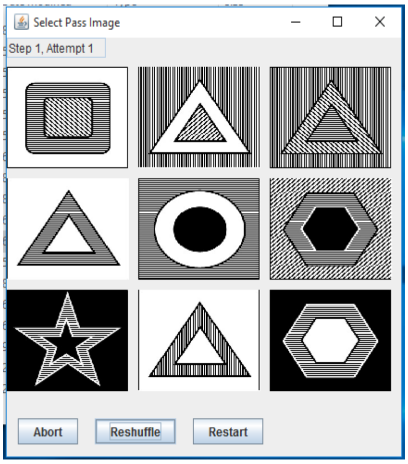
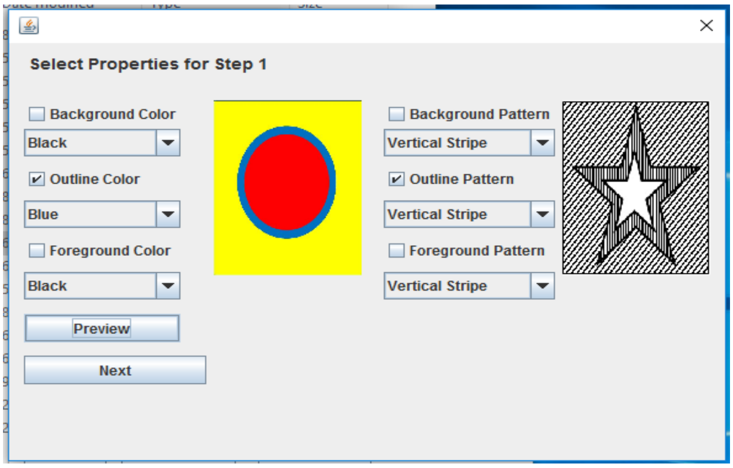


Fig. 4.9: Image selection grid for the pattern model.

4.3.3 The Mixed (Colour-Pattern) Model

Mixing is the process by which images from two or more authentication schemes or models are combined to produce a new model. In property based systems, mixing is of two types: step-wise mixing is the combination of images from independent models to form image grids of new models, each original model, however, occupies its own grid, while grid-wise mixing is the use of images from different models to form the various authentication grids of a new model. The type implemented in this work is the grid-wise mixing. For the mixed model, images from the researcher's colour and pattern models are combined into a single image set.

The mixed model presented in the course of this work utilises the 'OR' operator, that is, at each authentication step, the system presents the user with a grid containing pass images from either the colour or the pattern based models. In the registration phase, the user is presented with a properties and variants selection window for the selection of properties and variants for both of the models. The user *must* choose a property and corresponding variant for each of the models being mixed.



Select Properties for Step 1

□ Background Color
Black

☑ Outline Color
Blue

□ Foreground Color
Black

□ Background Pattern
Vertical Stripe

☑ Outline Pattern
Vertical Stripe

□ Foreground Pattern
Vertical Stripe

Fig. 4.10: Properties and variants selection window for the mixed model

In any of the authentication rounds that follow the registration and for each of the user's authentication steps, the user authenticates by identifying either of the images for the pattern or colour models, whose properties he had selected for that step in the registration process. As with other implementations, the user needs to ensure that he checks the checkboxes for the properties he intends to use in each of his authentication steps for each of the models. The 'preview' button, helps the user with a preview of the properties and variants he had selected for each of the models for that particular authentication step.

For demonstration, suppose a user makes the selection in figure 4.10 for a particular authentication step, the choice is of two sets of images, either a colour based image with a 'blue outline colour' or a pattern based image with 'vertical stripe outline pattern'. Now suppose the user is presented with the image grid in figure 4.11 during an authentication phase for this step, he needs to select an image that satisfies either of the conditions presented by his choice of properties and variants made in the registration phase. Only one of the images for either the colour or pattern based properties will be presented in the authentication grid, hence the user needs to observe the images presented very carefully. Looking carefully at the authentication grid, however, one will observe that there is no image that satisfies the 'vertical stripe outline pattern' condition, but one image satisfies the 'blue outline colour' condition. This image is the one in the 2nd row and 3rd column. The user thus authenticates by selecting this image. The mixed model is believed to provide better security at the expense of usability when compared to either of its component models.

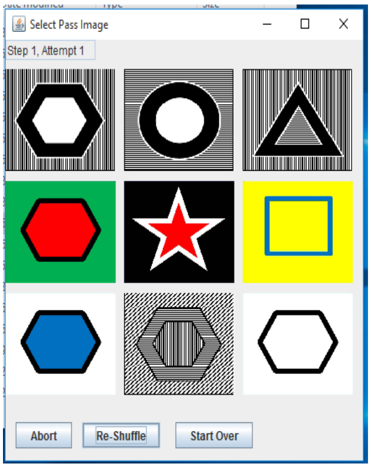
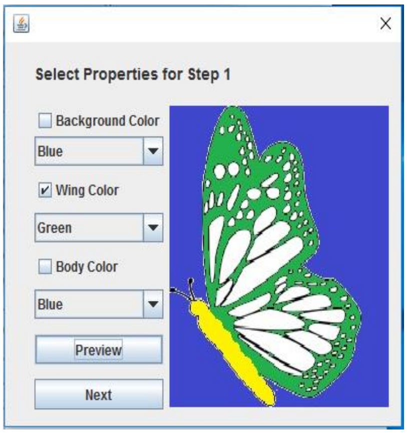


Fig. 4.11: Image selection grid for first step in mixed model.

4.3.4 The Butterfly Model

Each scheme in the property based approach can be implemented through many models. The “butterfly model” has been implemented in this work as another example of the fill based scheme. In this model, different parts of the images of butterflies form the various properties on which a user allocates his chosen variants (colours) during the registration phase. In each authentication round, the user has to identify the butterfly with the properties (image parts) and variants (colours) that satisfy his chosen properties.

In the image properties and variants selection window for the butterfly model, the image properties provided are the image background, the body and the wings. The variants for each of these properties are the colours yellow, blue, green, orange and purple. The properties and variants selection window for the butterfly model is presented in figure 4.12. The image presented in the preview is an image with ‘green wing colour’ which happens to be the user’s choice of properties and variants for this step.



Select Properties for Step 1

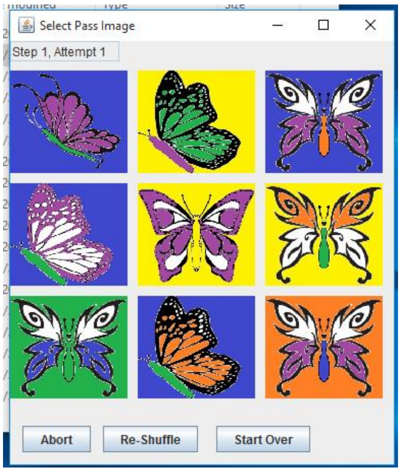
□ Background Color: Blue

☑ Wing Color: Green

□ Body Color: Blue

Fig. 4.12: A preview of properties and variants for butterfly model

For demonstration, suppose during an authentication round for this step the user is presented with the image grid in figure 4.13, the user then needs to identify and select an image that satisfies the ‘green wing colour’ condition. This condition is only satisfied by the image in the 1st row and 2nd column. Hence the user selects this as his pass image for this step.



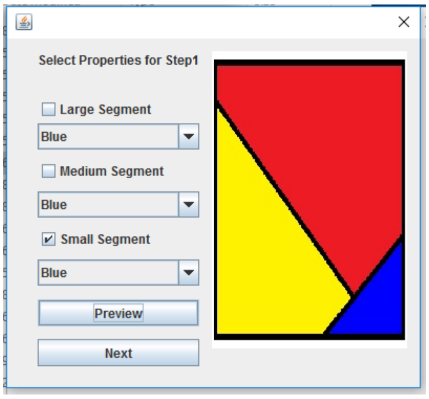
Select Pass Image

Step 1, Attempt 1

Fig. 4.13: Image selection grid for butterfly model

4.3.5 The Magnitude Based Scheme

Another implementation of the property based authentication approach is the magnitude based scheme. In the magnitude based scheme, an image is composed of a number of *objects* of varying magnitudes. The base of authentication in a magnitude based model is the relative magnitudes of the objects that make up the images in the model. The magnitude based model implemented in the course of this work is named ‘broken tiles’. In this model, each image is divided into three sections (or fragments). One of these sections is largest in appearance and is designated as ‘large segment’, another section appears medium sized and is designated as the ‘medium segment’ while a third section appears the smallest in size and is designated as ‘small segment’. These segments constitute the various properties of this model. To each of these segments is assigned a list of colour based variants. As with the fill based models, adjacent segments (properties) are not allowed to have the same variant (colour). The image properties and variants selection window for the magnitude based model is depicted in figure 4.14. In this diagram, the user has selected the ‘small segment’ property and has chosen the ‘blue’ variant. Thus his chosen image for this step is any image in which the smallest segment is coloured blue.



Select Properties for Step1

☐ Large Segment
Blue

☐ Medium Segment
Blue

☑ Small Segment
Blue

Fig. 4.14: Properties and variants selection window for magnitude based model

Suppose a system user is provided with the image grid presented in figure 4.15 during an authentication round to select his password image for the step depicted by figure 4.14, the user needs to identify and select the image in which the ‘small segment’ property is assigned a ‘blue’ variant. That is, he needs to identify and select an image with a ‘blue small segment’. Looking carefully at figure 4.15, the only image in the grid that satisfies the ‘blue small segment’ condition is the image in the 3rd row and 3rd column. On selecting this image, the user is either authenticated or provided with the image selection grid for the next authentication step.

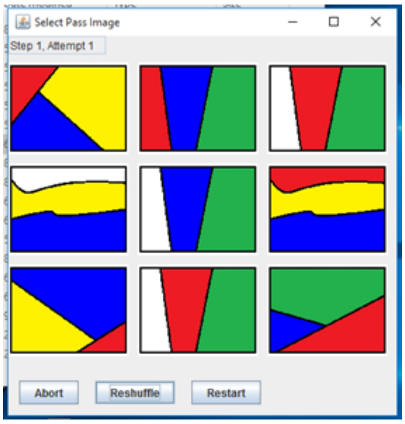
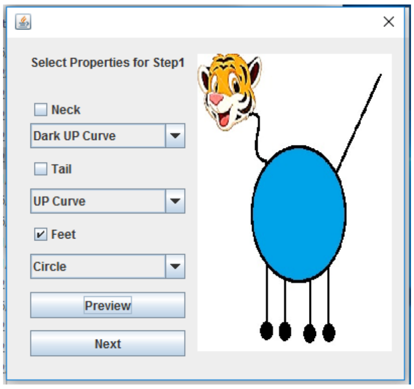


Fig. 4.15: Image selection grid for magnitude model

4.3.6 The Form Based Scheme

Another scheme implemented in the course of this study is the *form based scheme*. In the form based scheme, the visual appearance of objects in an image is the base for user authentication. Appearance may include the size, curvature, posture, shape, etc., of various components of objects within an image. Like all other schemes of the property based approach, there are so many ways in which form based systems could be implemented and how properties in this scheme could be assigned and varied. Variants may include the different braids or styles of human hair, different postures, different types or shapes of caps, different facial expressions, etc. A system that implements a simple clipart for veteran portraits may consider the different shapes of medals, the different types of headgear, the various symbols for the rank, etc.

The form based model developed and evaluated for this research work is termed ‘animal farm’, and image properties are designated by the various sections of a collection of animal images. The properties and variants selection window for the form based model is provided in figure 4.16. In this model, the various properties are the three parts of the animal, the neck, the tail and the feet and each property has five variants. The neck property has variants such as ‘thick curved’, ‘thick straight’, ‘thin curved’, ‘thin straight’ and ‘long’, the tail property has variants such as ‘up curve’, ‘up straight’, ‘down curve’, ‘down straight’, and horizontal, while the feet property has variants such as circle, rectangle, triangle, circle (hollow), and rectangle (hollow). The idea is to make the properties and variants conspicuously different such that they are easy for new users to understand and use.



Select Properties for Step1

☐ Neck

Dark UP Curve

☐ Tail

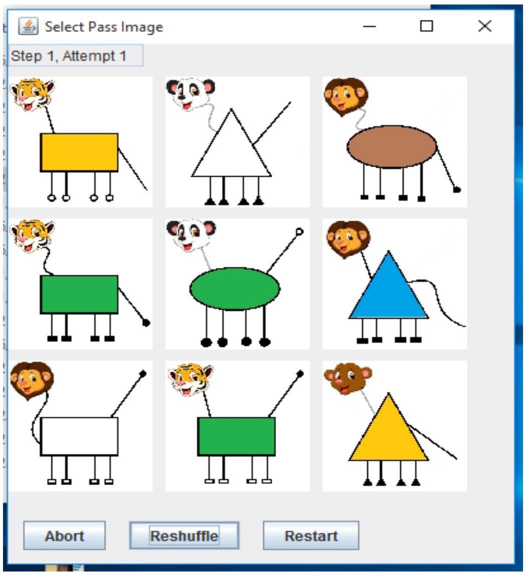
UP Curve

☑ Feet

Circle

Fig. 4.16: Properties and variants selection window for form based model

From figure 4.16, it can be clearly seen that the ‘feet’ property has been selected by the user, and the ‘circle’ has been selected as variant for that property. Hence the users chosen image for this authentication step is an animal with ‘circular feet’. And hence, when the user is presented with the image grid in figure 4.17 to select his chosen image for that step, he needs to identify and select the animal image with circular feet. In the grid presented, only the image in the 2nd row and 2nd column satisfies the condition and is thus the desired image.



Select Pass Image

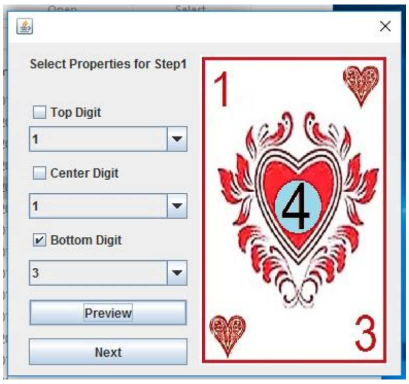
Step 1, Attempt 1

Fig. 4.17: Image selection grid for form based model

4.3.7 The Digit Based Model

Digit based models are a class of property based authentication systems in the number based scheme. The number based scheme is composed of two classes of models; digit based models and number representation based models. In digit based models, number is represented by numeric digits, while in the number representation based models, number is represented by physical representations of numeric value.

The sample digit based model implemented and evaluated in the course of this research work is term the 'playing card model' and is designed as a set of playing cards. The properties in this model are represented by the various positions on a set of playing cards to which numeric digits are allocated. The numeric digits are the variants. Figure 4.18 illustrates the properties and variants selection window for the digit based model. The properties demonstrated in this illustration include a numeric value positioned at the top of the card image and designated as 'top digit', a numeric value positioned at the centre of the card image and designated as 'center digit', and a numeric value positioned at the bottom of the card image and designated as 'bottom digit'. In the illustrated preview, as the checkbox for 'bottom digit' has been checked and the number '3' has been selected as a variant, it can be seen that the image selected by the user is any image in which the bottom digit is the number 3.



Select Properties for Step1

☐ Top Digit

1

☐ Center Digit

1

☑ Bottom Digit

3

Fig. 4.18: Properties and variants selection window for digit based model

Suppose the user is now presented with the image grid in figure 4.19 for his authentication during a subsequent authentication round, the user needs to locate and select the image in which the bottom digit is the number 3. The only image that fits this condition in the grid is the image in the 3rd row and 3rd column. Hence this is the image that the user needs to select to authenticate.

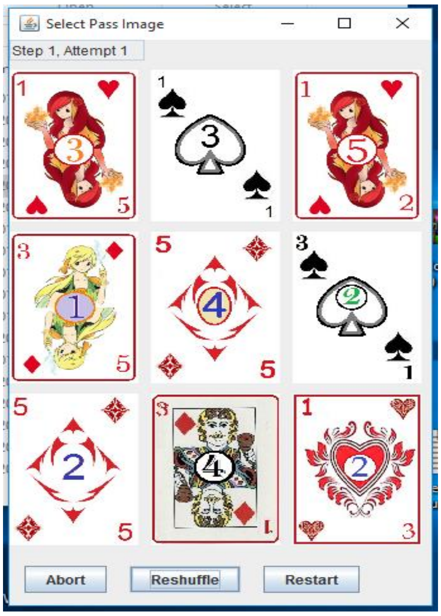
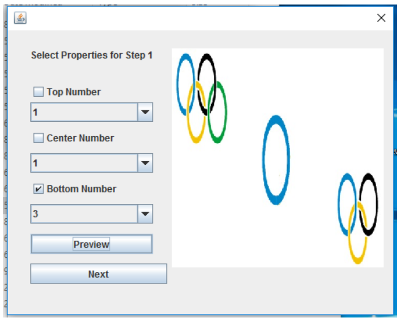


Fig. 4.19: Image selection grid for digit based model

4.3.8 The Representation Based Model

Another representative class of the number based scheme are the representation based models. In these models, numeric quantity is represented by other representations of numeric values, but not numeric digits. Figure 4.20 provides an illustration of the image properties and variants selection window for the representation based model implemented in this research. Like in the digit based model, the properties in this model are designated as 'top number', 'center number' and 'bottom number'. The design and implementation of this model is exactly the same as that in the digit based model, except that in this model there are no digits.

Looking closely at the image in figure 4.20, one would realize that the image represents the image of Olympic rings. The top position has four rings, the center position has one ring and the bottom position has three rings. Thus the image represents the formation: Top – 4, Center – 1, and Bottom – 3. In this demonstration (fig. 4.20), the 'bottom number' property checkbox has been checked, and the number 3 has been selected as the variant. Hence the user's choice image for this step is any image in which a numerical representation of the number 3 is provided at the lower part of the image.



Select Properties for Step 1

☐ Top Number

1

☐ Center Number

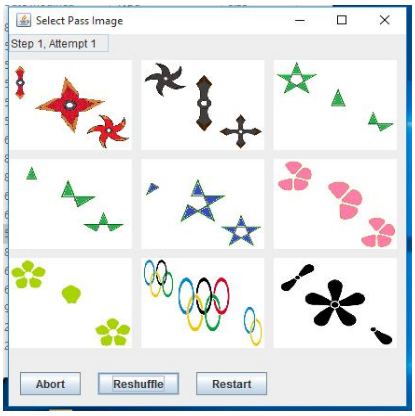
1

☑ Bottom Number

3

Fig. 4.20: Properties and variants selection window for representation based model

Suppose, for example, the user is provided with the image selection grid in figure 4.21 for the selection of his authentication image for this step during any authentication round, the user needs to locate and select any image that has the numerical representation of the number 3 as the number provided in the bottom position. The only image that satisfies this condition is the image in 2nd row and 1st column and is thus the user's pass-image.



Select Pass Image

Step 1, Attempt 1

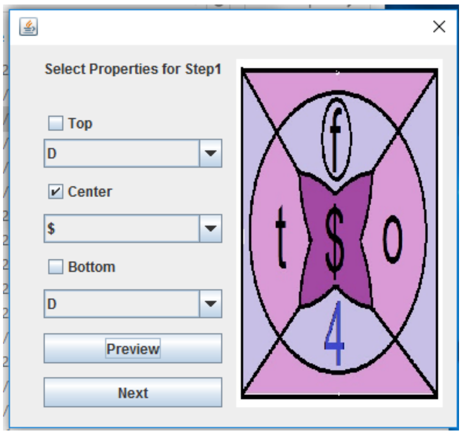
Fig. 4.21: Image selection grid for representation based model

4.3.9 The Character Based Model

Like in the number based scheme, the text based scheme is also made up of two classes of models; the first class is the class of *character based models*, while the second is the set of *word based models*. In a character based model, authentication is done by use of characters. That is, properties are represented by a set of printable characters, mostly alphanumeric characters and symbols.

In the character based model implemented in the course of this work, the image properties are a set of positions on an image to which a set of characters are assigned. From the preview of the image properties and variants selection window for the character based model illustrated in figure

4.22, the image properties are designated as ‘top character’, ‘center character’ and “bottom character’ and the variants are the characters d, e, f, 4, $ and &. In this model, however, other characters are provided as ‘distractor characters’ on the right and left hand sides of the image. From the preview, one could see that the property checkbox checked by the user is the ‘center character’ checkbox and the variant selected for this property is the dollar sign ($). Hence the user’s chosen pass-image is any image in which the center character is a $.



Select Properties for Step1

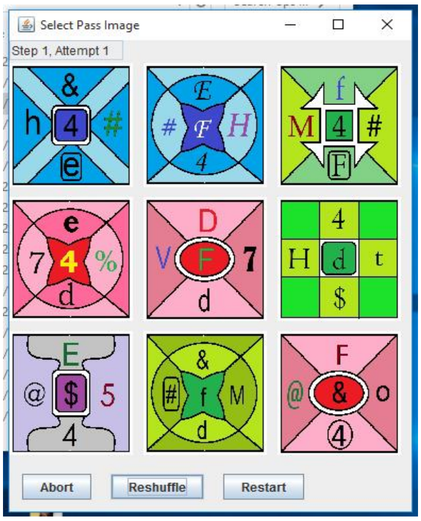
□ Top
D

☑ Center
$

□ Bottom
D

Fig. 4.22: Properties and variants selection window for character based model

Suppose the user is presented with the image selection grid in figure 4.23 during any of his authentication rounds for this step, he needs to locate and select any image with a $ as the centre character. From the diagram in figure 4.23, the only image that satisfies this condition is the image in the 3rd row and 1st column. This is thus the user’s pass-image for this step in this authentication round.

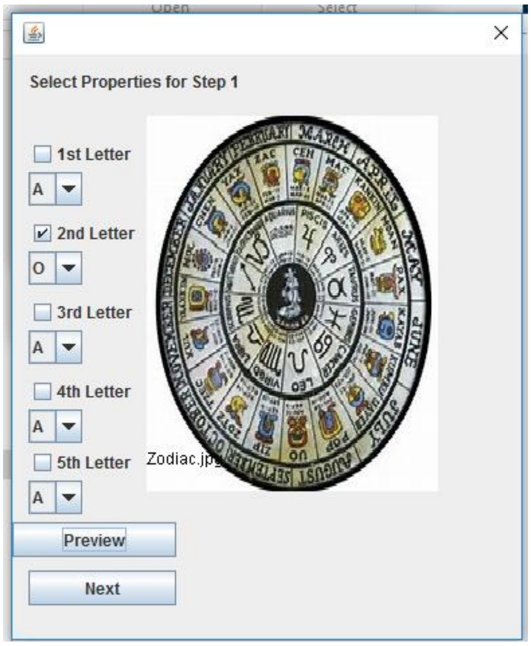


Step 1, Attempt 1

Fig. 4.23: Image selection grid for character based model

4.3.10 The Word Based Model

Word based models are another class of models with the text based authentication scheme. Word based models are designed such that image properties relate to a set of characters within English words. In the implementation of the word based model developed for this course, the properties are the relative positions 1st letter, 2nd letter, 3rd letter, 4th letter and 5th letter, to which alphabetic letters are assigned as variants to each of these positions. The properties and variants selection window for the word based model is illustrated in figure 4.24. As can be seen from this illustration, the user has checked the '2nd letter' checkbox and assigned the letter 'o' as variant for this property. Thus, his pass-image is any image in which the second letter of the word depicted by the image is a letter 'o'. From the image preview provided in figure 4.24 the word 'zodiac' is written in the bottom left corner of the picture. This indicates the content of the picture. During authentication, each image has an English word associated with it, and it is these words that are checked for the satisfaction of the property based condition.



Select Properties for Step 1

□ 1st Letter A

☑ 2nd Letter O

□ 3rd Letter A

□ 4th Letter A

□ 5th Letter A

Fig. 4.24: Properties and variants selection window for word based model

Suppose the same user is presented with the image selection grid in figure 4.25(a) to select his pass-image for this step in any of his authentication rounds, the user needs to locate and select the image in which the second alphabet letter of the word associated with that image is an 'o'. In all the images presented in the grid in figure 4.25(a), only the image in the 3rd row and 1st column satisfies this condition. This image represents the picture of a set of 'sugar tongs' and has the word ‘tongs’ written at the bottom of the image. The word ‘tongs’ is the only word in which the 2nd letter is an ‘o’, and hence the tongs image is the user’s pass image for this step.

Images in a word based model may and may not contain images representing the items the words present. Figure 4.25(a) illustrates a system on which pictorial representations are provided, while figure 4.25(b) illustrates the plain word based model. I word based models, there is a potential that pictures can add to the security of the system as a keen observer may not even observe the English words provided at the bottom left corner of each of the images, whereas it is these words that provide the real authentication factor for this authentication scheme.

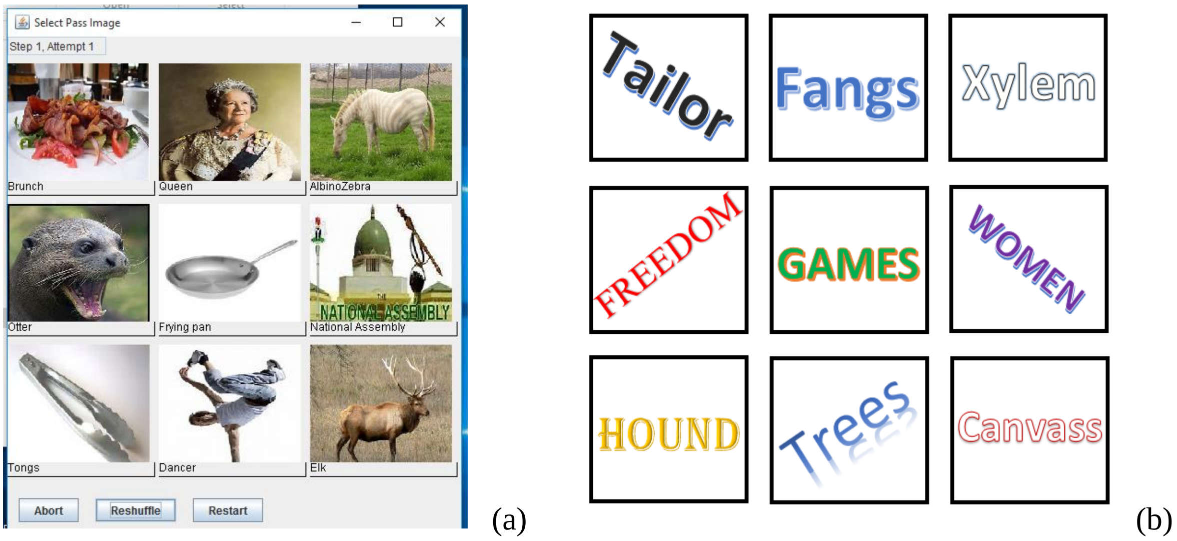


Fig. 4.25: Image selection grid for word based model

4.4 Conclusion

The screenshots provided in this chapter help to better understand both the registration and authentication phases of each of the authentication systems developed in the course of this work. They also help to understand the actual layout, design and behaviour of the systems as well as how one can navigate between the various options. The next chapter discusses the usability experiments conducted as part of this research work. The different experimental procedures followed in each experiment are presented in the chapter as well as well the compilation, analysis and discussions of the results.

Chapter Five – Usability in PBASs

5.1 Introduction

Graphical authentication systems are a relatively new and continuously evolving area of research [138]. As at this moment, there are no established standards in evaluating the usability of graphical authentication systems. Almost every system developed has used a different criteria. This fact has made it exceptionally difficult for researchers to compare the relative performances of graphical authentication systems [130]. In the evaluation of system usability, emphasis is made on the utilisation of methods and tools reported in existing literature. This chapter describes and discusses all experimental procedure, data analysis and results related to all usability related experiments conducted in the process of this research work. The chapter provides the details of experimental procedures, experimental tools and techniques as well as the details of the research findings. The first part of the chapter (from preliminary evaluation to the fourth experiment) evaluates the relative performances of the developed prototypes in relation to the usability based metrics of efficiency, effectiveness and user satisfaction. This is followed by experiments and data analysis (experiment five to experiment ten) related to some of the ideas and concepts developed in the course of this work such as the concepts of ordering and organised image selection for the fill and text based models.

5.2 HCI Usability Evaluation and Metrics

Usability evaluations have proven to be an invaluable tool in human computer interactions research [142] and are important in understanding the extent to which computing systems are used by system users as well as the extent to which the systems meet the users' demand. They are designed to capture and analyse important quantitative and qualitative system use data that are obtained through system login entries as well as user opinion data obtained using experiment questionnaires and interviews. The essence is to gather useful information on the overall performance of computing systems from the users' point of view. Usability data that quantifies usability metrics such as memorability, efficiency, effectiveness, ease of learning, ease of use and user satisfaction are captured and analysed through software login and user opinion questionnaires. According to [143], usability is defined through five *usability factors*. They are:

1. *Ease of learning. The system must be easy to learn for both novices and users with experience from similar systems.*
2. *Task efficiency. The system must be efficient for the frequent user.*

3. *Ease of remembering. The system must be easy to remember for the casual user.*
4. *Understandability: The user must understand what the system does.*
5. *Subjective satisfaction. The user must feel satisfied with the system.*

Researchers in [144] developed a table (table 5.1) that suggests the means by which data can be efficiently captured for data analysis in the usability evaluation of graphical authentication systems. This research has consistently used this model in the implementation and evaluation of the prototypes developed and presented for the hybrid property based graphical authentication system.

Dependent variable	**Behaviour to be measured**	**Method of measurement**
1 . Effectiveness	Ease to remember	Questionnaire
	Failure login rate	System log
2 . Efficiency	Authentication time + Enrolment time	System log
	Ease to enroll	Questionnaire
	Ease to find the authenticator image during authentication	Questionnaire
3. User satisfaction	Preference of the user	Questionnaire

Table 5.1: Dependent variables for usability tests [144]

5.2.1 Usability Metrics

There are a number of usability metrics [145] used to measure the extent to which the system is suitable for use by its intended users. These metrics include:

Effectiveness: This describes the success of interaction from the process point of view. It defines whether or not system users are able carry out tasks accurately and completely to achieve desired goals and to what extent the system is able to meet their needs.

Efficiency: The aim of system users is to carry out needed tasks to effectively reach desired goals. These goals must, however, be performed within acceptable times. The concept of acceptable times is relative and system and process dependent. In measuring the efficiency of a system, the following measures of time must be considered:
Password creation time: This is the time taken for a user to successfully create his new password during registration.

Password authentication time: This is the time it takes for a user to successfully authenticate himself on the system.

Password recovery time: This is the time by which the user is able to recover his password if it is lost or forgotten.

Memorability: Memorability denotes the ability of a user to remember his password without assistance over a relatively long period of time. Memorability is measured consecutively after short (days) and long (months) period of times varying the frequency of system use. Login success rate is used to determine memorability.

Knowledge/ User skills: The ease with which a user can learn, understand and use the system with minimum previous experience or technical expertise is called learnability. It is an important factor as people are normally not willing to spend much time learning to use a system and may dumb the system when they realise that it is difficult to use.

User satisfaction: This is a subjective assessment of the perception of users towards the system. It is a behavioural function that denotes the extent to which users are comfortable with the design and functioning of the system.

5.2.2 Usability Evaluations

In the evaluation of a system's usability, experts suggest a number of applicable methods [146] depending on a number of factors which include resource availability (time and labour), evaluator experience, ability and preference. The methods are:

- ✓ User-based: where a sample of the intended users try to use the application.
- ✓ Expert-based: where an HCI or usability expert makes an assessment of the application.
- ✓ Model-based: where an HCI expert employs formal methods to predict one or more criteria of user performance.

Of the specified methods, application testing using a sample user population is generally considered the most reliable and valid estimate of an application's usability [146]. The evaluations are performed in lab or field trials and are intended to determine the extent to which the application supports the intended users.

In this research, a number of graphical authentication systems have been developed and evaluated using laboratory experiments on a sample user population to ascertain the performance of the systems on a number of usability metrics. These metrics range from information logged onto the system such as timing details to subjective user opinion obtained from survey questionnaires. The aim is to ascertain if statistically significant differences will be recorded on each of these metrics between the various system implementations and to understand the underlying reasons for these differences.

5.2.3 Memorability Evaluations

Memorability tests or retention tests are carried out to test the ability of system users to remember a password system even after a prolonged period of time. They are longitudinal (long term) studies and normally require that participants return for repeated login sessions. They are normally set such that the participants reuse the systems during successive periods of increased interval length and may go on for a number of weeks or even months. As can be seen from table 5.1, however, memorability is a measure of the effectiveness of a system, which in turn forms an important part of usability.

Due to the difficulty to get all participants to return for the continued monitoring of memorability as with many similar projects, memorability experiments have been arranged separately with fewer participants. For this reason and due to timing constraints, it becomes impossible to measure the memorability of all systems under investigation. The memorability experiments are thus conducted with fewer models which are representative of the others.

5.2.4 Study Design and Empirical Evaluation

In the course of this work, a number of statistical data analysis tools have been utilised to help the researcher understand if the mean variation in the in the dependent variable was as a result of the variation of the test condition (the independent variable) or if the mean variation occurred purely by chance. Three statistical analysis methods were thus used depending on the nature of the data collected. ANOVA was used in comparing means among multiple groups, Kruskal-Wallis H test was used in comparing means of more than two groups of ordered categorical data (such as in likert scales were responses are discrete and ordered but cannot be assumed to be equidistant), while Chi-square has been used to compare two sets of non-ordered categorical or nominal data (such as 'yes' and 'no' responses or 'success' and 'failure' as used to obtain the login success rate). This is consistent with tests performed in various usability studies in the analysis of similar data [140, 141, 142]. The formulae for each of these statistical tools is presented in table 5.2. Where necessary, excel charts have also been used for comparisons.

Test	Usage	Formula	Parameters
ANOVA (Tukey post hoc analysis)	Compares variance of the means between more than two groups	X(a; b) = n, p < .05	a = between-groups degrees of freedom, b = within-groups degrees of freedom, n = value of the X statistic, used to determine p, p = significance level.
Kruskal-Wallis H test	Compares the probability distributions of more than two samples of ordered categorical data	H = n, p < .05	n = value of the H statistic, used to determine p, p = significance level.

Chi-square X^2	Compares the probability distributions of two or more samples of non-ordered categorical data	X^2(a, N = b) = n, p < .05	a = degrees of freedom,
			b = sample size,
			n = value of the X^2 statistic, used to determine p,
			p = significance level.

Table 5:2 Statistical data analysis tools

5.3 Preliminary Usability Evaluation

To better understand the workings of the systems and to make any necessary modifications to the experimental plan or procedures, a preliminary evaluation (pilot testing) on user performance was arranged. The experiment was designed to:

- Understand if the system will have any important design issues that may become noticeable to the research participants.
- Understand if there will be need for modifications in experimental design due to user concerns, suggestions or behaviour.

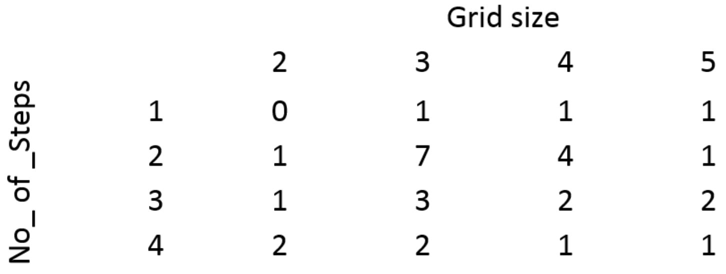
- Understand user choices to help researcher in the choice of the most suitable and most efficient research parameters.

5.3.1 Experimental Procedure

The experiment was set to last for one day to be able to monitor and understand if any action needed to be taken towards the betterment of system design or experimental plan. Thirty (30) student volunteers offered to help test the system and provide the needed feedback. Only one of the system prototypes (the colour based model) was used in the experiment. After a briefing on the use of the system and procedure for the experiment, the participants were each asked to create a password, use the password for two login sessions and provide instant feedback. Participants were not given any limits in the selection of the number of authentication steps and the size of the grid. This was to help the researcher in reaching a decision on the most suitable grid size and number of authentication steps to be used in subsequent user evaluations.

5.3.2 Preliminary Results

From system logs the researcher discovered that the average login time was about 22 seconds. This was considered good enough in consideration of the results obtained from the comparative analysis of existing graphical models presented in table 7.6 in which 6 out of 8 of the systems for which the login time was reported had login times exceeding 25s. This also plausible as the participants were all new to the use of such systems. This is consolidated by the fact that 6 out of the 30 participants had chosen to use up to 4 authentication steps, while 5 of the 30 have used a grid size of 5. The researcher collected the number of steps chosen by each user as well as his chosen grid size in order to understand user preferences in relation to the selection of grid size and number of authentication steps.



		Grid size			
		2	3	4	5
No_of_Steps	1	0	1	1	1
	2	1	7	4	1
	3	1	3	2	2
	4	2	2	1	1

Table 5.3: User Choice of Grid Size and Step Number for Preliminary Test

5.3.3 Observations

In terms of the security of the system, all participants believed that the system was secure enough to be adopted as a password system. Two of the participants, however, suggested that the creation of more properties would make the system safer. From the usability perspective, all participants reported that they were fully comfortable in using the system and that they enjoyed using the system. No suggestion was made for any adjustments to the experimental procedures. One student, however, suggested that the addition of more colours will make the system more attractive, and hence more usable.

In all implementations of the property based system, there are four grid sizes for users to select from. The grid sizes were: 2, 3, 4 and 5. There are also four authentication steps for users to select from; these are 1, 2, 3 and 4. Since each user has four grid sizes to select from, and each user also has four authentication steps to select from, a choice had to be made as to the most suitable grid size/step combination to use in the experiments. Rather than a random selection, the researcher adopts the grid/step combination from the pilot study that is adopted and used by the highest number of participants. This combination happened to be the one with 2 steps and a grid size of 3, which was adopted by the highest population of 7 users and was thus adopted as a control variable.

5.4 Experiment 1

The aim of the experiment was to understand if significant mean variation will be recorded in the sign up (registration) times and login (authentication) times of three of the developed property based authentication models. These are: the colour based model, the pattern based model and the magnitude based model. A comparison of subjective user opinion on the performance of each of the models on various usability metrics was also performed.

5.4.1 Hypothesis

This experiment is aimed at investigating the following hypothesis in relation to the registration (sign up) time, the time to complete the first authentication step (step time 1), the time to complete the second authentication step (step time 2) and the total authentication time (sum of time for step 1 and step 2) performed by the participants. The hypothesis are:

1) *That at least one of the authentication models will incur significantly greater mean registration time than the other models.*
2) *That at least one of the authentication models will incur significantly greater mean login time for step 1 than the other models.*

3) *That at least one of the authentication models will incur significantly greater mean login time for step 2 than the other models.*
4) *That the mean total authentication time will be significantly greater for one of the models than the other models presented.*

5.4.2 Research Participants

Thirty three undergraduate science students participated in the research. All participants were between the ages of 22 and 35 years and each had at least one email address and one bank account, which means that each has at least one password and one PIN. All participants claimed to have used computers and the internet for a number of years and were thus experienced in the use of computers. The use of a student population also ensured that there was not much disparity in proficiency and computing expertise among members of the sample population.

5.4.3 Experimental Design

A within users design was used for the experiment in which thirty three participants were each allocated the three test conditions which were:

1. A colour based implementation of the property based scheme.
2. A pattern based implementation of the property based scheme.
3. A magnitude based implementation of the property based scheme.

The operational procedures and the interface layout of each of the prototypes is identical with the only difference being in the *factor* with which the authentication takes place. The tasks to be performed by each of the participants on each of the prototypes was also the same.

The decision to use a within users design was borne out of the necessity to have a considerably large sample population for the testing of each of the models so as to obtain acceptable and statistically relevant results when the actual participant population was low. It can also help to ensure small variations among the samples as users are tested among themselves.

5.4.4 Experimental Variables

The independent variables are the three property based models used in the experiment. The dependent variables are the system log and user performance data obtained from subjective user opinion through the use of experimental questionnaires. These are the registration and login times and scores awarded by the participants on a number of usability metrics such as ease of use, ease of learning, security and user satisfaction. A post-experiment questionnaire was used to obtain subjection user opinion on a likert type scale of 1 to 9 for all questions that were to be scored by the users.

Although, by design, the grid size for authentication and the number of authentication steps in each scheme for each user is chosen by the user during registration, in each experiment, however, the researcher has chosen a fixed grid size of nine and two authentication steps as control variables for the research. This is to provide the needed uniformity in the number of tasks performed by each of the users in each experiment.

5.4.5 Apparatus and Materials

- A desktop PC running windows vista, 4. 00 GB RAM and 22” monitor
- Three prototypes of the property based system, identical in every aspect of the design and the tasks/procedures the participants are expected to perform.
- A research questionnaire and a consent form to be filled by each participant before the experiment.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

There are basically two operations to be performed in the experiment and each operation is achieved through a set of tasks:

1. **The registration phase**

- o Click on the “sign up” button
- o Enter a chosen username in the textbox provided
- o Select image properties for step 1 in the image properties window
- o Select property variant for 1st property
- o Select image properties for step 2 in the image properties window
- o Select property variant for 2nd property
- o Click on the “next” button

2. **The authentication phase**

- o Enter your chosen username in the textbox provided
- o Select image for step 1 in the step 1 image selection grid
- o Select image for step 2 in the step 2 image selection grid

5.4.6 Experimental Procedure

The following procedure was followed in the conduct of the experiment:

The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their consent before the conduct of the experiments. The basic operations to be performed by each of the participants on each of the system prototypes are to: (1) sign up (or register) their credentials and choices onto the systems, and (2) sign in (log in) into the systems using the choices and credentials they had used to register onto the systems. The systems to be tested form the three experimental conditions:

- A colour based model of the property based scheme.
- A pattern based model of the property based scheme.
- A magnitude based model of the property based scheme.

The laboratory setting was selected so as to isolate each of the participants as they undertake the tasks individually without distraction and without interference. As they arrive the venue of the experiment, the participants are welcomed and given the information sheet to read through. The information sheet contains the basic information about the tasks the participants need to perform as well as their rights in the conduct of the experiments.

After going through the information sheet, the researcher explains the basic procedures of the experiment and asks the participants if they needed any further clarifications. The researcher then launches the program and explains to the participants the layout of the system as well as the choices they have as they go through the registration process. The “preview” button is used to help the participants in understanding the choices they have made. The researcher then observes as the participants go through the authentication process, instructing them only when it was necessary to do so.

On completing the needed experimental tasks, the participants are instructed to fill a post experiment questionnaire. The questionnaire contains the participant’s personal and demographic information, open and closed questions as well as the usability questions that will help to score the system they had tested on number of usability metrics which include their score on the registration and authentication time, security of the system against shoulder surfing and overall user satisfaction.

5.4.7 Experimental Results for Experiment 1

Data analysis was needed to be able to compare the mean variation between the samples. Since there are more than two independent sample groups, a one-way analysis of variance (ANOVA) would be most convenient for the data. Thus, a one-way ANOVA was performed on the data followed by a Tukey post hoc test to determine where the difference occurs in the results if significant differences are recorded. From the output generated by the ANOVA analysis (Appendix 1), it can be seen that significant differences were recorded in the sign up time between groups [F(2,96) = 3.2, p=0.45]. Significant differences were also recorded in the step time 1 between groups [F(2,96) – 5.553, p=0.005], the step time 2 between groups, [F(2,96) = 12.11, p=0.000], and the total authentication time between groups [F(2,96) = 10.66, p=0.000].

The results of multiple comparisons from the Tukey post hoc test, however, reveal that for the sign up time, significant differences are recorded between the pattern based (condition 2, M = 85427, SD = 62016) and the colour based (condition 1, M= 60882, SD = 25606) with p=0.42. For step time 1, significant difference occurs between the colour based (condition 1, M = 4299, SD = 3535) and the pattern based (condition 2, M = 12032, SD = 15404) with p=0.004. For step time 2, significant differences are recorded between the pattern based (condition 2, M = 19025, SD = 20239) and the colour based (condition 1, M = 3814, SD = 2488), p=0.000 and between the pattern based (condition 2, M = 19025, SD = 20238) and the magnitude based (condition 3, M = 10401, SD = 7737), p=0.018. For the total authentication time, significant difference occurs between the pattern based (condition 2, M = 31057, SD = 32785) and the colour based (condition 1, M = 8114, SD = 4980), p=0.000 and between the pattern based (condition 2, M = 31057, SD = 32785) and the magnitude based (condition 3, M = 17336, SD = 11749), with p=0.02.

5.4.8 Discussion of Results for Experiment 1

In spite of the similarity in the operational procedures and interface layout for all of the prototype models for this system (the property based authentication scheme) developed for this research, the researcher has anticipated significant differences in the registration and authentication time for the various authentication models due to the variation in the *factor* with which the authentication is performed. From the results of the ANOVA analysis, significant difference has been marked between groups in all the dependent variables under investigation. A Tukey post hoc analysis has therefore been done to highlight the areas in which the significant difference has occurred.

The Tukey post hoc analysis has revealed that these significant differences have occurred in the sign up time between the pattern based model and the colour based model, with the pattern based model incurring significantly more sign up time than the colour based model. In spite of the fact that the pattern based model incurred more sign up time than the magnitude based model and the magnitude model incurring more sign up time than the colour based model, these differences are not statistically significant, with p=.187 and p=.771 respectively. In step time 1, the trend is exactly the same as in the sign up time. The difference between the pattern based model and the colour based model were statistically significant, with p=0.04. The pattern model also incurred more time than the magnitude model, which in turn incurred more time than the colour based model, but the differences were not statistically significant, with p=0.83 and p=.506, respectively. In step time 2 and the total authentication time, there was significant difference between the pattern based model and colour based model as well as the pattern based model and the magnitude model (p=0.00 and p=0.018) and (p=0.00 and p=0.020) respectively with no other statistically significant differences. In spite of these, the pattern based model has consistently recorded higher times than the other models, while the magnitude model records higher times than the colour model, although their mean difference is not statistically significant.

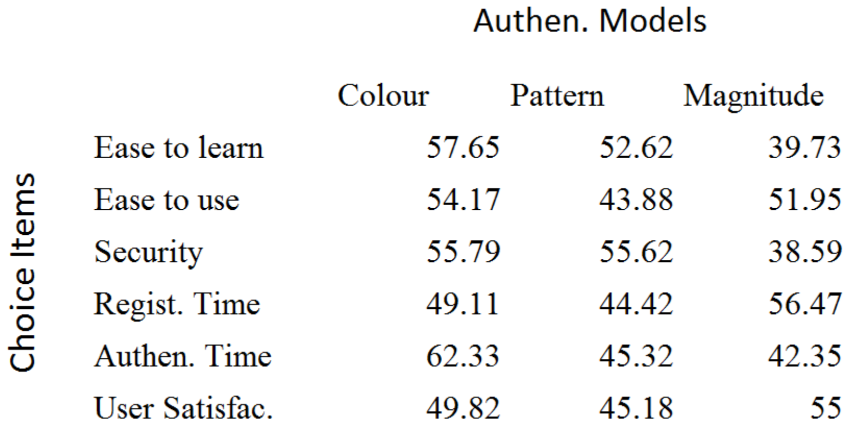
From participant opinion, it could be understood why the pattern based model used up more time as a considerable number of participants complained about the similarity of the patterns and that the patterns were not as conspicuous as the colours used in the other models. The result confirms the hypothetical assumptions that at least one of the analysed models (here, the pattern based model) will incur statistically significant difference in terms of the registration and authentication times than other models.

5.4.9 Analysis of Subjective Opinion (Experiment 1)

Subjective user opinion is useful in usability evaluations and helps to understand and analyse the trends and patterns that may emerge from the user studies. Questionnaires and interviews are among the methods employed to obtain subjective user opinion on the performance of computing systems.

In this work, a research questionnaire was developed and administered to help understand user choices and opinions on the performance of the system prototypes presented. A Likert scale of 1 to 9 was adopted to obtain user opinion on the systems performance in relation to the ease with which the systems can be learned, the ease with which the systems can be used, the security of the systems against shoulder surfing, their satisfaction with the systems registration and authentication times as well as their overall satisfaction with the performance of the system. The large range of the likert scale was selected to provide high granularity of user responses. A non-parametric (Kruskal-Wallis) test was used in the analysis. The responses for each of the metrics stated was analysed and the mean ranks presented in table 5.4 as obtained from the Kruskal-Wallis test. These results have been converted into the bar chart in figure 5.1.

As already stated, Kruskal-Wallis H test was used in the analysis of subjective data obtained from likert scales in the research questionnaire to obtain values for the six items which include Ease to learn, Ease of use, Registration time, Authentication time, Security, and User satisfaction. For the ‘Ease to learn’ data, the results confirmed statistically significant difference in score between the different models, $X^2(2) = 7.615$, $p = 0.022$, with mean rank score of 57.67 for Colour, 52.62 for Pattern and 39.73 for the Magnitude model. The results for Ease of use’ showed no statistically significant variation in mean rank score among the models with $X^2(2) = 2.554$, $p = 0.279$ and the mean rank score of 54.17 for Colour, 43.88 for Pattern and 51.95 for the Magnitude based model. The ‘Security’ data also shows significant variation in mean rank $X^2(2) = 8.782$, $p = 0.012$ with a mean rank of 55.79 for Colour based, 55.62 for Pattern based and 39.59 for Magnitude based. Results for ‘Registr. Time’ does not indicate significant variation in mean rank $X^2(2) = 3.263$, $p = 0.196$ and with mean rank score of 49.11 for the Colour model, 44.42 for the Pattern and 56.47 for the Magnitude model. The results for ‘Authen. Time’ also shows statistically significant mean variation in rank with $X^2(2) = 10.684$, $p = 0.005$, with mean rank score of 62.33 for the Colour model, 45.32 for the Pattern model and 42.35 for the Magnitude model. The results for ‘User satisfactn’ does not indicate statistical significance in mean rank $X^2(2) = 2.279$, $p = 0.32$, with mean rank score of 49.92 for the Colour model, 45.18 for the Pattern model and 55.00 for the Magnitude model. This result is also presented in the chart in figure 5.1.



		Authen. Models		
		Colour	Pattern	Magnitude
Choice Items	Ease to learn	57.65	52.62	39.73
	Ease to use	54.17	43.88	51.95
	Security	55.79	55.62	38.59
	Regist. Time	49.11	44.42	56.47
	Authen. Time	62.33	45.32	42.35
	User Satisfac.	49.82	45.18	55

Table 5.4: Comparison of mean ranks (Experiment 1)

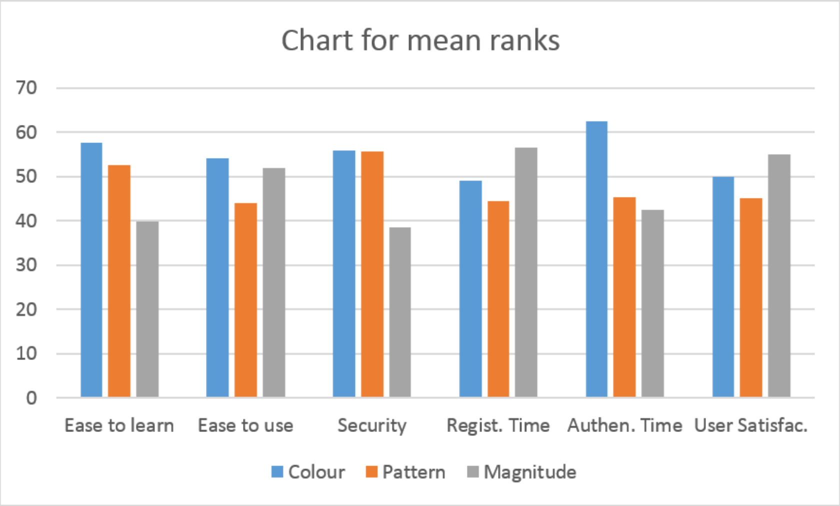


Fig. 5.1: Comparison of mean ranks of models (Experiment 1)

5.5 Experiment 2

Experiment 2 was conducted about two months after experiment 1. In experiment 2, five software prototypes were used instead of the three prototypes used in experiment 1. The researcher wanted to know if statistically significant differences will be recorded in the registration and login times of five property based models: a colour based model, a pattern based model, a mixed (colour-pattern) model, a magnitude model and a butterfly based implementation of the colour model (the butterfly model). A comparison of the data gathered on the subjective opinion of users on the performances of the models on various usability metrics was also performed.

5.5.1 Main Hypotheses

This experiment is aimed at investigating a number of hypotheses in relation to the dependent variables of registration (sign up) time, the time to complete the first authentication step (step time 1), the time to complete the second authentication step (step time 2) and the total authentication time (sum of time for step 1 and step 2) all collected through system logging during the conduct of the experiment. The hypothesis are:

1) *That at least one of the authentication models will incur significantly greater mean registration time than the other models.*
2) *That at least one of the authentication models will incur significantly greater mean login time for step 1 than the other models.*

3) *That at least one of the authentication models will incur significantly greater mean login time for step 2 than the other models.*
4) *That the mean total authentication time will significantly be greater for at least one of the models than the other models presented.*

5.5.2 Research Participants

Eighteen undergraduate science students were recruited for a within users study of the five prototype models. All participants were between the ages of 22 and 38 years and each had at least one email and one bank account, hence, each participant had at least one online password and one numerical PIN and thus had an experience in the use of passwords. All participants claimed to have used computers and the internet for between one and six years and were thus all experienced in the use of computers. The use of a student population ensured little disparity in computing expertise among members of the participant population.

5.5.3 Experimental Design

A within users design was used for the experiment in which eighteen participants were recruited and each was allocated the five test conditions which were:

1. A colour based implementation of the property based scheme. (see section 4.3.1 – 4.3.5)
2. A pattern based implementation of the property based scheme.
3. A mixed (colour-pattern) based implementation of property based model.
4. A butterfly model implementation of the colour based scheme.
5. A magnitude based implementation of the property based scheme.

The operational procedures and the interface layout of each of the prototypes is identical with the only difference being in the *factor* with which the authentication is performed. The tasks to be performed by each of the participants on each of the prototypes was also the same.

Like in experiment 1, the decision to use a within users design was done due to the necessity to have a considerably large sample population for the testing of each of the sample prototypes for acceptable results when the sample user population was small.

5.5.4 Experimental Variables

The independent variables are the five property based models being investigated in the experiment. The dependent variables are timing data for registration and authentication captured automatically by the systems in the conduct of the experiments and subjective user opinion data collected through the use of experimental questionnaires issued during the conduct of the work to collect subjective user opinion on the performance of the systems in relation to a number of usability metrics. The dependent variables are the registration and authentication times and the scores awarded by the participants on a number of usability metrics such as ease of use, ease of learning, security and user satisfaction. A post-experiment questionnaire was used to obtain subjective user opinion on a likert type scale of 1 to 9 for all questions that were to be scored by the users.

Although, by design, the grid size for authentication and the number of authentication steps in each scheme is determined by the user during his registration process, in each experiment, however, the researcher had chosen a fixed grid size of nine and two authentication steps as control variables for the research. This is necessarily to provide the needed uniformity in the number of tasks performed by each of the research participants.

5.5.5 Apparatus and Materials

- An ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6” monitor
- Five prototypes of the property based system, identical in every aspect of the design and the tasks/procedures the participants are expected to perform.
- A research questionnaire and a consent form to be filled by each participant before the experiment.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

There are basically two operations to be performed in the experiment and each operation is achieved through a set of tasks:

1. **The registration phase**
   - ✓ Click on the “sign up” button
   - ✓ Enter a chosen username in the textbox provided
   - ✓ Select image properties for step 1 in the image properties window
   - ✓ Select image properties for step 2 in the image properties window

2. **The authentication phase**
    - ✓ Enter your chosen username in the textbox provided
    - ✓ Select image for step 1 in the step 1 image grid
    - ✓ Select image for step 2 in the step 1 image grid

5.5.6 Experimental Procedure

The following procedure was followed in the conduct of the experiment:

The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their consent before the conduct of the experiments. The basic operations to be performed by each of the participants on each of the system prototypes are to: (1) sign up (or register) their credentials and choices onto the systems, and (2) sign in (log in) into the systems using the choices and credentials they had used to register onto the systems. The systems to be tested form the five experimental conditions:

- A colour based model of the property based scheme. (see 4.3.1 – 4.3.5)
- A pattern based model of the property based scheme.
- A mixed (colour and pattern) model of the property based scheme.
- A magnitude based model of the property based scheme.
- A butterfly based implementation of the colour based scheme.

The laboratory setting was selected so as to give the participants the desired isolation in doing the needed tasks without distraction while still using the systems in an environment they are familiar with. Each of the participants was made to undertake the tasks individually without interference. Unlike in the first experiment, a collective training session was organised for the volunteers in which a display was made of the various prototypes and their operational procedures to help acquaint them with the functioning of the systems. As they arrive the venue of the experiment, the researcher ensures they are comfortable. When the participant is well seated, the researcher hands him the information sheet to read through. The information sheet contains the basic information about the tasks the participants need to perform as well as their rights in the conduct of the experiments.

The researcher then launches the system prototype and waits for the user to complete the desired tasks. On completing the needed experimental tasks, the participants are instructed to fill a post experiment questionnaire. The questionnaire contains sections on the participant’s personal and demographic information, background information and score based usability related questions to capture the participant's subjective opinion on the use of these systems.

5.5.7 Experimental Results for Experiment 2

A one-way analysis of variance (ANOVA) was performed on the data with a Tukey post hoc test to compare the means of the dependent variables in relation to the independent variables (Appendix 2). From the ANOVA analysis it could be seen that no statically significant difference was observed for the registration and step time 1 between the groups [F(4,85) = 1.059, p=0.382] and [F(4,85) = 1.027, p=0.398]. Statistically significant difference between groups was observed in Step Time 2, Authentication Time and Average Time in [F(4,85) = 10.345, p=0.001], [F(4,85) = 5.414, p=0.000] and [F(4,85) = 5.414, p=0.001]. Tukey post hoc test reveals that in step time 2, there is a significant difference in mean time for step 2 between the mixed model (condition 3, M = 23595, SD = 10497) and the colour model (condition 1, M = 8983, SD = 4425), with p=0.000, and between the mixed model (condition 3, M = 23595, SD = 10497) , p=0.000, and magnitude model (condition 4, M = 10163, SD = 6294), p=0.000, between the mixed model (condition 3, M = 23595, SD = 10497) and the butterfly model (condition 5, M = 11776, SD = 9382) p=0.000, The Tukey test also reveals significant difference in the total authentication time (Authen. Time) between the colour model (condition 1, M = 19725, SD = 7956) and the mixed model (condition 3, M = 37862, SD = 17740), p=0.001 and between the pattern model (condition 2, M = 21510, SD = 8440), and the mixed model (condition 3, M = 37862, SD = 17740), p=0.003.

5.5.8 Discussion of Results for Experiment 2

From the data presented in Appendix 2 and the preceding section in can be seen that no statistically significant mean variation was computed for the registration time and step time 1 between the groups. However, for step time 2, there was a statistically significant mean variation between the mixed model (condition 3) and all the other models with p=0.000. For both the total authentication and average authentication times, the Tukey test also reveals statistically significant variation in means only between the between the mixed model (condition 3) and the colour p=0.001 and pattern (p=0.003) models. This result is consistent with three of the main hypotheses. Only assumption 2, *that a least one of the models will incur a statistically significant mean variation in mean login time for step 1* did not hold. In the ANOVA analysis, the mixed model had significantly greater mean login time than the other models. There is an assumption even among participants that the mixed model is more difficult to work with. Since the mixed model operates somewhat as a "combined model" it will not be surprising if it takes a longer to locate its images.

5.5.9 Analysis of Subjective Opinion (Experiment 2)

In experiment 2, as in the first, a research questionnaire was administered to sample user opinion on a number of usability metrics using a likert scale of 1 to 9. The likert scale of 1 to 9 was adopted for increased granularity in user response. As in experiment 1, these metrics are systems performance based items such as user satisfaction in the registration and authentication times, usability issues such as the ease of learning and ease of use, overall user satisfaction in the design and layout of the system as well as the presumed security of the system. The responses for each of the metrics relation to the independent variables (the models) has been analysed in a non-parametric Kruskal-Wallis test and the mean ranks of scores presented by the analysis for each of the items is presented in table 5.5. The test results obtained have further been translated into the chart in figure 5.2 for direct comparison.

As in experiment 1, Kruskal-Wallis H test was used in the analysis of subjective data obtained from likert scales presented for the values of the six system use items which include Ease to learn, Ease of use, Registration time, Authentication time, Security, and User satisfaction. For the 'Ease to learn' data, the results do not indicate statistically significant difference in rank score between the different models, $X^2(4) = 6.913$, $p = 0.141$, with mean rank score of 57.83 for Colour, 37.19 for Pattern, 48.08 for Magnitude, 53.36 for Butterfly and 37.03 for the mixed model. The results for Ease of use' showed statistically significant variation in mean rank score among the models with $X^2(4) = 30.216$, $p = 0.000$ and a mean rank score of 36.31 for Colour, 43.44 for Pattern and 59.03 for the Magnitude, 64.00 for Butterfly and 24.00 for the mixed model. The 'Security' data does not indicate statistically significant variation in mean rank $X^2(4) = 4.007$, $p = 0.405$ with a mean rank of 39.19 for Colour based, 42.83 for Pattern based and 42.53 for Magnitude based 49.22 for Butterfly and 53.72 for the mixed model. Results for 'Registr. Time' indicates significant variation in mean rank between models $X^2(4) = 9.985$, $p = 0.041$ with mean rank score of 55.39 for the Colour model, 32.89 for the Pattern model, 44.56 for the Magnitude, 53.78 for the Butterfly model and 40.89 for the mixed model. The results for 'Authen. Time' show no statistically significant mean variation in rank with $X^2(4) = 6.865$, $p = 0.143$, with mean rank score of 57.33 for the Colour model, 35.50 for the Pattern model and 45.31 for the Magnitude, 45.22 for the Butterfly and 44.14 for the mixed model. The results for 'User satisfactn' does not indicate statistical significance in mean rank $X^2(4) = 5.973$, $p = 0.201$, with mean rank score of 52.22 for the Colour model, 43.17 for the Pattern model, 44.83 for the Magnitude, 52.22 for the Butterfly and 35.06 for the mixed model.

	Authen. Models				
Choice Items	Colour	Pattern	Magnitude	Butterfly	Mixed
Ease to learn	51.83	37.19	46.08	53.36	37.03
Ease to use	36.31	43.44	59.03	64	24.72
Security	39.19	42.83	42.53	49.22	53.72
Regist. Time	55.39	32.89	44.56	53.78	40.89
Authen. Time	57.33	35.5	45.31	45.22	44.14
User Satisfac.	52.22	43.17	44.83	52.22	35.06

Table 5.5: Comparison of mean ranks for authentication models (Experiment 2)

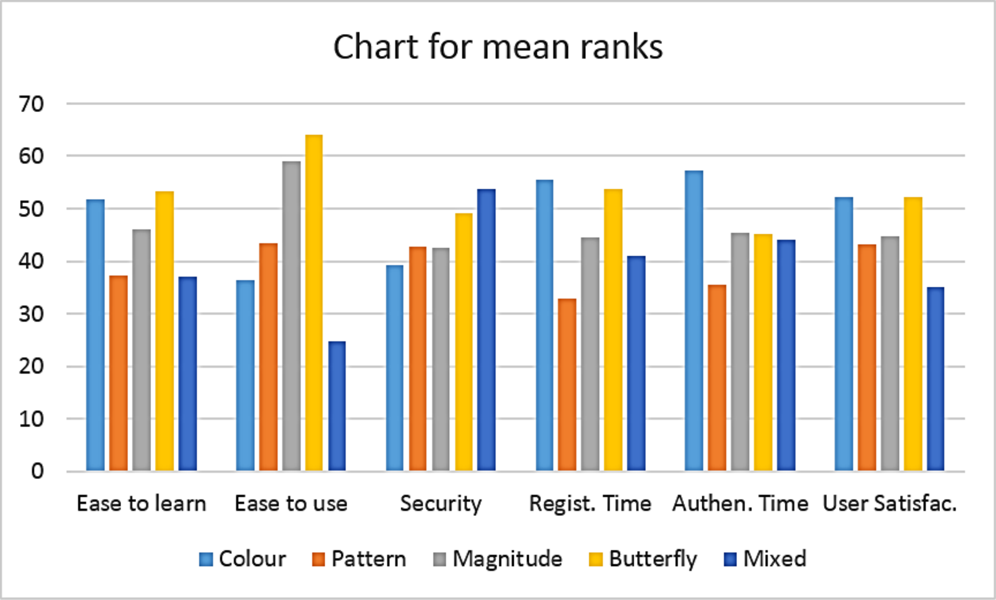


Fig. 5.2: Comparison of mean ranks for authentication models (Experiment 2)

5.5.10 Discussion of Research Findings

The aim of this work is to ascertain the usability, security and acceptability of the property based approach to graphical authentication. In doing this, subjective opinion is gathered and used alongside system generated data for data analysis and interpretation. The preceding sections provide details of the implementation and analysis of five implementations of the property based paradigm. The findings suggest that property based systems indeed have both the usability and security capabilities to be adopted and utilised as an efficient algorithm for graphical user authentication.

From the analysis of user registration and authentication for a two-step authentication on five models, the mean registration time was not more than 80 seconds for the second experiment and the mean authentication (login) time was about 25 seconds. The result is not surprising as the user needs to take some time in the registration phase to make a choice in terms of both the acquisition of a username and a graphical password. Whereas the participant only needs to recall and key-in the username and then select his password in the authentication phase. ANOVA results of the timing variables also shows a reduction in time between the first experiment and the second. This is probably due to the separate training session introduced before the commencement of the second experiment as opposed to the first.

Subjective user opinion also indicates significant promise for the property based model. In both the first and second usability trials, on a likeart scale of 1 to 9 designed to measure the ease of learning, ease of use, user satisfaction in the registration and authentication time, security against shoulder surfing and overall satisfaction, the lowest mean score was 5.67. This clearly indicates that the participants were generally satisfied with performance of the various prototypes presented.

5.6 Experiment 3

Purpose: Experiment to compare the usability of five prototype models: The digit based model, the number representation based model, the form based model, the character based model and the word based model

Aim: To collect and analyse data on user and system performance in relation to these models.

5.6.1 Main Hypotheses

This experiment is aimed at investigating a number of hypotheses in relation to the dependent variables of registration (sign up) time, the time to complete the first authentication step (step time 1), the time to complete the second authentication step (step time 2) and the total authentication time (sum of time for step 1 and step 2) all collected through system logging during the conduct of the experiment. The hypotheses are:

1) *That at least one of the authentication models will incur significantly greater mean registration time than the other models.*
2) *That at least one of the authentication models will incur significantly greater mean login time for step 1 than the other models.*

3) That at least one of the authentication models will incur significantly greater mean login time for step 2 than the other models.

4) That the mean total authentication time will significantly be greater for at least one of the models than the other models presented.

5.6.2 Research Participants

Twenty participants were recruited from a university's undergraduate computing science student population for a within users study of the five prototype models. All participants were between the ages of 20 and 35 years of age and each had at least one email and one bank account, hence, each participant had at least one online password and one numerical PIN and thus had an experience in the use of passwords. All participants claimed to have used computers and the internet for between one and six years and were thus all experienced in the use of computers. The use of a student population ensured little disparity in computing expertise among members of the participant population. The study was a lab study conducted within a period of two weeks.

5.6.3 Experimental Design

A between users design was used for the experiment in which twenty participants were recruited and each was allocated the five test conditions which were:

1. A digit based implementation of the property based scheme. (see 3.3, 4.3.6 – 4.3.10)
2. A number representation based implementation of the property based scheme.
3. A form based implementation of property based model.
4. A character based implementation of the property based scheme.
5. A word based implementation of the property based scheme.

The operational procedures and the interface layout of each of the prototypes is identical with the only difference being in the *factor* with which the authentication is performed. The tasks to be performed by each of the participants on each of the prototypes was also the same.

The experiment is a repetition of experiment 2, but with newer models. Hence, each participant was asked to create a password using one of the aforementioned models and then asked to login to the system using his password. The participant is then asked to fill a post experiment questionnaire to obtain his opinion on the performance of the system.

5.6.4 Experimental Variables

The independent variables are the five property based models being investigated in the experiment. The dependent variables are the registration and authentication timing data collected automatically by the systems in the conduct of the experiments and the subjective user opinion data collected through the use of experimental questionnaires issued during the conduct of the work to collect subjective user opinion on the performance of the systems in relation to a number of usability metrics. The dependent measures are the registration and authentication times and the scores awarded by the participants on a number of usability metrics such as ease of use, ease of learning, security and user satisfaction using a likert type scale of 1 to 7 for all questions to be scored by the users.

5.6.5 Apparatus and Materials

- Two ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6” monitor
- Five prototypes of the property based system, identical in every aspect of the design and the tasks/procedures the participants are expected to perform.
- A research questionnaire and a consent form to be filled by each participant before the experiment.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

There is basically two operations to be performed in the experiment and each operation is achieved through a set of tasks:

1. The registration phase

✓ Click on the “sign up” button

✓ Enter a chosen username in the textbox provided

✓ Select image properties for step 1 in the image properties window

✓ Select property variant for selected property for step 1

✓ Select image properties for step 2 in the image properties window

✓ Select property variant for selected property for step 2

2. The authentication phase

✓ Enter your chosen username in the textbox provided

✓ Select image for step 1 in the step 1 image grid

✓ Select image for step 2 in the step 1 image grid

5.6.6 Experimental Procedure

The following procedure was followed in the conduct of the experiment:

The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their consent before the conduct of the experiments. The basic operations to be performed by each of the participants on each of the system prototypes are to: (1) sign up (or register) their credentials and choices onto the systems, and (2) sign in (log in) into the systems using the choices and credentials they had used to register onto the systems. The systems to be tested form the five experimental conditions:

- A digit based implementation of the property based scheme. (see 4.3.6 – 4.3.10)
- A number representation based implementation of the property based scheme.
- A form based implementation of property based model.
- A character based implementation of the property based scheme.
- A word based implementation of the property based scheme.

The laboratory setting was selected so as to give the participants the desired isolation in doing the needed tasks without distraction while still using the systems in an environment they are familiar with. Each of the participants was made to undertake the tasks individually without interference. As they arrive the venue of the experiment, the participants are given the information sheet to read through. The information sheet contains the basic information about the tasks the participants need to perform as well as their rights in the conduct of the experiments.

After going through the information sheet, the researcher further explains the purpose and procedure for the experiment and asks the participants if they needed any further clarifications. The researcher then launches the system prototype on which the participant will work and answers any questions the participant may wish to ask. The “preview” button helps the participants in understanding the choices they have made especially with regards to the choice of properties and their corresponding variants. The researcher then observes as the participant undertakes and completes the tasks needed for authentication.

On completing the needed experimental tasks, the participants are instructed to fill a post experiment questionnaire. The questionnaire contains sections on the participant’s personal and demographic information, background information and score based usability related questions to capture the participant’s subjective opinion on the use of the system.

5.6.7 Experimental Results for Experiment 3

A one-way analysis of variance (ANOVA) was performed on the data with a Tukey post hoc test to compare the means of the dependent variables in relation to the independent variables (Appendix 3). From the ANOVA analysis it could be seen that statically significant mean variation was observed for the Registration time between groups [F(4,95) =4.051, p=0.004], for step time 1 between groups [F(4,95) = 5.116, p=0.001], for step time 2 between groups [F(4,95) = 7.043, p=0.000]and authentication time (Authent. Time) between groups [F(4,95) = 6.627, p=0.000]. The Tukey post hoc test reveals that the mean variation takes place for the registration time between the character based (condition 6, M = 53165.25, SD = 13864.348) and the word based (condition 10, M = 37023.70, SD = 14923.471), p =0.47, and between the digit based model (Condition 7, M = 56732.75, SD = 32738.771) and the word based model (condition 10, M = 37023.70, SD = 14923.471) p = 0.008. The statistically significant mean variation for step time 1 is between the character based model (condition 6, M = 6651.10, SD = 5465.659) and the form based model (condition 9, M = 20644.10, SD = 15501.655), p = 0.000 and between the digit based model (condition 7, M = 10739.10, SD = 9989.373) and the form based model (condition 9, M = 20644.10, SD = 15501.655), p = 0.21. The mean variation is statistically significant for step time 2 between the character based model (condition 6, M = 11403.50, SD = 4908.341) and the form based model (condition 9, M = 29140.90, SD =17485.371), p = 0.000, between the character based model (condition 6, M = 11403.50, SD 4908.341) and the word based model (condition 10, **M =** 22037.65, SD = 10785.182), p = 0.24 and between the digit based model (condition 7, M = 17069.90, SD = 10043.936) and the form based model (condition 9, M = 29140.90, SD = 17485.371), p = 0.007. The mean variation is statistically significant for authentication (login) time is between the character based model (condition 6, M = 18054.60, SD = 9383.247) and the form based model (condition 9, M = 49785.00, SD = 32344.921), p = 0.000 and between the digit based model (condition 7, M = 27809.00, SD = 18517.177) and the form based model (condition 9 M = 49785.00, SD = 32344.921), p = 0.007

5.6.8 Discussion of Results for Experiment 3

From the results presented by the Tukey post hoc analysis, it can be seen that the statistically significant mean variation was recorded for the registration times between the character and digit based models and the word based model. The character and digit based models each incurred a mean registration time of almost a minute, while the word based model had a mean registration time of 37 seconds. The reason for the reduction is that although the word based model has a higher number of properties to select from, all selection is done on a single window. The others models all use three properties and these are selected in two separate windows. Hence the mean registration time for the word based model is significantly lower than that of all the other models.

In both step 1 and step 2, significant mean variation is recorded between the character based model and the form based model as well as between the digit based model and the form based model. Both the character and digit models recorded significantly lower mean registration times for both step 1 and step 2 (7 seconds and 11 seconds, and 11 seconds and 17 seconds respectively) than the form based model (21 seconds and 29 seconds respectively). One will reason with this results since it may be a bit more difficult to identify pass image objects in the form based model then in the digit and character based models. The mean variation in the 1st and 2nd steps of the authentication circle adds up to the mean variation in the total authentication time which shows the same pattern in the significance in mean variation between the character and digit models against the form based model.

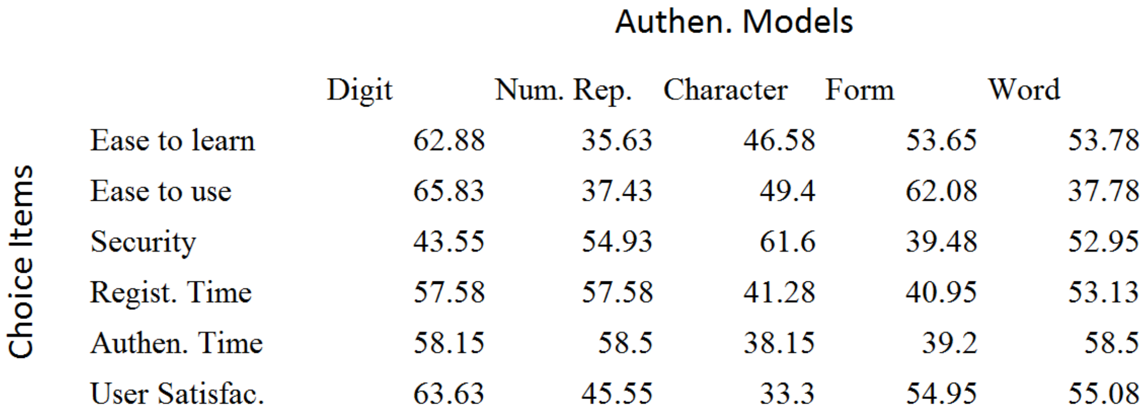
The results of the post hoc test confirms all four of the hypotheses that (1) *at least one of the authentication models will incur significantly greater mean registration time than the other models,* (2) *at least one of the authentication models will incur significantly greater mean login time for step 1 than the other models,* (3) *at least one of the authentication models will incur significantly greater mean login time for step 2 than the other models, and* (4) *the mean total authentication time will significantly be greater for at least one of the models than the other models presented.*

This clearly indicates that probably due to design related issues such as the specific procedure of user registration, the procedure of image selection, or the factor of authentication, significant variations do occur in the different timing parameters of a property based model. The results indicate that users are generally slower in using some of the systems than others, proving that some implementations may thus be more efficient than others. Timing is a vital component of efficiency, just as efficiency is a vital component of the overall usability of the system.

5.6.9 Analysis of Subjective Opinion (Experiment 3)

This section puts together the data collected for qualitative analysis of the system through user feedback obtained using survey questionnaires given to every research participant. In the questionnaires, participant responses to questions relating to the usability, security and user satisfaction are rated using a likert scale of 1 to 7. The scale of 1 to 7 was thought to present greater clarity of response than the 9 point scale especially as the participants were generally new to the use of likert scales. As with the first two experiments, a non-parametric (Kruskal-Wallis H test) was used to analyse the responses. Mean rank scores for each of the evaluated models as reported by the test are collectively compared in table 5.6. Table 5.6 is further converted into the chart in figure 5.3.

Kruskal-Wallis H test was used in the analysis of subjective user opinion obtained from likert questions in the questionnaires. The likert items were six usability and system use information which include Ease to learn, Ease of use, Registration time, Authentication time, Security, and User satisfaction. For the 'Ease to learn' data, the results indicate that statistically significant variation in rank score exists between the models, $X^2(4) = 10.640$, $p = 0.031$, with mean rank score of 62.88 for Digit, 35.63 for Num. Rep. Pattern, 46.58 for Char, 53.65 for Form and 53.78 for the Word based model. The results for Ease of use' showed statistically significant variation in mean rank score among the models with $X^2(4) = 18.019$, $p = 0.001$ and a mean rank score of 65.83 for Digit., 37.43 for Num. Rep., 49.40 for the Char., 62.08 for Form and 37.78 for the Word based model. The 'Security' data does not indicate statistically significant variation in mean rank $X^2(4) = 8.202$, $p = 0.084$ with a mean rank of 43.55 for Digit based, 54.93 for Num. Rep. based, 61.60 for Character based, 39.48 for Form based and 52.95 for Word based model. Results for 'Registr. Time' does not indicate statistically significant variation in mean rank between models $X^2(4) = 7.805$, $p = 0.099$ with mean rank score of 57.58 for the Digit model, 57.58 for the Num. Rep. model, 41.28 for the Character model, 40.95 for the Form model and 55.13 for the Word model. The results for 'Authen. Time' show statistically significant mean variation in rank with $X^2(4) = 12.019$, $p = 0.017$, with mean rank score of 58.15 for the Digit model, 58.50 for the Num. Rep. model and 38.15 for the Character model, 39.20 for the Form based model and 58.50 for the Word based model. The results for 'User satisfactn' also indicate statistical significant variation in mean rank $X^2(4) = 13.659$, $p = 0.008$, with mean rank score of 63.63 for the Digit model, 45.55 for the Num. Rep. model, 33.30 for the Character model, 54.96 for the Form and 55.08 for the Word based model



Choice Items	Authen. Models				
	Digit	Num. Rep.	Character	Form	Word
Ease to learn	62.88	35.63	46.58	53.65	53.78
Ease to use	65.83	37.43	49.4	62.08	37.78
Security	43.55	54.93	61.6	39.48	52.95
Regist. Time	57.58	57.58	41.28	40.95	53.13
Authen. Time	58.15	58.5	38.15	39.2	58.5
User Satisfac.	63.63	45.55	33.3	54.95	55.08

Table 5.6: Comparison of mean ranks for authentication models (Experiment 3)

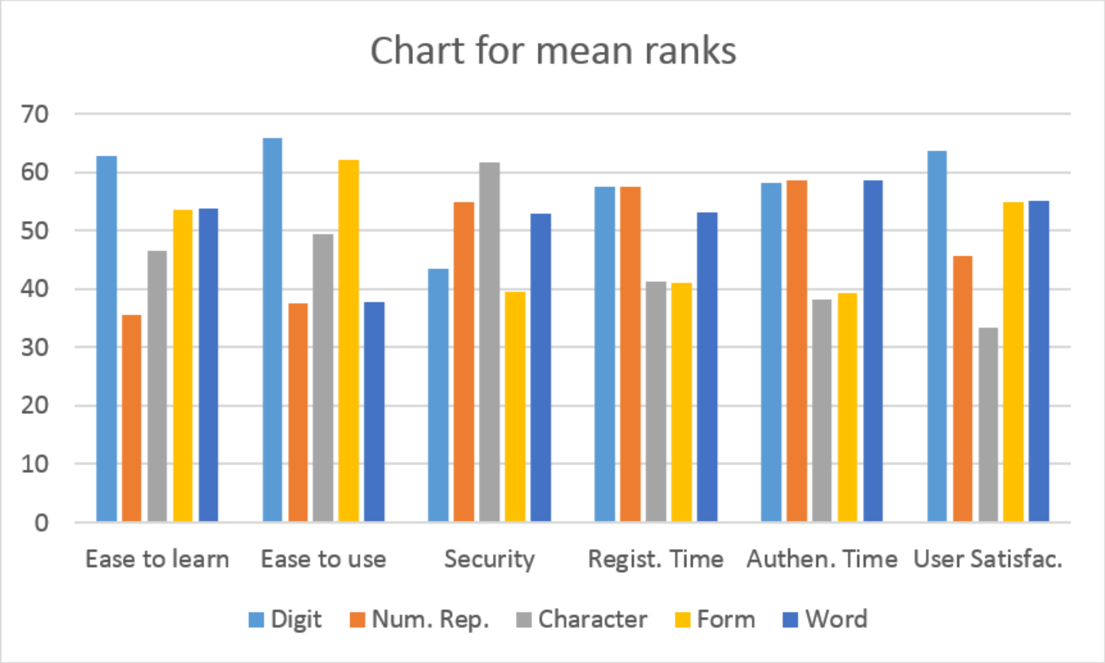


Fig 5.3: Comparison of mean ranks for authentication models (Experiment 3)

5.7 Experiment 4

Purpose: Comparative memorability evaluation for colour, mixed, digit, and word based models

Parameters: Login success rate

This section describes an experiment to evaluate and compare the memorability (retention rate) of four implementations of the property based authentication model. Memorability experiments are normally conducted as part of the usability analysis of a system as memorability is itself a vital part of the usability of a system. However, since memorability evaluations are normally conducted as longitudinal trials (continuous login visitations over a long period of time), it is extremely difficult, if not impossible to conduct memorability evaluations for all ten prototypes of the property based system implementation for a number of reasons. First and foremost, unlike in the usability tests conducted (experiments 1, 2 and 3), where participants are asked to simply create a password and then use the password to login, hence they may be permitted to assess more than one system, a participant conducting a memorability test is only allowed to use a single model for the duration of the experiment. The researcher had to ensure that this is done such that the results are not affected by multiple password interference and the tendency for increased mental pressure on the participants. Secondly, longitudinal trials on memorability are normally conducted over several weeks, or even months, and with other equally significant components of the system to evaluate, devoting too much time on memorability trials may not be worthwhile. Thirdly, many participants consider longitudinal trial extremely boring due to their repetitive nature and may not endure till the end of the experiment, while experimental results need a considerable number to be acceptable. Hence arrangements are made to mitigate the effects of the tendency that participants may decide to drop out of the experiment prematurely [73].

5.7.1 Main Hypotheses

The experiment hypothsises that across the various login sessions, the memorability of at least one of the experimental conditions (models) will be significantly higher than the memorability of the other test conditions.

Ho: That statistically significant variation in login success rate will not be recorded for any of the models under investigation (test conditions)
H1: That statistically significant mean variation in login success rate will be recorded for at least one of the system models under investigation in login session 1.
H2: That statistically significant mean variation in login success rate will be recorded for at least one of the system models under investigation in login session 2.
H3: That statistically significant mean variation in login success rate will be recorded for at least one of the system models under investigation in login session 3.
H4: That statistically significant mean variation in login success rate will be recorded for at least one of the system models under investigation in login session 4.

5.7.2 Research Participants

Twenty five participants are recruited for each of the models under investigation. Participants are drawn from the undergraduate student population of a university. At the end of the experiment, the records of only twenty participants are randomly selected for evaluation, the remaining are discarded as the increased number only helps to safeguard against the premature withdrawals of participants from the experiment. All participants are between the ages of 20 to 35 years of age and each has at least one email and one bank account, hence, each participant has at least one online password and one numerical PIN and thus had an experience in the use of passwords. All participants claimed to have used computers and the internet for between one and six years and were thus all experienced in the use of computers. The use of a student population ensured little disparity in computing expertise and mental capabilities among members of the participant population.

5.7.3 Experimental Design

Here, a between users design was adopted for the experiment in which twenty five participants were recruited and each was allocated one of the four test conditions, which were:

1. A fill (colour) based implementation of the property based scheme.
2. A mixed implementation of the property based scheme.
3. A digit based implementation of property based model.
4. A word based implementation of the property based scheme.

The operational procedures and the interface layout of each of the prototypes is identical with the only difference being in the *factor* with which the authentication is performed. The tasks to be performed by each of the participants on each of the prototypes was also the same. No questionnaires were issued to participants in the conduct of this experiment.

5.7.4 Experimental Variables

The independent variables are the four test conditions (prototype property based models) while the dependent variables are the login success rates logged on to the system during each of four authentication sessions. In this experiment, as in all previous experiments, participants are allowed only to use 2 authentication steps and a fixed grid size of 9.

5.7.5 Apparatus and Materials

- Two ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6” monitor

- Four prototypes of the property based system, identical in every aspect of the design and the tasks/procedures the participants are expected to perform.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

5.7.6 Experimental Procedure

The following procedure was followed in the conduct of the experiment:

In the first authentication session, a participant is expected to create a graphical password using one of the four test conditions (software prototypes). The participant then logs onto the system using the password details chosen in the password creation part. Only data related to the success of user authentication in the different authentication sessions is needed by the researcher. The participant is then asked to return at a later date for the next authentication session. For this experiment, four login sessions were needed for each participant. The first login session is done on the day the password is created. The second login session is done two days after the first login session. The third login session is done a week after the second login session and then the third login session is done two weeks after the third login session. The time is increased gradually to be able effectively measure the variation.

5.7.7 Experimental Results for Experiment 4

The login success rates for the four models under investigation are presented in appendix 4. The results have summarised using excel into table 5.7. The contents of the table have been used to generate the histogram in figure 5.4. From the figure it can be clearly seen that in the first login session participants using the colour model and the digit based model recorded 100% login success. The users of the word based model and the mixed model recorded 95% and 80% success rates respectively. In the second login session, participants using the colour based model and those of the digit based model again recorded 100% success, while users of the word based and mixed models recorded 85% and 70% respectively, this is an overall percentage decline of 10% and 5% from the previous results for both models. In the third authentication session, the digit based model still maintains the 100% lead, while the colour model declines to an overall drop of 5%, the word based model maintains its 85% success rate from the previous session, while the mixed models drops a further overall drop of 5% to reach an overall success rate of 65%. In the fourth authentication session, the digit model again maintains a success rate of 100%, the colour model and the mixed model both lose another Overall 5%, while the success rate for the word based model is maintained at 85% from its drop in login session 2. From this chart it could be seen that only participants in the digit based model could remember their passwords throughout the four sessions of the experiment. The mixed model had the lowest success rate at the beginning of the experiment and had the lowest at the end of the experiment.

	1st Login	2nd Login	3rd Login	4th Login
colour	100	100	95	90
mixed	80	70	65	60
digit	100	100	100	100
word	95	85	85	85

Table 5.7: Data table for login success rates of all models

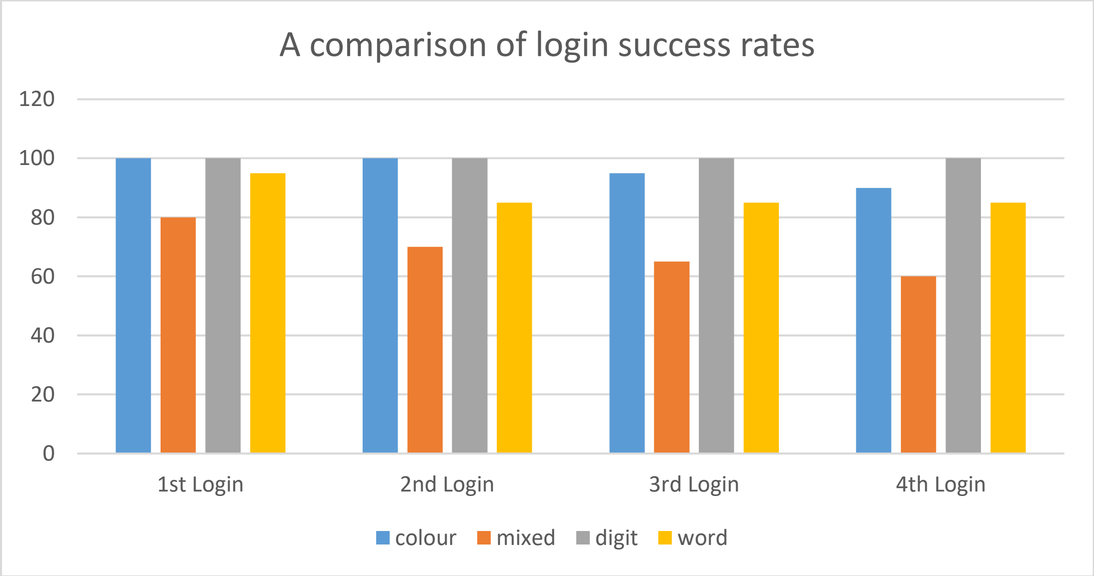


Fig. 5.6: Histogram of comparative success rates of all models

To evaluate the significance in variation of login success rate for all models, a chi-square analysis was conducted. The results for the chi-square test is presented in appendix 4B. From the chi-square test, the case processing summary for all login entries indicates that all values used for the analysis were valid (100%). In comparing the models to the 1st login success rate, the Pearson chi-square value is 9.173 at 3 degrees of freedom, p = 0.027. Phi and Cramer's V indicates a significance value of p=0.027. This shows significant variation between the models in the 1st login session. For the second login session, the chi-square value of 9.8 at 3 degrees of freedom, p=0.022, also indicating significant variation between the models in login success rate. For the 3rd login session, the chi-square value was 10.196 at 3 degrees of freedom, p=0.017, revealing significant success rate variation between the models. In the 4th login session, the Pearson's chi value was 14.902 at 3 degrees of freedom, with p = 0.002.

5.7.8 Discussion of Results for Experiment 4

The results presented in the chi-square tests to test if significant variation between the various software models and the login success rates at each login session to indicate that significant variations do exist between the models in all four login sessions. The result also indicate a gradual increase in the significance between the groups from the 1st login session to the 4th login sessions (from p = 0.27 to p = 0.002). In the light of these results, it is fair to acknowledge that the null hypothesis is thus invalid. Hence significant variations do occur across all four login sessions between the various authentication system prototypes. Hence the null hypothesis that *statistically significant variation in login success rate will not be recorded for any of the models under investigation (test conditions)* has to be rejected while the other four hypotheses that state that statistically significant mean variation will occur in at least one of the conditions in at least one of the login sessions is accepted.

5.8 Experiment 5

Purpose: To determine the effects of grid size on authentication time and to compare results using two models, fill based (colour) and magnitude based (tile)

Parameters: The four grid sizes 2, 3, 4 and 5.

This experiment is designed to investigate the possibility that significant variations in mean authentication time will be observed across the various grid sizes of property based graphical authentication systems. In the course of this project, except where explicitly acknowledged, a fixed grid size of 3 (9 image grid) and step size of 2 (2 authentication steps) have been consistently used as control variables. This has helped in providing some form of control to the allocation of research variables to support the overall consistency of the results in the course of this work. In all the developed prototypes of property based systems, however, there are up to four grid size options to select from. Can the variation in grid sizes, if employed by system users, have any effect on the magnitude of a user's authentication time? Grid size is an important parameter in the calculation of the password space of any authentication system.

5.8.1 Main Hypotheses

The experiment investigates the relation between grid size and authentication time (total login time and average login time). A number of hypotheses in relation to the relationship between the independent variables (grid sizes, 2, 3, 4 and 5) and the dependent variables (total authentication time and average authentication time) have been made. These hypotheses are

> *Ho1: None of the grid sizes will incur significantly greater mean total authentication time than other grid sizes.*
> *H1: That at least one of the grid sizes will incur significantly greater mean total authentication time than the other grid sizes.*
>
> *Ho2: None of the grid sizes will incur significantly greater mean average authentication time than other grid sizes.*
> *H2: That at least one of the grid sizes will incur significantly greater mean average authentication time than the other grid sizes.*

5.8.2 Research Participants

Thirty participants from a university's undergraduate science student population, 18 male and 12 female, were recruited for a between users study of the various grid sizes. All participants were between the ages of 19 and 35 years and each has at least one email and one bank account, hence, each participant has at least one online password and one numerical PIN and thus has an experience in the use of passwords. All participants also claimed to have used computers and the internet for between one and six years and were thus all experienced in the use of computers. The use of a student population ensured little disparity in computing expertise among members of the participant population.

5.8.3 Experimental Design

A within users design was used for the experiment in which thirty participants were recruited and each was asked to create a password and then authenticate himself four times using the colour based model of the system prototype. In each of the four registration and login attempts, the participant selects a different grid size. As each participant uses the same authentication model for each of the four grid sizes, the design, procedure and layout of the system remains the same for all sessions. The only parameter that changes across authentication sessions is the grid size.

5.8.4 Experimental Variables

The independent variables in this experiment are the four grid size (NxN) options: 2, 3, 4, and 5. A grid size of 2 represents 4 images, 3 represents 9 images, 4 represents 16 images and 5 represents 25 images in the image selection grid. The dependent variable are the two timing variables representing the total and average authentication times automatically logged onto the system. The control variable is the number of authentication steps which remained fixed at 2.

5.8.5 Apparatus and Materials

- An ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6" monitor
- A colour based prototype of the property based system installed on the system.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.
- No questionnaires are issued for this experiment.

5.8.6 Experimental Procedure

The experiment was conducted as follows: The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their consent before the conduct of the experiments.

There are basically two operations to be performed at each stage of the experiment on each of the four experimental conditions (four grid sizes) to be used in the experiment. These are subdivided into a number of tasks which include:

1. The registration phase

✓ Click on the "sign up" button

✓ Enter a chosen username in the textbox provided

✓ Select the number of authentication steps to be used in the experiment (which is 2)

✓ Select grid size (2, 3, 4, or 5, depending on the session)

✓ Select image properties for step 1 in the image properties window

✓ Select image properties for step 2 in the image properties window

2. The authentication phase

✓ Enter your chosen username in the textbox provided

✓ Click on the "continue" button

✓ Select image for step 1 in the step 1 image grid

- ✓ Click on the “continue” button
- ✓ Select image for step 2 in the step 1 image grid
- ✓ Click on the “continue” button

The laboratory setting was selected for the experiment for ease of control and to the give the participants the desired isolation in doing the needed tasks without distraction while still using the systems in an environment they are familiar with. Each of the participants was made to undertake the tasks individually interference.

5.8.7 Experimental Results for Experiment 5

A one-way analysis of variance (ANOVA) was performed (Appendix 5) on the data set to compare the means of the dependent variables and to determine the statistical significance of the relationship between the independent variable (four grid sizes) and the dependent variable (total and average authentication times) in the data set. A Tukey post hoc test was done to determine the exact related variables and the statistical significance of the relationship.

From the ANOVA analysis it could be seen that significant mean variation was recorded for both the total login time between groups and the average login time between groups [F(3,116) = 2.744, p=0.046] for both variables. The Tukey post hoc test reveals that the mean login time varies significantly between grid size n=2 (condition 2, M = 17637.60, SD = 15851.669) and n=5 (condition 5, M = 36196.23, SD = 27092.755), p = 0.038 and the mean average login time varies significantly between grid size n=2 (condition 2, M = 8819.10, SD = 7925.849) and n=5 (condition 5, M = 18098.40, SD = 18773.146), p = 0.038. No statistically significant mean variation was recorded for any other pair of experimental conditions.

5.8.8 Discussion of Results for Experiment 5

The details of the results in appendix 5 indicate statistically significant mean variation between the grid size of 2 and the grid size of 5 in both total login time and average login time. Hence both of the null hypotheses (*Ho1* and *Ho2*) that *none of the grid sizes will incur significantly greater mean total and average authentication times than the other grid sizes* had to be dropped. Looking at the results in appendix 5, however, one can observe that the mean total and average authentication times have increase steadily from grid size 2 to grid size 5. The increase between successive grid sizes, i.e., between 2 and 3 (17637.60 and 31383.10), between 3 and 4 (31383.10 and 31557.40) and between 4 and 5 (31557.40 and 36196.23), for the login time, have not been marked to be statistically significant. The same applies to the mean variation in average login time between successive steps 2 and 3 (8819.10 and 15691.87), 3 and 4 (15691.87 and 15778.87), and 4 and 5 (15778.87 and 18098.40).

The grid size of 2 is the smallest grid size with just 4 images and the grid size of 5 is the largest with 25 images. It is thus hypothesized that a significant amount of time variation will be observed between the two variables as it will take more time to locate a user's pass image in the 25 image grid as compared to the 4 image grid.

5.9 Experiment 6

Purpose: Determine the effects of object based ordering of magnitude (tile) based systems on authentication time.

Parameters: login time entries for an ordered, unordered and standard magnitude based system.

For magnitude property based authentication systems, ordering is the act of developing magnitude based systems in which image objects (properties) are arranged in either increasing or decreasing order of magnitude for each image in the system. An ordered system has all images arranged in order of magnitude, an unordered system is a system in which none of the images in the system is ordered, while a standard system contains both ordered and unordered images. This experiment is designed to investigate if the concept of ordering can significantly reduce a user's authentication time.

5.9.1 Main Hypotheses

In conducting this experiment, the following hypotheses are made in relation the user's login time and the 3 experimental conditions:

> *$H_{0:}$ That none of the 3 test conditions will incur statistically significant greater mean login time than the other conditions*
>
> *H_1That at least one of the 3 test conditions will incur statistically significant greater mean login time than the other conditions.*

5.9.2 Research Participants

Forty university undergraduate computing science students, 28 males and 12 females were recruited for a within users study of the 3 test conditions; the ordered, the unordered and the standard magnitude based authentication models. All participants were between the ages of 19 and 35 years of age and each had at least one email and one bank account, hence, each participant had at least one online password and one numerical PIN and thus had an experience in the use of passwords. All participants claimed to have used computers and the internet for a number of years and hence were all experienced in the use of computers. The use of a student population ensured that the disparity in skill, proficiency and understanding as well as computing skill among members of the participant population was small.

5.9.3 Experimental Design

A within users design was used for the experiment in which forty participants were recruited and each was allocated the three test conditions which were:

1. An ordered implementation of the magnitude (tile) based model. (see section 3.8)
2. An unordered implementation of the magnitude (tile) based model.
3. A standard implementation of the magnitude (tile) based model.

The operational procedures, interface design and layout of each of the prototypes was identical with the only difference being that the images were from one of the three test conditions. Each participant was to use all three of these systems. The tasks to be performed by each participants on each of the prototypes was also the same.

5.9.4 Experimental Variables

The independent variables are the three implementations of the magnitude based model (ordered, unordered and standard) being investigated in the experiment. The dependent variable is the total login time logged onto the system in each implementation.

5.9.5 Apparatus and Materials

- Three hp pavilion laptop PCs running windows 10, 6. 00 GB RAM and 15.6” monitor
- The laptops run the three prototypes of the magnitude based model, identical in every aspect of the design and the tasks/procedures the participants are expected to perform.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

- No questionnaires are used in the conduct of this experiment.

5.9.6 Experimental Procedure

The following procedure was followed in the conduct of the experiment:

The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their consent before the conduct of the experiments. Each participant tests each of the three test conditions. All three conditions are installed on each of the PCs.

There are basically two operations to be performed at each stage of the experiment on each of the three experimental conditions to be used in the experiment. Each participant registers onto the system in the first instance, and the logs onto the system. These are subdivided into a number of tasks which include:

1. **The registration phase**

✓ Click on the “sign up” button
✓ Enter a chosen username in the textbox provided
✓ Select the number of authentication steps to be used in the experiment (which is 2)
✓ Select image properties for step 1 in the image properties window
✓ Select image properties for step 2 in the image properties window

2. **The authentication phase**

✓ Enter your chosen username in the textbox provided
✓ Click on the “continue” button
✓ Select image for step 1 in the step 1 image grid
✓ Click on the “continue” button
✓ Select image for step 2 in the step 1 image grid
✓ Click on the “continue” button

The laboratory environment was selected for the experiment for control and serenity. Each participants worked on all three test conditions.

5.9.7 Experimental Results for Experiment 6

The experimental results were collected and a one-way analysis of variance (ANOVA) was performed on the dataset (Appendix 6) and the analysis did not show any statistically significant mean variation between groups [F(2, 117) = 2.932, p = 0.57]. A Tukey post hoc analysis, however, shows significant variation between the ordered (model 11, M = 25086.03, SD = 18093.535) and the unordered (model 12, M = 37277.15, SD = 23347.476), p = 0.047.

5.9.8 Discussion of Results for Experiment 6

Although the ANOVA analysis did not reveal significant mean variation between any of the groups, the Tukey post hoc analysis did reveal that significant mean variation does occur between the ordered and the unordered pairs of magnitude based systems. The results indicate that the participants' login time was less in the ordered implementation than in the unordered implementation. Thus the null hypothesis that *none of the 3 test conditions will incur statistically significant greater mean login time than the other conditions* does not hold as a statistically significant variation in mean login time exists between the models. The main reason for this is that the human brain is engineered towards a 'goal oriented search', and it is established that sorting (ordering) can very much enhance search performance [147]. Hence the ordering process has made it easier for the participants in the ordered model than in the unordered model.

5.10 Experiment 7

Purpose: To determine the effects of organised image selection on authentication times of users in the word based model

Parameters: Compare mean login (authentication) times of each user's login session for four forms of organised image selection (standard spelling, ordinal spelling, fixed lettering and ordered lettering) and the random selection for the word based authentication model.

In the word based model, there are a number of ways a user can 'organise' the way his word based password is being selected and used. There are several 'styles' of organised image selection. A detailed explanation of the meaning and methods of organised image selection for a word based model are presented in *Appendix 7B.* The concept of organised image selection is introduced in the quest to improve password memorability. In this experiment, participants are asked to create several passwords on a word based authentication system, each time adopting one of the various 'styles' of organised image selection. The login time incurred between sessions while adopting these styles is computed and analysed for significant mean variation against randomized image selection.

5.10.1 Main Hypotheses

The experiment is aimed at understanding if significant mean variation will be established between the random selection style (condition 5 of the experiment) and any of the organised conditions (1, 2, 3 or 4). Hence, the following hypotheses are made:

> *H_0: That the random selection (condition 5) will not incur significantly greater mean login time than any of the organised selection styles (conditions 1, 2, 3 or 4).*
>
> *H_1: That the random selection (condition 5) will incur significantly greater mean login time than at least one of the organised selection styles (conditions 1, 2, 3 or 4).*

5.10.2 Research Participants

Fifteen computer science undergraduate students were recruited for a within users study of the five experimental conditions (selection styles). The participants were all between the ages of 22 and 35, and each has at least one email and one bank account. Each participant hence has at least one online password and one numerical PIN and is experienced in the use of passwords. All participants claimed to have used computers and the internet for at least 3 years and were thus all considerably skilled in the use of computers.

5.10.3 Experimental Design

A within users design was used for the experiment in which fifteen participants were recruited and each participant was asked to create a passwords with each of the five styles of user password selection to for the word based model as test conditions. The styles are:

1. Standard Spelling. (see section 3.11)
2. Ordinal Spelling.
3. Fixed Lettering.
4. Ordered Lettering.
5. Random Selection.

The operational procedures and interface for each selection style remained the same, with the only difference being the *format* of password selection. The tasks to be performed by each of the participants on each of the password selection styles was the same.

5.10.4 Experimental Variables

The independent variables are the five password selection styles of the word based model being investigated in the experiment. The dependent variable is the registration (login) time that is captured by the system. The control variables are the grid size and number of authentication steps. No questionnaire was used in this experiment.

5.10.5 Apparatus and Materials

- An ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6" monitor
- A prototype implementation of the word based authentication system installed on the system.
- A consent form to ensure participant's informed consent.

*** No questionnaires are issued for this experiment.

5.10.6 Experimental Procedure

The participants were recruited by means of a recruitment form. A consent form was provided to each of the participants to sign and confirm their informed consent before the conduct of the experiments. A participant is expected to adopt one of the selection styles provided (experimental conditions) and to perform the two operations (1) create a password using one of the styles, (2) login to the system using the password he has created in (1). Each participant tests all the five experimental conditions one at a time.

These two operations are each divided into a number of tasks, however, the experiment is only interested in the login data, i.e., data collected for the 2nd (authentication stage). The stages are:

1. **The registration (password creation) stage**

✓ Click on the "sign up" button
✓ Enter a chosen username in the textbox provided
✓ Select the number of authentication steps to be used in the experiment (which is 2)
✓ Select image properties for step 1 in the image properties window
✓ Select image properties for step 2 in the image properties window

2. **The authentication stage**

- ✓ Enter your chosen username in the textbox provided
- ✓ Click on the "continue" button
- ✓ Select image for step 1 in the step 1 image grid
- ✓ Click on the "continue" button
- ✓ Select image for step 2 in the step 1 image grid
- ✓ Click on the "continue" button

The system logs timing data for both stages, the timing data for the authentication stage shall be used in the analysis of the experiment and the evaluation of its findings.

5.10.7 Experimental Results for Experiment 7

A one-way analysis of variance (ANOVA) was performed on the login data generated from system logs (Appendix 7). The ANOVA results showed no statistically significant variation of means between groups for the login time [F(4, 70) = 1.589, p=0.187]. The Tukey post hoc analysis also shows no significant mean variation between any pair of the various image selection styles investigated in this experiment.

Although the post hoc analysis shows no significant mean variation between the random selection (condition 5) and any other style (conditions 1 to 4), condition 5 still has the highest mean of all the styles. This shows that it on average, it took longer for participants to login using condition 5 compared to all other selection styles. The variation in the mean time it took to login between all the models is just not statistically significant.

5.10.8 Discussion of Results for Experiment 7

In spite of the expected significant mean variation between the random selection and the other 'organised' selection styles, the ANOVA analysis and Tukey post hoc analysis both suggest to the contrary. Hence the results confirm the null hypothesis that *that the random selection (condition 5) will not incur significantly greater mean login time than any of the organised selection styles (conditions 1, 2, 3 or 4).* This is the analysis of the results available at the moment. Since the condition 5 has the highest mean login time, and the difference between the mean in condition 5 and the largest mean in the 'organised' conditions (condition 4) is much larger than the difference between any two means among the organised conditions, the results may change with a larger participant population size. This is however left for future experiments

5.11 Experiment 8

Purpose: Determine the effects of organised image selection on authentication time in concentric fill based model.

Parameters: authentication time for organised image selection for fill based (colour) model. The conditions are: 1 (Inward painting), 2 (Outward painting), 3 (Fixed painting) and 4 (Random painting).

As in experiment 7, this experiment (experiment 8) was conducted to determine if significantly significant mean variations will exist in login times between the random image selection style and the 'organised' image selection styles of the fill based (colour) model. A detailed explanation of the meaning and procedure of organised image selection for a concentric fill based model is presented in *appendix 8B*. The concept is developed to improve memorability for concentric fill based models.

5.11.1 Main Hypotheses

This experiment is aimed at investigating if statistically significant mean variation will exist in login times between the various organised image selection styles of a concentric fill based model when compared to the random selection (condition 4, random painting). Here, the following hypotheses are made:

> *H_0: That there will be no difference in mean login time between the random painting (condition 4) and any of the organised selection styles (conditions 1, 2 or 3).*
>
> *H_1: That there will be significantly greater mean login time for the random painting (condition 4) than at least one of the organised selection styles (conditions 1, 2 or 3).*

5.11.2 Research Participants

Fifteen undergraduate science students were recruited for the within users study of the four authentication styles for the colour based model. All participants were between the ages of 22 and 35 years of age and each had at least one email and one bank account. Hence, each participant had at least one online password and one numerical PIN and thus had an experience in the use of passwords. All participants claimed to have used computers and the internet for between one and six years and were thus all experienced in the use of computers.

5.11.3 Experimental Design

A within users design was used for the experiment in which fifteen participants were recruited and each asked to log on to the system using each of the various image selection styles (experimental conditions) which were:

1. Inward painting (see section 3.11)
2. Outward painting
3. Fixed painting
4. Random painting

The operational procedures and interface layout of each of the selection styles are identical. The tasks expected of each of the participants are also identical for each of the image selection styles. Each participant is expected to create a password and authenticate using each of the various image selection styles (run all 4 conditions).

5.11.4 Experimental Variables

The independent variables for this experiment are the various image selection styles (conditions 1, 2, 3, and 4), while the dependent variable is the authentication (login) time. Control variables are the number of authentication steps which is fixed at 2 and the grid size, which is fixed at 3 (9 images). No subjective opinion data was generated for this experiment.

5.11.5 Apparatus and Materials

- An ASUS N55s laptop PC running windows 10, 6. 00 GB RAM and 15.6” monitor
- An installed copy of the concentric fill (colour) based authentication system on which the experiment to use the four selection styles will be conducted.
- An information sheet that provides the participants with information about the experiment and what they are expected to do.

** No post experiment questionnaire is issued for this experiment.

5.11.6 Experimental Procedure

As in experiment 7, the participants were recruited by means of a recruitment form. A consent form is also used to confirm the consent of participants before the conduct of the experiment. A participant is expected to adopt each of the selection styles (experimental conditions) provided in turn and to perform each of the two stages (1) create a password using one of the styles, (2) login to the system using the password created in (1).

These two operations are each divided into a number of tasks, however, the experiment, as in experiment 7, is only interested in the login data, i.e., data collected for the 2nd (authentication stage). The stages are:

1. **The registration (password creation) stage**

✓ Click on the "sign up" button
✓ Enter a chosen username in the textbox provided
✓ Select the number of authentication steps to be used in the experiment (which is 2)
✓ Select image properties for step 1 in the image properties window
✓ Select image properties for step 2 in the image properties window

2. **The authentication stage**

✓ Enter your chosen username in the textbox provided
✓ Click on the "continue" button
✓ Select image for step 1 in the step 1 image grid
✓ Click on the "continue" button
✓ Select image for step 2 in the step 1 image grid
✓ Click on the "continue" button

The system logs timing data for both stages, the timing data for the authentication stage shall be used in the analysis of the experiment and the evaluation of its findings.

5.11.7 Experimental Results for Experiment 8

A one-way analysis of variance (ANOVA) was conducted on the login time data (experimental results) and the results are presented in appendix 8. ANOVA indicates that statistically significant variation exists between groups [F(3, 56) = 6.183, p=0.001]. Tukey post hoc analysis (multiple comparisons) indicates statistically significant mean variation between outward painting (condition 2, M = 15270.53, SD = 5450.910) and random painting (condition 4, M = 25634.47, SD = 6598.242), p=0.003 and between fixed painting (condition 3, M = 15363.13, SD = 8314.870) and random painting (condition 4, M = 25634.47, SD = 6598.242), p=0.004. The result thus clearly indicates that statistically significant mean variation in login time exists between condition 2 and condition 4 and between condition 3 and condition 4.

5.11.8 Discussion of Results for Experiment 8

Unlike in experiment 7, the results for experiment 8 indicate that statistically significant mean variation does exist between the random selection style (condition 4) and two of the 'organised' selection styles (outward painting and fixed painting, conditions 2 and 3). The results contradict the null hypothesis and confirm the hypothesis that *the random painting selection style (condition 4) will incur significantly greater mean login time than at least one of the organised selection styles (conditions 1, 2 or 3).* Hence the belief that organised image selection for fill based models may greatly reduce a participant's authentication time is justified.

5.12 Conclusion

This chapter discusses usability issues and the main usability experiments conducted as part of this research project. It also discusses the corresponding results obtained from the experiments and the way the data is analysed. Although not explicitly stated, the chapter is divided into three distinct parts, each providing insight into the concept of usability as it relates to property based systems and the entire concept of graphical authentication.

The first part consists of the first two sections of the chapter that provide a highlight on the concept of usability and its place in the field of human computer interaction. Table 5.1 provides a generalized guideline on the relationship between the various components of usability in the setting of a graphical authentication system, how data is organised within each system, and how it is collected and evaluated to reflect the measures of effectiveness, efficiency and user satisfaction embodied in each authentication system.

The second part consists of sections three to section seven (experiments 1 to 4). This sections provide the details of all the experiments conducted on the idea of a novel hybrid property based system for user authentication. Section three discusses some preliminary work conducted to give the researcher some insight into the workability and user experience on the concept of property based authentication. Sections four to seven discuss experiments conducted to provide information on the efficiency, effectiveness and user opinion on the concept of property based authentication. Within these sections, a lot of comparison has been made between various implementations of the property based paradigm to understand the various similarities and differences that exist within the systems in relation to user registration time, authentication time, user satisfaction, login failure rate, and other usability evaluation metrics as part of the fundamental usability evaluation of all authentication systems.

The third part consists of sections eight to eleven (experiments 5 to 8) that deal specifically on some novel concept related to the concept and design of property based authentication. Section eight evaluates the effect of grid size on authentication time, section nine evaluates the influence on order on authentication time for magnitude based systems, while sections ten and eleven evaluate the idea of organised image selection as it relates to the word based and fill based authentication systems.

Having gone through these sections, one will understand that the chapter as answered all enquiries related to the research question of whether or not the idea of property based authentication is applicable as a novel system of user authentication and if it can effectively meet the usability and design needs of system users. Property based authentication is indeed a promising concept in user authentication systems as demonstrated by the numerous experiments and very much caters to the usability needs of system users.

The next chapter shall discuss the security experiments conducted as part of this research work. Several experiments were conducted to evaluate the vulnerability of these systems to observational attacks simple guessing attacks and vulnerability to verbal and written description. These experiments are performed to evaluate the strengths of the systems considering security issues that have direct bearing on the part of the user.

Chapter Six – Security Evaluation of Property Based Models

6.1 Introduction

Security vulnerabilities such as shoulder surfing, the tendency for guessing attacks and the ability of passwords to be written down, stolen or communicated to others have been the serious issues that have hindered the effective use of alphanumeric passwords. Graphical passwords were thus suggested as alternatives to text based passwords. Graphical passwords are believed to be far more secure than alphanumeric passwords as they are less likely to be transmitted verbally or in writing, and are less prone to shoulder surfing and guessing attacks. In fact, these have been the motivating factors in the proliferation of graphical passwords as alternatives to text based passwords. Research has, however, discovered the tendency that images in some graphical schemes can be effectively described. Whenever descriptions are possible, there is that tendency of launching both guessing and social engineering attacks. Although considered far better than textual passwords, most recognition based graphical passwords are also prone to shoulder surfing attacks and this has been studied in numerous literature.

This chapter evaluates and discusses the security vulnerabilities of the property based graphical authentication scheme. In particular, the vulnerabilities of the systems to guessing attacks, shoulder surfing attacks and the ability to describe images in various implementations of the system were investigated. We are particularly interested in these vulnerabilities as they are the ones that present the system user as the weakest link in the security chain [4]. .Although investigations into the vulnerabilities of graphical authentication systems to description and guessing attacks have not been explicitly performed in existing literature, a number of studies exist in which verbal and written descriptions are studied as motivations for guessing attacks [16]. The procedure for these experiments takes its cue from these investigations. The aim is to ascertain the strengths and weaknesses of the implementation of property based algorithms in relation to attacks on the user side.

6.2 Security Metrics

The security metrics are those items used to determine the extent to which the system is able to withstand unwanted attacks. According to [71], these metrics include:

Guessability: This is the ease with which a user's password can be guessed correctly. The success of dictionary and brute force attacks are generally used to determine the guessability of user password. While the intruder tries all possible combinations of passwords in a brute force attack, a dictionary attacks is only possible if there is a pattern of predictability, which can be used to organise a dictionary of expected passwords.

Observability: This is the tendency of having someone observe a user's login activity as he logs on to his system. The human observer can keenly observe as the user enters his password on the system (shoulder surfing), try to capture the actions with a technical equipment (through filming) or the use of hardware or software.

Recordability: This metric deals with the ability to share passwords. The first category of these arises when someone writes his password down and it is eventually leaked to or stolen by someone else. Other means include using dubious means (social engineering) to get a user to disclose his password to others.

6.3 Analysis of Shoulder Surfing for Prototype Set 1

Shoulder surfing remains the greatest challenge facing existing graphical authentication systems that is believed to have made it difficult to address the usability and security contention in most authentication systems [148]. This section aims to analyse the vulnerability of various implementations (set 1) of property based authentication systems to the problem of shoulder surfing and to help understand if the factor of authentication in property based scheme can affect such vulnerability. The first set (set 1) of the property based authentication implementations comprise of four *'fill based models'*, which include the colour based model, the pattern based model, the mixed model, and the butterfly model, and a magnitude based model (called the 'broken tile'). This experiment is aimed at helping to understand if the number of authentication steps used in each implementation as well as the number of authentication rounds performed can increase the risk of shoulder surfing among the various implementations for set 1. Three tests are performed to analyse the login failure rates of keen observers as the researcher uses a chosen password to authenticate on each of the developed prototypes under the various authentication configurations. The login failure of a keen observer is an indication of the security of the system. In doing this, the researcher borrows from shoulder surfing experiments performed in [16, 18].

The experiment seeks to:

1) Determine the variation in the level of shoulder surfing vulnerabilities in the one-step authentication configuration for all property based implementations (Set 1) and determine if these variations are statistically significant.

2) Determine the variation in the level of shoulder surfing vulnerabilities in the two-step authentication configuration of all property based implementations (Set 1) and determine if these variations are statistically significant.
3) Determine the variation in the level of shoulder surfing vulnerabilities in the two rounds and two steps configuration of all property based implementations (Set 1) and determine if these variations are statistically significant.

Hence, with the configurations, the experiment seeks to help understand if any correlation exists between vulnerabilities in each of the three test conditions and the various implementations of the property based system and if the correlation is statistically significant.

6.3.1 Experimental Variables

Since the research seeks to determine the variation in the observation failure rates between the one step, two step and two-step two rounds configuration among all models, the various implementations of the authentication models serve as the independent variable, the login failure rate is the dependent variable, while the authentication configurations are control variables.

6.3.2 Research Participants

All participants were university students between the ages of 18 and 35. They all have experience in the use of passwords and PINs. All the participants claim they have never interacted with a picture based password. The study was conducted as a laboratory experiment in a within subject design, in which each student was allowed to observe authentication on any one of the system prototypes. The participants were randomly allocated to one of the authentication test configurations. For the sake of comparison and data analysis, the researcher ensured that the same number of participants was used for each of the test cases. The number of participants for each test case was 75, that is, 15 participants per authentication system.

6.3.3 Experimental Procedure

The experiments were organized in a laboratory environment and each participant was treated individually. The choice of a laboratory environment was to allow the participants feel as comfortable as possible while working in an environment they are already used to and without external distraction. On arrival, each participant was issued a consent form to sign and given an information sheet that explains the purpose of the experiment and the role of the participants in the conduct of the experiment. The participant is then given the data form on which he enters demographic information including his name, age, sex, and level of studies. The data form is also used to collect the participant's success or failure in being able to succeed in guessing or observing the password of the researcher.

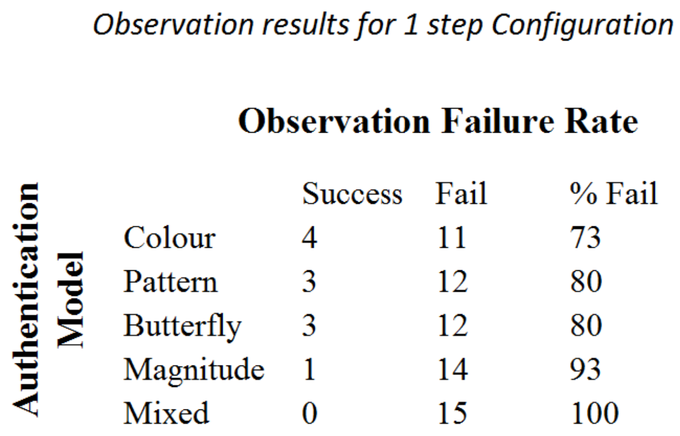
The participant then receives a brief orientation on the layout and authentication procedure of the property based authentication system prototype he is going evaluate. The participant is then asked to play the role of an attacker who keenly observes the data entry of a 'victim', which is played by the researcher. The researcher aims to provide the best conditions for shoulder surfing, hence, the participant may choose between a sitting position, in which he sits on a chair next to the supposed victim while the victim authenticates, and a standing position, where he stands about 30 centimetres behind the supposed victim while the victim authenticates onto the allocated system. This is the same procedure that has been used in other investigations on the shoulder surfing attack [16]. In each of the experiments, the supposed attackers (the participants) are asked to focus their attention keenly on the screen while the authentication takes place. No tasks were given to participants between the observations and the supposed attacks. As in [16], however, the participants were permitted to take notes and are provided with the necessary aid to do so if they so wish. The researcher uses a data entry form to capture the attack success or otherwise. The three authentication configurations under investigation include:

- ✓ A one-step single login configuration of any of the five authentication models.
- ✓ A two-step single login configuration of any of the five authentication models
- ✓ Two step dual login authentication of the two step configuration of any of the authentication models under investigation

At the end of each participant's authentication login, the experimenter enters a ✓ into the data entry form for a correct guess to indicate successful attack and an ✕ for an incorrect guess. This is done for every user login throughout the experiment.

6.3.4 Results for 1 Step Single Login Authentication

Seventy five (75) participants, fifty one (51) males and twenty four (24) females participated in the test for the 1 step configuration. The results are displayed on table 6.1.



Observation results for 1 step Configuration

Observation Failure Rate

Authentication Model		Success	Fail	% Fail
	Colour	4	11	73
	Pattern	3	12	80
	Butterfly	3	12	80
	Magnitude	1	14	93
	Mixed	0	15	100

Table 6.1: Success and failure rates for 1 step single login authentication

The table has three data columns for the number of observation successes, the number of observation fails and the fail percentage. From the table, it can be seen that the colour based model had the highest success rate of 4 successes and 11 fails in the 15 trials in the experiment. This gives the colour model a 73% failure rate. The pattern based and butterfly models each had 3 successes and 12 fails each, giving each an 80% failure rate. The magnitude model had 1 success and 14 fails in the 15 trials, giving it a 93% failure rate for the one-step configuration. While the mixed model had no successes in all 15 attempts, giving it a 100% failure rate.

From this results, the histogram on figure 6.1 is constructed. The histogram is a plot of the number of login failure and success rates. This results are somewhat consistent with the user opinion data collected in the usability tests for these same models in experiment 2. In these data, the mixed model scored the lowest in ease of use and ease to learn, but highest in user opinion on security. The colour and butterfly models scored the highest in user satisfaction, where the colour model scored the lowest in terms of security

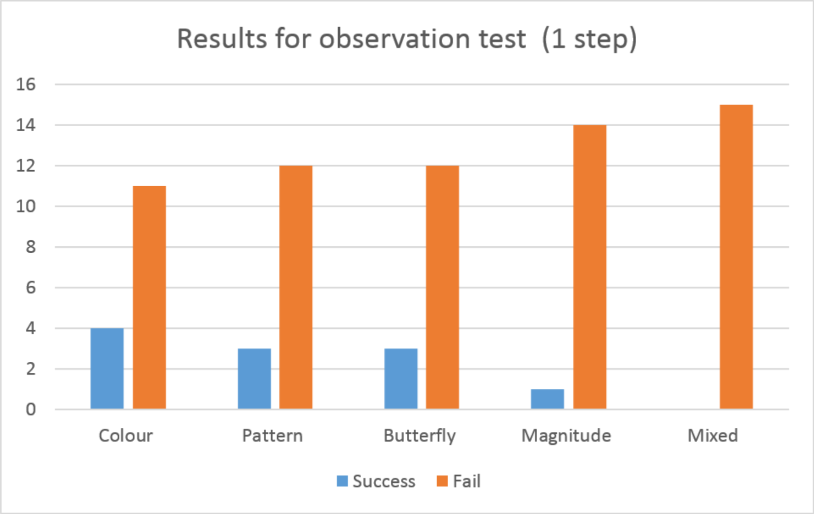
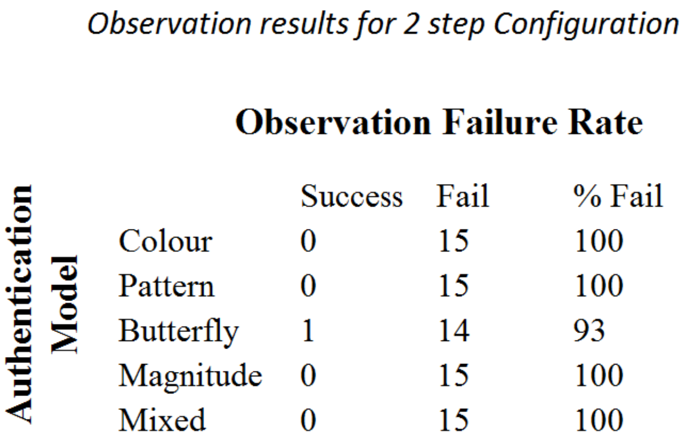


Fig. 6.1: Observation chart for 1 step single login

6.3.5 Results for 2 Step Single Login Authentication

The second test consists of the observability test for the 2 step single login configuration of each of the authentication models (set 1). The results are summarized in table 6.2. Seventy five (75) participants participated in the trial for the 2 step login configuration. From the table, it could be observed that although the colour based model had the lowest fail percentage in the 1 step configuration, it now records no observation success in the 2 step login configuration, just like 3 other models (pattern , magnitude and mixed). The butterfly model was the only model that recorded a single authentication success in its 15 trials in the two step configuration, giving it a 93% login observation failure rate. The score of this test is also plotted on the histogram in figure 6.2.



Observation results for 2 step Configuration

Observation Failure Rate

Authentication Model		Success	Fail	% Fail
	Colour	0	15	100
	Pattern	0	15	100
	Butterfly	1	14	93
	Magnitude	0	15	100
	Mixed	0	15	100

Table 6.2: Success and failure rates for 2 step single login authentication

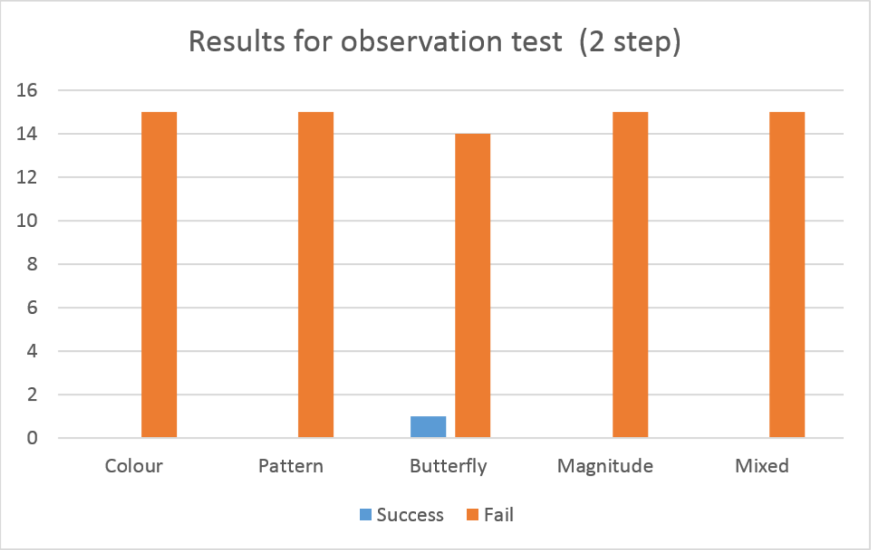
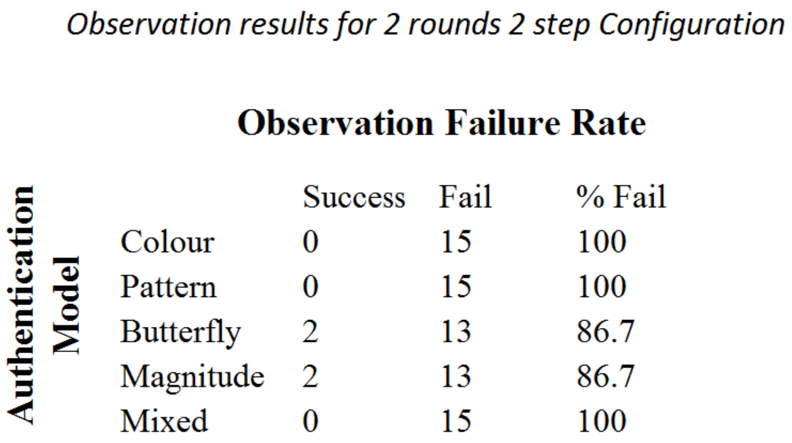


Fig. 6.2: Observation chart for 2 step single login authentication

6.3.6 Results for Dual Login Authentication

The observation tests for a dual login configuration are performed. These are performed such that the participant (the supposed hacker) observes two consecutive authentications logins in a succession. Seventy Five (75) participants conducted the observations for the two rounds configuration. The results are outlined in table 6.3. From this table it could be observed that only the butterfly and magnitude models were successfully hacked by two of the fifteen participants assigned to each of the models, giving both models an 86.7% fail percentage as compared to the rest of the models that still remained with 100% fail percentage. The results in the table are translated into the chart in figure 6.3.



Observation results for 2 rounds 2 step Configuration

Observation Failure Rate

Authentication Model		Success	Fail	% Fail
	Colour	0	15	100
	Pattern	0	15	100
	Butterfly	2	13	86.7
	Magnitude	2	13	86.7
	Mixed	0	15	100

Fig. 6.3: Results for dual login observation test

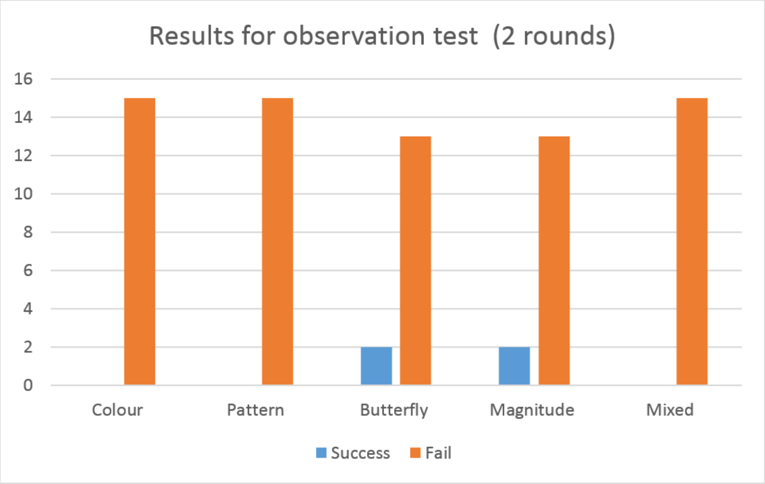
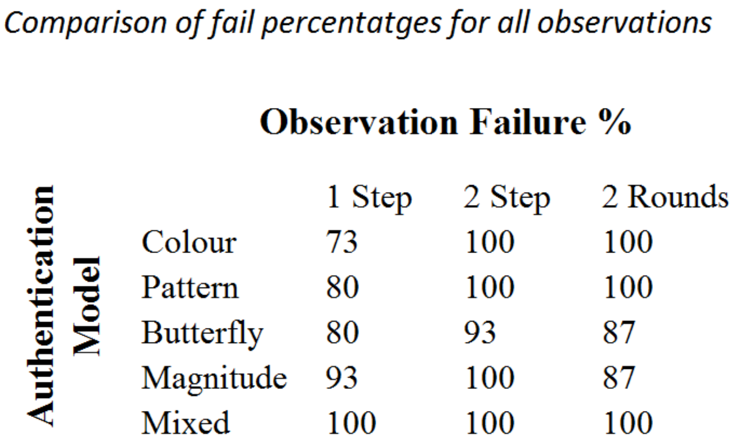


Fig. 6.3: Observation chart for dual logins authentication

6.3.7 Comparison of Results for Vulnerability Test

The results of fail percentages in the 1 step login, 2 step single login and dual login authentication configurations for each model are combined for comparison to form table 6.4, and used to obtain the histogram on figure 6.4.



Comparison of fail percentatges for all observations

Observation Failure %

		1 Step	2 Step	2 Rounds
Authentication Model	Colour	73	100	100
	Pattern	80	100	100
	Butterfly	80	93	87
	Magnitude	93	100	87
	Mixed	100	100	100

Table 6.4: Percentage failure rates for 1 step single, 2 steps single and dual login authentication

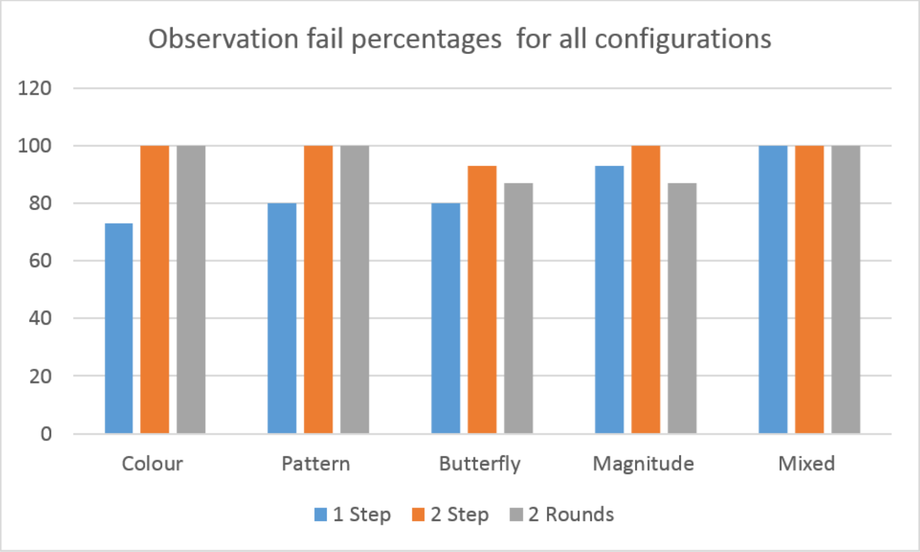


Fig. 6.4: A comparison of observation fail percentage for 1 step, 2 steps and dual login authentication

6.3.8 Discussion of Results for Observability Tests

The percentage failure rates presented in table 6.4 and figure 6.4 present a glaring image of the vulnerability of the various implementations of the property based authentication model to observational (shoulder surfing) attacks. Of all models, only the mixed model maintained a 100% failure rate for all configurations. As mentioned earlier, this is consistent with user opinion data collected in usability tests performed for these models, as the mixed model was rated the highest in security.

A chi square test conducted on results for each of the three configurations reveals that there is no correlation between authentication models and login failure rate $X^{(4)}$ = 5.753, p = 0.218 for 1 step authentication, $X^{(4)}$ = 4.054, p = 0.399 for 2 step single login and $X^{(4)}$ = 6.338, p = 0.175 for dual logins. Hence no correlation exists between the authentication models and login failure or success rate.

6.4 Predictability Test

Predictability tests are tests conducted to ascertain the predictability of password systems. Predictability has been an important issue in the use of text based passwords as user's select passwords they can very easily remember, but which are highly predictable [60, 130]. Considerable research has been conducted in trying to understand the guessability of image passwords and measures that can be taken to reduce such vulnerability [84]. The research on guessability has, however been focused on the provision of cues which may assist an attacker in his ability to guess a user's password. Such cues include the use of mnemonics [17, 73] and the use of verbal and written descriptions of a user's image portfolio [84]. Researcher in [46] also conducted research on measures that could be employed to suppress the ability to guess face-based passwords from verbal and written descriptions.

In this research, experiments are performed to ascertain the guessability of property based passwords. As in existing research [17, 84], the researcher investigate the possibility of launching a guessing attack on a property based system using some 'hint'. The hint selected for use in the work is 'favourite colour' or 'favourite number'. The experiment was motivated by the belief of some research participants during previous experiments that understanding a user's favourite colour or number can make a property based password guessable. Although suggestions were brought forward to first look into the possibility of succeeding with what can normally be called a 'blind guess' on property based systems, the idea was not considered due to timing constraints. A blind guess can be considered as a guessing attack launched solely from predictions made by the attacker himself. This is contrary to what can be called a 'hinted guess', a guessing attack launched when some form of a clue or 'hint' has been provided for the attacker by the user about the content of his password. It is, however, highly unlikely that a totally blind guess will succeed on a property based system, as this type of attack is only possible if predictable patterns can be observed in the use of a password system.

6.4.1 The Guessability Test

Considerable work has been done in existing literature on a guessability of image passwords [17]. This research takes its cue from those projects. In this work, a user creates a password with one of the implementations of the property based paradigm. The user ensures that for both the first and second steps of his password selection, he had selected the 'favourite' feature (either 'favourite colour' or 'favourite number', depending on the system implementation) as part of the properties for his image password. Five models were selected for this test; these include the colour, the magnitude, the mixed, the digit and the representation based models. These represent three 'favourite colour' and two 'favourite number' models.

6.4.2 Experimental Variables

The experiment seeks to understand if any correlation exists between the authentication models being examined and the login failure rate for a guessing attack if the user's favourite colour or favourite number have been given away. Hence the dependent variable is the login failure rate, while the independent variables are the models being examined. The number of authentication steps and the size of the image selection grid are control variables. In each of the experiments, the number of steps for authentication is 2, while the grid size (a number (NxN) which represents the number of decoy images + the user's password image) is chosen as 3. This gives 9 as the number of images to select from in each grid.

6.4.3 Research Participants

All participants were university undergraduate students between the ages of 20 and 35. They were all studying either computer science, mathematics or statistics. They all have experience in the use of passwords and PINs. All the participants claim they have never interacted with a picture based password. The study was conducted as a laboratory experiment in a between subject design, in which each student was allowed to observe authentication on any one of the system prototypes. The participants (the 'victims' and the 'attackers') were randomly allocated to the authentication systems which they used. For ease of comparison and data analysis, the researcher ensured that an even number of participants was used for each of the test cases. Twenty (20) participants were allocated to each of the authentication systems to act as victims, hence another twenty were allocated to act as the attackers.

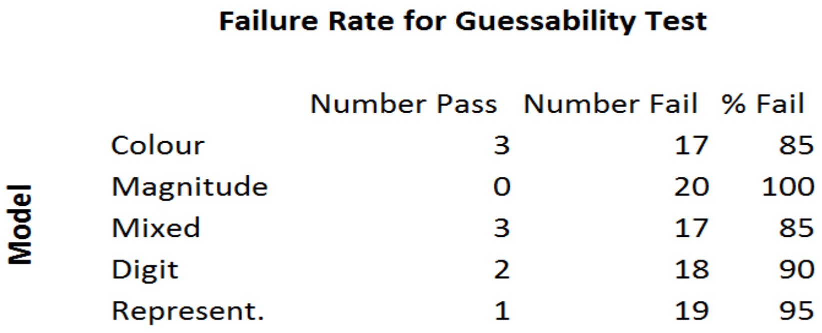
6.4.4 Experimental Procedure

The experiment was conducted in a laboratory setting. The participants were grouped according to the manner in which they arrived. On arrival, the participants are taken through some form of training on procedure for password creation in the specific authentication system they will use for the research. This is to orient the participants on the use of the system and for the attackers to know where to look at when the hints are provided. In this experiment, the researcher chose not to act as the 'victim' so as to allow for a wider range of choices from the 'password creator' participants, which in turn will reflect the multiplicity of password choices in the real world.

One of the participants is then asked to create a password on the system using either his favourite colour or favourite number, depending on the specifics of the systems being used. At this time, the other participant stands or sits at a location from which the password creation process will not be visible to him. After successful password creation and single login entry by the 'victim' participant, he lets out the favourite number or colour he has used in his password creation and allows the 'attacker' to take his seat and try to guess the password. A data entry form is used to capture correct and incorrect guesses. A ✓ is entered into the data entry form for a correct guess and an ✕ for an incorrect guess. This is repeated for every victim-attacker pair throughout the experiment.

6.4.5 Results for guessability test

One hundred students participated in the guessability test. The results for the number of login success and failures for the guessability test are presented below.



Failure Rate for Guessability Test

		Number Pass	Number Fail	% Fail
Model	Colour	3	17	85
	Magnitude	0	20	100
	Mixed	3	17	85
	Digit	2	18	90
	Represent.	1	19	95

Table 6.5: Success and failure rates for guessability test

From the table it can be seen that in the 20 participant allocated to each of the models, the colour model and the mixed model each recorded three successes, the digit model recorded 2 successful logins, the number rep. model recorded one successful login, while the magnitude model recorded no successful login entry. The fourth column of the table contains the login failure percentage of each of the models. From here, it can be seen that the highest login failure percentage goes to the magnitude model which has 100%. The magnitude model is next with 95%, then the digit model with 90% and then the colour and mixed models with 85% each. The data in the table is represented in figure 6.5

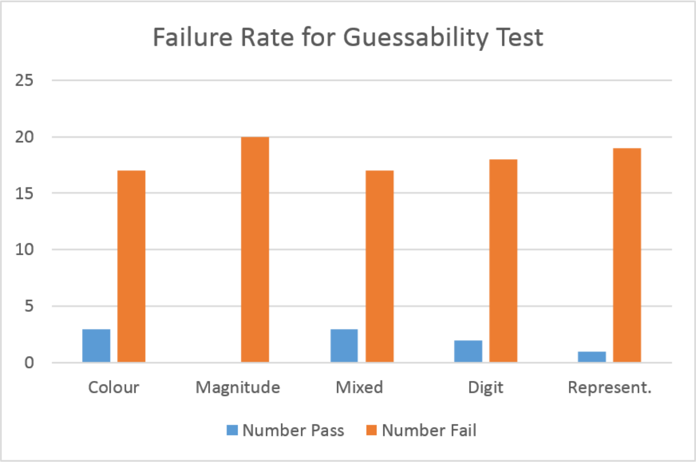


Fig. 6.5: Chart for guessability success rate

A chi-square test conducted on the results (appendix 10) reveals that no statistically significant correlation exists between the authentication model being used and the failure login rate. The chi square value is given by *X(4)* = 4.151, p = 0.386

6.5 Analysis of Shoulder Surfing for Prototype Set 2

The experiment to determine the vulnerability of property based authentication systems to observational attacks (shoulder surfing) is here repeated for the second set of implementation for the system. The five new models comprise of the number based models (digit and number representation), the text based models (character and word) and the form based model. As in the experiment in section 6.2, these experiment seeks to help understand if there is correlation between the failure rate of shoulder surfing attacks and the specific authentication model being used. It also helps to understand the effects of two login sessions versus one login session on the authentication failure rate for each of the authentication models. However, in the investigation of the effects of the shoulder surfing attacks conducted for set 2, due to timing constraints and the problem of participant population, a single experiment is conducted with two configurations. The configurations are those for a single login session and those for a dual login sessions. Thus in this experiment, the researcher seeks to:

4. Determine the variation in the level of shoulder surfing vulnerabilities in single login authentication configuration of all property based implementations (Set 2) and if statistically significant correlation exists between the models and their login failure rates.
5. Determine the variation in the level of shoulder surfing vulnerabilities in dual login authentication configuration of all property based implementations (Set 2) and if statistically significant correlation exists between the models and their login failure rates.

Like for implementation set 1, the experiment seeks to help understand if any correlation exists between vulnerabilities in each of the two configurations (test conditions) and the various implementations of the property based system.

6.5.2 Experimental Variables

Since the research seeks to determine the variation in the observation failure rates between the single login session and dual login session experimental configurations among all models in set 2, the various implementations of the authentication models serve as the independent variables, the login failure rates are the dependent variables, while the experimental configurations are control variables.

6.5.3 Research Participants

All participants were university students of ages between 20 and 40. They all have experience in the use of passwords and PINs. The study was conducted as a laboratory experiment in a within subject design, in which each student was allowed to observe authentication on any one of the system prototypes. The participants were randomly allocated to one of the authentication test configurations. An even number of participants was spread among the authentications systems. Each of the authentication prototypes for each of the experiments was allocated 20 participants to create the password and 40 others to shoulder surf and crack the password, 20 participants each for the single login and the dual login configurations.

6.5.4 Experimental Procedure

The experimental procedure is similar to that presented in section 6.2.4 for the authentication systems prototype set 1. The experiments were organized in a laboratory environment and each set of participants were treated individually. A data entry form was also used to collect the participants’ successes or failures in being able to succeed in guessing or observing the password of the supposed victim. After a brief orientation on the specific authentication they shall work on, the participants are grouped in groups of three to make two victim-attacker pairs and the victim is asked to create his password. The attacker is not allowed to view the password creation phase as this is not part of the tasks that need to be evaluated. After the password is created, the participant is asked to login to his password, just to ensure that he understands and clearly remembers the password he has created.

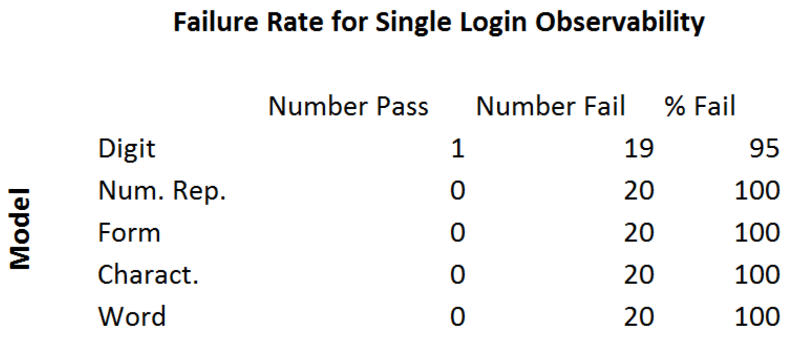
The victim is then asked to login to his password while the first attacker takes a position (sitting or standing) beside or behind the supposed victim. The attacker is allowed to take notes if he so wishes. The freedom to choose any position to take for the shoulder surfing attack is to give a more realistic probability for the shoulder surfing attack as it can actually be done in any position. The second attacker takes position after the success or failure of the first attacker has been recorded. The attackers were also allowed to take notes if they so wished. The second attacker is not allowed to see the single login observations of the first attacker. This is to help do away with the possibility of some learning effects between the login sessions, which may introduce some confounding variable in the experiment.

The two experimental authentication configurations that are evaluated are:

1. A single login for any of the five authentication models.
2. Two logins for any of the authentication models under investigation.

6.5.5 Results for 1 Login Authentication

A hundred (100) student participants, 20 for each authentication model, were asked to create passwords during the experiment. Another set of a hundred participants observed the user's single login entries. And yet another set of a hundred students observed the participants' double login entry. Hence, a total of 300 participants participated in the experiment. The results for the single login observations are presented in table 6.6.



Failure Rate for Single Login Observability

		Number Pass	Number Fail	% Fail
Model	Digit	1	19	95
	Num. Rep.	0	20	100
	Form	0	20	100
	Charact.	0	20	100
	Word	0	20	100

Table 6.6: Failure rates for single login observation

From the table one can see that in the 20 login attempts for each of the five system prototypes, only the participants that used the digit based model were able to secure a single login success. The 1 successful login gave the digit based model a 95% login failure rate on the part of the attacker. There was not a single attack success in all the other four authentication prototypes, hence all the others recorded a 100% login failure rate. For ease of interpretation, a histogram (figure 6.6) was drawn from the results in table 6.6.

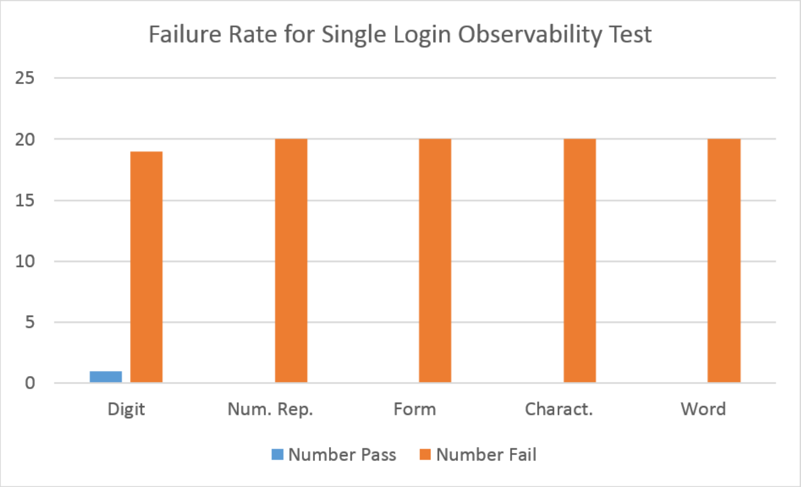
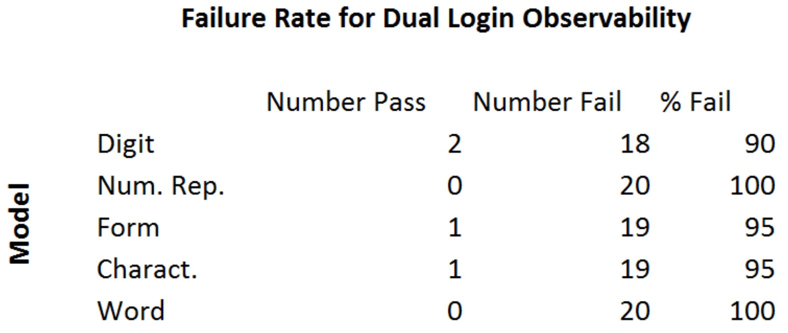


Fig. 6.6: Representative chart for single login observational failure rates

6.5.6 Results for Dual Login Observational Test

The second case for consideration in this experiment is the observation success rate for dual login entries. The experiment is conducted as specified in the operational procedure in section 6.5.4. The results for this test are presented in table 6.7. From this table, one can observe that out of the 20 attempts made for each of the models in the dual login study, the digit model had the lowest login failure rate with two successful attempts. The form based model and the character based models both have a failure rate of 95% making them the second lowest, while the number representation based model and the word based model both have a 100% login failure rate. This data is represented by the histogram on figure 6.7.



Failure Rate for Dual Login Observability

		Number Pass	Number Fail	% Fail
Model	Digit	2	18	90
	Num. Rep.	0	20	100
	Form	1	19	95
	Charact.	1	19	95
	Word	0	20	100

Table 6.7: Success and failure rates for dual login observation

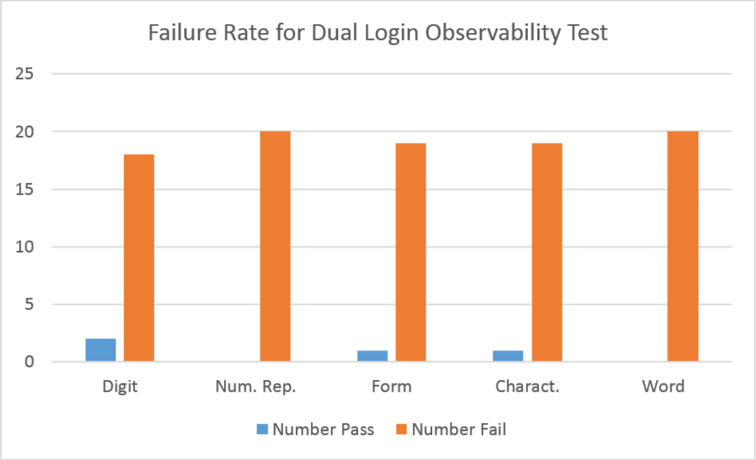
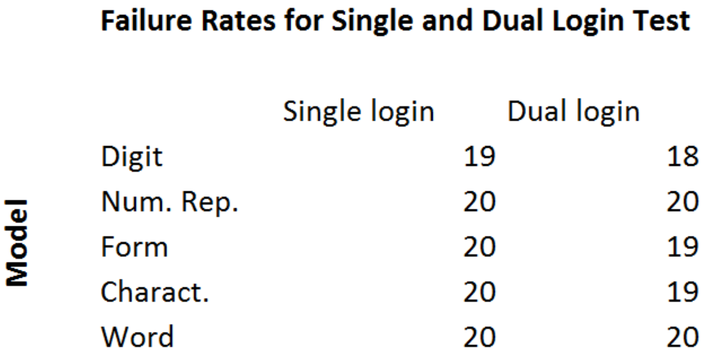


Fig. 6.7: Representative chart for dual login observational test

6.5.7 Discussion and Comparison of Results for Observability Test (Set 2)

For the sake of comparison, the results for the single and dual login observation tests are combined and presented in table 6.8. From the table, it is easy to observe that both the number representation based and the word based model had no authentication success for both the single and the dual observation tests. Hence, they each maintained a 100% login failure rate. the form and character based models each had a single login success rate for the dual login session, while the digit based model that had a single login success in the single login now had two login successes in the dual login test. This makes the digit based model the most vulnerable to shoulder surfing among the implemented prototypes for set 2. The contents table 6.8 are plotted and represented by the histogram in figure 6.8.



Failure Rates for Single and Dual Login Test

Model		Single login	Dual login
	Digit	19	18
	Num. Rep.	20	20
	Form	20	19
	Charact.	20	19
	Word	20	20

Table 6.8: Observation Failure Rates for Single and Dual Logins

The result set clearly indicates increased vulnerability with the increased number of login sessions being observed. However, a chi-square test performed on the results (appendix 11 (A and B)) indicate that no statistically significant correlation exists between the authentication type and login failure rate, $X^{(4)}$ = 4.04, p = 0.401 for the single login test and $X^{(4)}$ = 2.105, p = 0.716.

One interesting finding is the disparity in observation vulnerability between the number representation based model and the digit based model. While the digit based model gave the worst performance, the number representation model is one of the best two. This disparity may be due to the fact that the number representation model is somewhat may not be seen by an attacker as a purely numerical model.

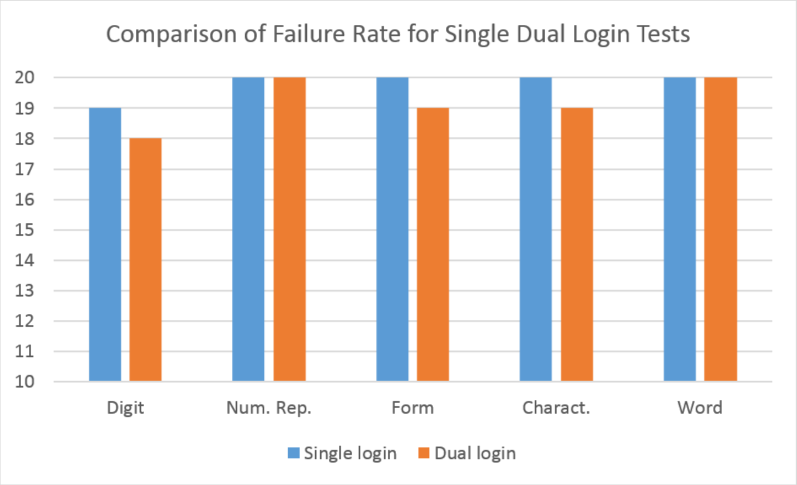


Fig. 6.8: Chart of Observation Failure Rates for Single and Dual Logins

6.6 Vulnerability to Verbal and Written Description

Considerable research has been conducted to investigate the effect of verbal and written descriptions of graphical passwords on the password guessability. The effects of verbal and written descriptions on various types of images used in the story scheme, for example had been investigated in [17], while the vulnerability of the passfaces scheme to descriptions was considered in [46]. The idea was to understand the susceptibility of these systems and image types to being communicated and how the risk of such communication to the security of the systems can be reduced.

Being a novel system of authentication, it will be interesting to understand the extent to which verbal and written descriptions increase the risk of guessing attacks on property based passwords. Hence in this work, the vulnerability of several prototype implementations of the property based system of authentication are being investigated. The researcher thus seeks to discover the level of susceptibility of property based systems to guessing attacks due to verbal or written descriptions of a user's password and if significant correlation will exist between the various implementations of the property based systems and guessing success rates due to verbal and written descriptions. Six authentication models were selected for the vulnerability test for verbal and written descriptions. These include the colour, pattern, magnitude, mixed, digit and representation based models. The researcher conducts two separate experiments which shall be used to:

- ✓ Determine the variation in the level of vulnerability to guessing attacks due to verbal descriptions for the models under investigation and if statistically significant correlation exists between the models and the attacker's login failure rate.
- ✓ Determine the variation in the level of vulnerability to guessing attacks due to written descriptions for the models under investigation and if statistically significant correlation exists between the models and the attacker's login failure rate.

6.6.2 Experimental Variables

The experiments are performed to determine the mean variation in login failure rates due to verbal or written descriptions among the various prototype implementations of property based systems. Hence, the system prototypes (or models) serve as the independent variables while the login success or failure are the independent variables.

6.6.3 Research Participants

As with other experiments, the research participants were university students of ages between 18 and 40 years of age. They all have experience in the use of passwords and PINs. The study was conducted as a laboratory experiment in a within subject design, in which a pair of participants were randomly allocated to one of the authentication systems. Twenty participants were asked to create passwords on each of the authentication systems and were asked to divulge the password either verbally or in writing to another set of twenty participants, depending on the exact experiment.

6.6.4 Experimental Procedure

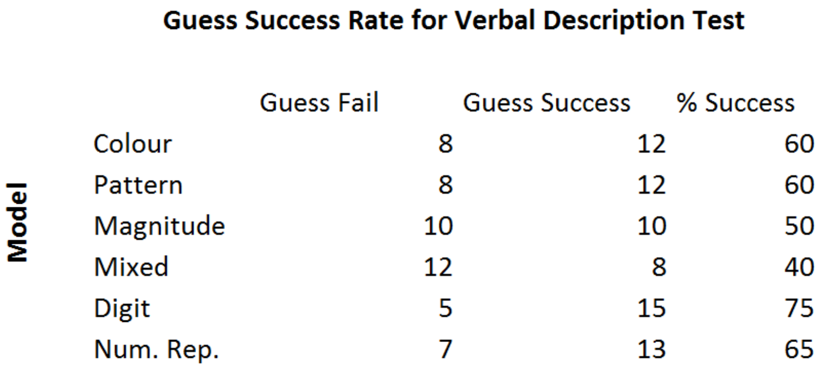
Two experiments were conducted, the first to investigate the effects of verbal descriptions of password on their guessability, and the second to investigate the effects of written descriptions of passwords on their guessability. The two experiments were conducted separately and not combined as in the shoulder surfing experiments in section 6.5. This was to do away with the possibility of the second 'attacker' getting a hint a of the user's password through the first 'attacker', i.e., through a mode that was not meant for him. If the second attacker is able to understand the password using the first attacker's mode rather than the one meant for him, and then uses it for his guessing attack rather than through his own mode, then the validity of the results may be compromised.

The experiments are performed with similar settings as the experiments performed in [84]. Due to the time spent in trying to explain the authentication procedure for each of the authentication models, a special training session was organised to acquaint each of the participants on the workings of each of the authentication systems. Thus as at the time of conducting the experiments, the participants were already familiar with the workings of each of the authentication systems, having practiced the procedure themselves during the training session.

During the experiments, the participants are paired with one participant acting as a user (or 'victim') while the other acts as the 'attacker'. The user is asked to create a password on using any of the authentication system prototypes under investigation. While this takes place, the attacker sits on the opposite side of the table. The user then passes the password on to the attacker either verbally or in writing depending of the specific experiment. After the exchange, the attacker takes the seat of the user and tries to guess the users password using the descriptions he has obtained from the user. The researcher records the login failure or success of each login attempt in a data entry form.

6.6.5 Results for Verbal Description Experiment

Two hundred and twenty (240) participants conducted the vulnerability to verbal descriptions experiment, twenty participants for each authentication model acted as the user (or 'victims'), while another set of twenty participants acted as the attackers for each of the authentication models. The results of the authentication failure rates for the verbal descriptions experiment are presented in table 6.9.



Guess Success Rate for Verbal Description Test

Model		Guess Fail	Guess Success	% Success
Model	Colour	8	12	60
	Pattern	8	12	60
	Magnitude	10	10	50
	Mixed	12	8	40
	Digit	5	15	75
	Num. Rep.	7	13	65

Table 6.9: Guessability success rates for verbal description

From the table, the digit based model has the highest success rate of 15 successful guesses (75%) among the 20 total attempts. The number representation based model is the second with 13 successful login guesses (65%). The colour based model and the pattern based model both have 12 successes and 8 failure, giving each a 60% success rate. The magnitude model is the fifth with 10 successes and 10 failures, while the mixed model is the least susceptible to guessability by verbal descriptions as it only records 8 successful guesses in the 20 attempts made in the experiment. This gave the mixed model a 40% success rate in guessability due to verbal description. The results from the table are plotted into the graph in figure 6.9.

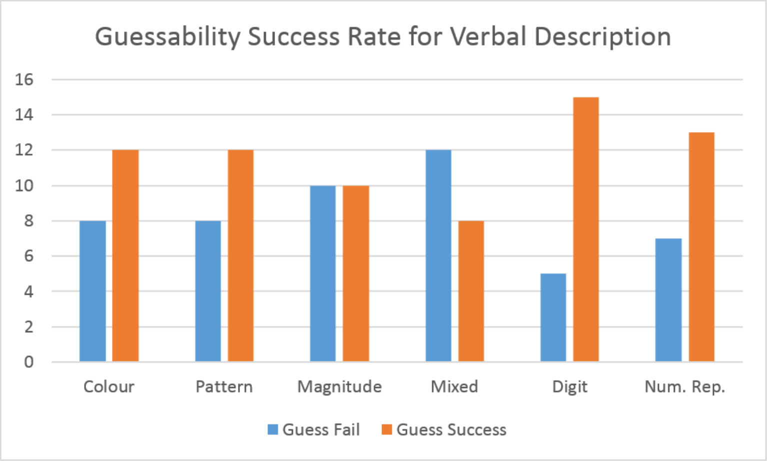
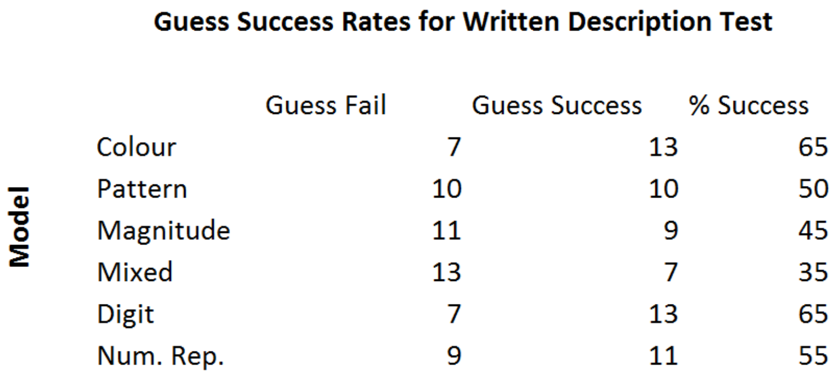


Fig. 6.9: Representative chart guessability due to verbal descriptions

6.6.6 Results for Written Descriptions Experiment

The second experiment is the experiment to ascertain the vulnerability of property based authentication systems to guessing attacks due to written descriptions of user passwords. In this experiment too, 120 participants acted as the legitimate users (or ‘victims’) in the experiment, while another 120 participants acted as the attackers. The experiment was conducted as specified in section 6.6.4. The results for this experiment is presented in table 6.10. A generalized view of the table when compared to table 6.9 shows that there is a slight decline in guessability success rate for all the models except the colour based model which witnessed increased vulnerability between the verbal and written description guessability attacks. From the table, the mixed model is the least guessable using written descriptions with success in only 7 attempts in the 20 trials given it a 35% guess success rate. The magnitude based model follows the mixed model with 9 successful guesses and scoring a 45% success rate. The Magnitude model scores 10 successful attempts taking the third position with 50% guess success rate. The number representation model takes the fourth position with 11 guess successes and 9 guess failures. The colour and digit based models are the most vulnerable to guessing attacks due to written description as they each had 13 successful guessed login entries and 7 failed login guesses due to written descriptions. The results in table 6.10 is represented in the by the chart in figure 6.10.



Guess Success Rates for Written Description Test

		Guess Fail	Guess Success	% Success
Model	Colour	7	13	65
	Pattern	10	10	50
	Magnitude	11	9	45
	Mixed	13	7	35
	Digit	7	13	65
	Num. Rep.	9	11	55

Table 6.10: Guessability success rates for written descriptions

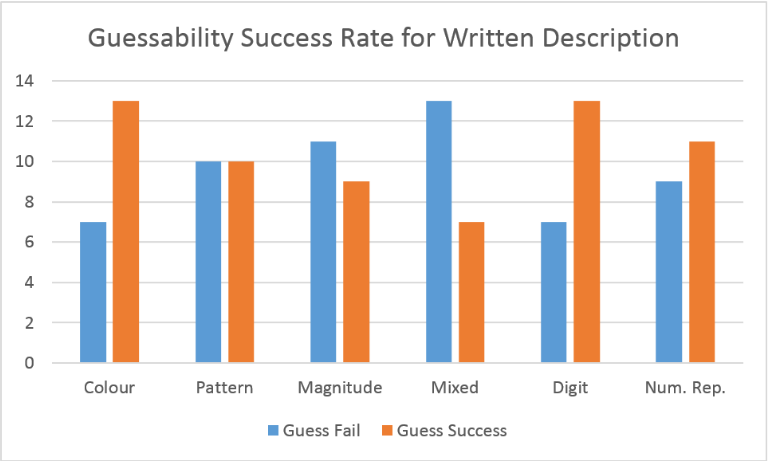
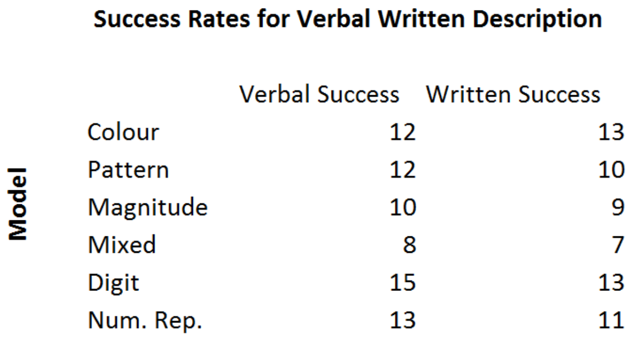


Fig. 6.10: Representative chart for dual login observational test

6.6.7 Discussion and Comparison of Results for Verbal and Written Descriptions

The results in tables 6.9 and 6.10 are combined into table 6.11 to provide a vivid picture of the comparison of the results for the experiments on the verbal and written descriptions. From the table it could be seen that the guess login success rates are generally higher in the experiment for verbal description than the experiment for written description showing that property based systems are more susceptible to attacks due to verbal descriptions than attacks due to written descriptions. From this results, one can insinuate that it is either more difficult to describe the property based images in writing than when spoken verbally or that it is more difficult to understand written descriptions of property based images than verbal description of them. From table 6.11, for the ease of comparison, a bar chart is provided in figure 6.11.



Success Rates for Verbal Written Description

		Verbal Success	Written Success
Model	Colour	12	13
	Pattern	12	10
	Magnitude	10	9
	Mixed	8	7
	Digit	15	13
	Num. Rep.	13	11

Table 6.11: Comparing success rates for verbal and written descriptions

From the figure it can be seen that the digit based model is the most vulnerable of all the property based systems used in the descriptions experiments, while the mixed model is the most secure. A chi square test conducted on the results of both the verbal and written vulnerability experiments indicate that no statistically significant correlation exists between the models and guess success rates. The results were $X^{(5)} = 6.034$, p = 0.303 for the verbal description test and $X^{(5)} = 5.514$, p = 0.356.

During the conduct of the experiments, as presented in the experiments in [84], no restrictions were made as to how a user’s password needed to be written down or how it is to be verbally described. It is interesting to note, however, that except for the magnitude and representation based models, a considerable number of the participants (more than half the population) that investigated other models were keener to provide sketches of their passwords rather write the descriptions in sentences while doing the experiment on written descriptions.

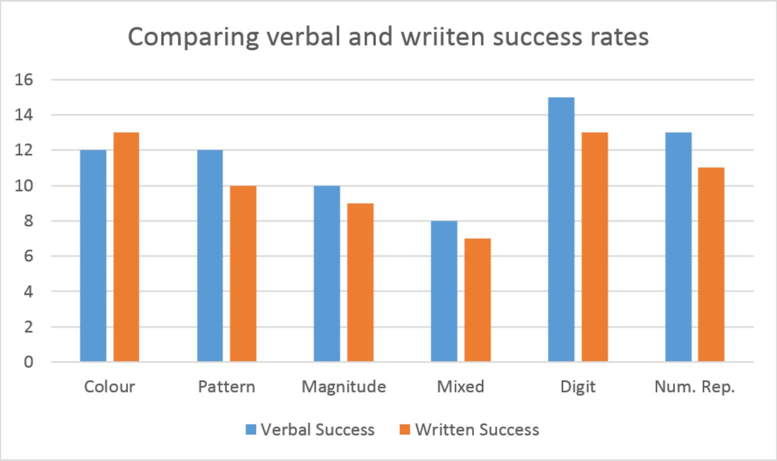


Fig. 6.11: Chart for Comparison of Success Rates in Verbal and Written Descriptions

6.7 Conclusion

The research question seeks to both discover the possibility of using the property based paradigm as a novel means of developing secure and usable systems that can be adopted as hybrid means of graphical authentication and the tendency that this novel method is able to bridge the usability and security gap or contention that has existed since the foundation of research interests in graphical authentication systems about three decades ago. Usability and security have always been at crossroads in the design of authentication systems, and there is an ever increasing need to develop new systems that can meet the challenge of both good usability and good security.

The experiments presented in this chapter have affirmed the belief of the researcher that in spite of the general acceptance of property based systems among study participants and their obvious simplicity in learning and in use as presented by research findings in chapter 5, property based systems are resistant to most common security attacks such as observational and guessability attacks to which most graphical authentication systems are prone. Hence, this strongly proves that property based authentication systems can potentially close the long standing gap between security and usability in graphical authentication systems.

From the results presented in this chapter, it can be easily seen (from section 6.2.5) that even a ‘one step’ implementation of a property based password indicates strong resistance to observational attacks that cannot be matched by existing recognition based graphical authentication systems. Judging, however, from the increased number of observation successes between the single login and dual login authentications, one is tempted to conclude that the risk of observational attacks increases with the number of observations being made, which is, however, a common trend with most authentication systems as humans tend to retain the memory of events they see quite often. The actual confirmation of this fact is subject to further research.

From the research findings, it can be observed that property based systems are generally more prone to guessing attacks due to descriptions than they are to other common attacks on the user side, such as observational attacks and hinted guess attacks (such as those motivated by knowing a user's favourite authentication factor). It is also imperative to state that from the research findings, property based systems are more susceptible to attacks due to verbal descriptions than they are to those due to written descriptions. It is also important to note that the notable variation that exists among various implementations of the property based paradigm in terms of susceptibility to various observational and guessing attacks has not been proven to be statistically significant.

Chapter Seven – Comparative Overview of Authentication Systems

7.1 Introduction

This chapter provides a comparative performance overview of existing graphical authentication algorithms alongside research findings for property based graphical authentication systems. Quite significant research has been done to quantify the performances of various authentication systems in terms of security, effectiveness, efficiency and user satisfaction through the use of metrics such as password creation time, password login time, and vulnerability to different attacks. Sections 7.1 to 7.3 are used to highlight usability and security comparisons of existing authentication systems conducted by various researchers while section 7.4 has been used for a more critical usability and security analysis. In this section too the researcher starts by highlighting a previous research study that provides a more critical evaluation of existing graphical authentication systems (7.4.1) before making a personal critical usability and security comparison of authentication systems (7.4.2) summarizing the results into two tables (7.6 and 7.7) for usability and security analysis respectively and the comparing these findings to selected models of property based systems.

7.2 Usability Studies

A number of surveys have been conducted in the literature to compare the usability of different graphical authentication systems. One of such surveys is the one conducted by researchers in Malaysia [145] in which they compared the usability of eight existing graphical authentication systems. They compared the systems in terms of user satisfaction, efficiency and effectiveness. The researchers divided the concept of user satisfaction into a number of distinct attributes such as mouse usage, simplicity of password creation, meaningfulness of images, whether images are user or system assigned, the system memorability, the beauty of the interface, simplicity of training, the beauty of the images, applicability, and R&A. No details were provided as to the actual meaning of some of the attributes, which may be rather confusing, such as applicability and R&A. No details were also provided as to the exact reason why some of the cells were painted. As in the previous usability comparison, this study also relied on information on these systems that are currently available in the literature. Moreover, it is extremely difficult to compare authentication systems even from studies done in the literature. This is because there is mostly no similarity in either design or experimentation. Even when similar experiments are performed, data analysis normally varies. In spite of these issues, researchers try their best in making as honest comparisons as possible.

With this in mind, an honest comparison of these systems with property based systems is performed. It is, however, significant to make an honest comparison of these items of usability in terms of the design and performance of property based systems from what is understood. Hence property based systems are placed in the table as the ninth item of comparison (font coloured in light green). In terms of mouse usage, keyboard based implementations of the property based system have not yet been implemented, hence all prototypes are mouse based. The passwords are simple to create. This is confirmed by qualitative opinion data obtained from study questionnaire provided and analysed in section 5.6.9. The images in property based systems are meaningful. Unlike the déjà vu scheme that is built on abstract images, property based systems are built on basic shapes and common colour that could be understood and related with. Without the meaningfulness, the idea of property based authentication will not be possible. The images in property based systems are also user assigned. That is, the user selects the properties with which he will like to authenticate, although the system randomly assigns images during authentication, which is an important feature of property based systems that may not be found in other systems. This idea actually bridges the usability and security gap between user selected images, believed to be more usable, and system selected images, believed to be more secure.

		Usability Feature										
		Satisfaction									Efficiency	Effectiveness
Row	**Recognition based scheme**	**Mouse Usage**	**Create Simply**	**Meaningful**	**Assignable Image**	**Memorability**	**Simple Steps**	**Nice Interface**	**Training Simply**	**Pleasant Picture**	**Applicable**	**R & A**
1	**Passfaces**	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
2	**Déjà vu**	Y	Y	N	Y	N	Y	N	Y	N	N	Y
3	**Triangle**	Y	Y	N	N	Y	Y	N	N	N	N	Y
4	**Movable Frame**	Y	Y	N	N	Y	Y	N	N	N	N	Y
5	**Picture Password**	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N
6	**Story**	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N
7	**Man**	Y	Y	N	Y	Y	Y	N	Y	N	Y	N
8	**Jetafida**	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N
9	**Property Based**	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-

Table 7.1: A Usability Comparison of Existing Authentication Systems [145]

Memorability is another strong point for property based systems. According to results obtained in the memorability experiment in chapter five, the digit based model maintained a 100% login success rate throughout the memorability evaluation of more than three weeks. The authentication steps in property based systems are very simple to understand and to carry out. This is also confirmed by the analysis of user opinion data in chapter 5. The next item of usability in the table is the ‘nice interface’ which depicts the beauty of the user interface design. The question on user satisfaction with the layout of the interface from in user studies answers this question as part of the usability survey in relation to user satisfaction. The extremely simple and short user training in each experiments as well as opinion data from user studies point to the exact position of property based systems in terms of user training needs. All images used in property based system were developed or modified by the researcher to ensure that they were both nice and very easy to understand. From the comparison in table 7.1, it is obvious that property based systems are the most usable of all recognition based systems presented in the study.

Researchers in [31] also made a comprehensive comparison of the usability and security capabilities of graphical authentication systems. This study also relied on what was obtained by the researchers from available literature. Twelve authentication systems were considered in the usability and security comparison. The contents of the usability comparisons are presented in table 7.2. In this table, the first two columns are used to designate the authentication technique, whether recognition or recall based. The rest of the columns provide information on the systems in relation to a number of usability features. The researchers further subdivided the usability features of graphical systems into memorability, efficiency, input reliability and accuracy, easy and fun to use, grid based and drawing password. The last two features depict the design of the password system, whether it is a drawing or a grid (image selection) based system. The researchers then subdivided memorability into eight sub-themes. Sub-themes that are believed by the researchers to assist memorability. These include meaningfulness, human faces, organised by theme, user assigned images, icon based, abstract image, navigating images, freedom of choice. While other memorability based features relate to the way the system is constructed, meaningfulness regards to the fact that some meaning could be attached to the presentation of images, user assigned images means whether or not the user choses the authentication images or they are systems supplied.

Comparing property based systems alongside other systems analysed in the table will help understand their usability features and advantages in relation to other systems. Hence, property based systems are introduced into the last row of the table. First of all, as a hybrid systems, exploiting both elements of recognition and recall, property based systems are difficult to place explicitly as either recognition or recall based systems. In terms of the usability features presented in table 7.2, and in terms of the memorability, property based systems have meaningful images. Hence their susceptibility to social engineering attacks. Only meaningful images can be transmitted through social engineering.

Graphical Password Schemes	Techniques		Usability Features on Graphical Password												
			Memorability												
	Recognition	Recall	Meaningfulness	Human faces	Organised by theme	User assign image	Icon based	Abstract image	Navigating image	Freedom of Choice	**Efficiency**	**Input reliability & accuracy**	**Easy and fun to use**	**Grid based**	**Drawing password**
Jansen et al.	√		√		√						X		√	√	
Passfaces ™	√			√		√					X	√	√	√	
Triangle	√						√				X		√		
Movable Frame	√						√				X		√		
Intersection	√						√				X		√		
Pict-O-Lock	√						√				X	√		√	
Déjà Vu	√							√			X		√	√	
Blonder		√	√							√	X				
VisKey SFR		√	√			√				√	X	√			
Passlogix v-Go		√	√		√	√			√		X		√		
PassPoints		√	√	√						√	√	√	√	√	
DAS		√	√			√						X		√	√
Property Based	√	√	√			√				--	√	√	√	√	
√ = Yes, **X** = No, Blank = not mentioned															

Table 7.2: Usability comparison of graphical authentication systems [31].

Property based images are not composed of human faces, are not organised by theme, but the images are user assigned. This is because the user selects the specifics of the passwords himself. They are also not icon based, and do not contain abstract images. Also the images are not navigated like those of the passlogix system. The term ‘freedom of choice’ is not fully explained by the researchers and hence it purposefully left blank (hence the dash).

Considering the other elements of usability, unlike the researchers analysis of other systems, property based systems are efficient. Efficiency is a measure of the speed of registration and authentication collected through system logs and the ease of registration and authentication collected through survey questionnaires. This data has been collected and analysed in chapter 5. Property based systems also have ‘input reliability and accuracy’ as specified for the passfaces scheme. Property based systems are easy and fun to use, they are grid based and not drawing based passwords.

Looking at the table one will realize that property based systems have six checked columns in the usability comparison table. This is only surpassed by the passpoints scheme which is a good indication of the usability potentials of the property based paradigm in user authentication.

7.3 Security Comparisons

Security is another important attribute of good authentication systems. The security of a system is the ability of a system to withstand being breached by unauthorised persons. A number of comparative security studies on graphical authentication systems have been performed. The researchers in [145] also did a comparative study on the on the security of recognition based graphical authentication schemes. They considered the same eight authentication models they had considered in their security evaluation in section 7.2. Their findings have been organised into table 7.3. From the table it could be seen that the strongest of the systems considered are those that show resilience to four of the attacks and are susceptible to two. The systems include the Man scheme, the movable frame method and the triangle scheme. The déjà vu scheme and the passfaces scheme both show resilience to three of the attack types and are susceptibility to the other three. There was no sufficient data to help categorise the performance of the remaining three authentication schemes, which include the picture password, the story scheme and the Jetafida scheme.

In comparison to these systems and in relation to the six items of security, the performance of property based systems is entered in the last row. The first security item in the table is the brute force attack. A brute force attack is an attack launched aggressively and perpetually until the attacker succeeds. In an actual implementation of property based systems, a lockdown mechanism prevents continuous login attempts as the system locks out the user after three unsuccessful attempts. This mechanism does not allow the success of a brute force attack, and hence a brute force attack is unlikely. The next security item implies the susceptibility of a system to dictionary attacks. Dictionary attacks are possible only when data relating to user chosen secrets is stored in plain text. In property based systems, no information is stored about a chosen image, but about a chosen property, which will be difficult to understand by a hacker. Hence a dictionary attack will be quite difficult to carry out on an implementation of the property based system.

Row	**Recognition based schemes**	**Attacks**					
		Brute Force	**Dictionary**	**Guessing**	**Spyware**	**Shoulder Surfing**	**Social Engineering**
1	**Passfaces**	Y	Y	Y	N	Y	N
2	**Déjà vu**	Y	N	Y	N	Y	N
3	**Triangle**	Y	N	Y	N	N	N
4	**Movable Frame**	Y	N	Y	N	N	N
5	**Picture Password**	-	-	-	-	Y	-
6	**Story**	-	-	-	-	Y	-
7	**Man**	Y	N	N	Y	N	N
8	**Jetafida**	-	-	-	-	-	-
9	**Property Based**	N	N	N	N	N	Y

Table 7.3. Comparison of Susceptibility to Common Attacks [145]

From the results of the guessability experiments obtained section 6.4.5 of this thesis, property based systems are resistant to guessing attacks. None of the systems examined in the experiment scored a login failure rate below 85%. In fact the magnitude model, which was the best of the five, scored a login failure rate of 100%. Hence, property based systems are resilient to guessing attacks. Moreover, the locking mechanism that locks out a user after three failed attempts deters unauthorised users from blind guessing attacks. The next item on the list was spyware. Spyware are programs installed on a computer to gain information on user activity through the recording of the user’s keyboard or mouse dynamics. Property based systems use mouse based data entry, at least for now. For the spyware’s record of mouse dynamics to be significant, they must follow a definite pattern. In property based systems, the position of a user's pass image within the image selection grid changes in every session. This is a particularly difficult problem for spyware. Furthermore, in property based systems, the user selects his pass images during registration, but the systems dynamically assigns the users pass images in each session of authentication. This is one of the strong contributions of property based systems as they bridge the gap between user selected images, believed to be more usable and system selected images, believed to be more secure [145].

The next security item in the table was the resistance of the system to shoulder surfing attacks. A number of experiments have been done on the vulnerability of property based systems to shoulder surfing attacks. Looking at results from sections 6.2, 6.3 and 6.5, one will be convinced of the strength of property based systems against observational attacks. Even for the dual login observation, and without intermediate tasks, the minimum login failure percentage among five models was 90%. This is a difficult score to achieve by any other system.

The last security item for comparison in the table is social engineering. Social engineering is only possible where passwords can be can be transmitted to others either verbally or in writing in such a way that they can easily understand. Property based systems are vulnerable to social engineering attacks. Looking back at the results for the experiments on the vulnerability of the systems to description in section 6.6., of the six property based systems selected for evaluation, five of the systems analysed scored 50% and above in guess success rates in terms of verbal descriptions, and four scored 50% and above in terms of written descriptions. This shows that property based systems will be vulnerable to social engineering attacks.

When one looks at all the systems compared in the table, one will realize that only property based systems may be able to claim resilience to five of the six security items presented in the analysis. This suggests that from the knowledge of existing systems, property based systems may be the most resilient authentication systems developed. This is, however, too early an assumption to make as the introduction of property based systems to the scientific community may spawn research interests, and, of course, debate.

Researcher in [31] also analysed a number of password systems in terms of their security features and susceptibility to a number of attacks. Twelve authentication systems are used in the analysis. Their research findings are summarised into table 7.4. The research also utilised what was available from existing literature. In the table, the first two columns designate the authentication technique, either recognition or recall with which the authentication system is identified. The next six columns identify six attack types upon which the authentication systems are compared. These attack types include brute force attack, dictionary attack, guessing attack, spyware attack, shoulder surfing attack and social engineering attack. These are exactly the attacks analysed in table 7.2.

Having discussed the resilience of property based systems in relation to table 7.3, one will simply examine the contents of the table's other columns. The table has six other columns that specify significant security features employed in the design of authentication systems. These features include large password space, randomly assigned images, hash function, image variation, decoy images, repeat verification. As compared to recall based authentication systems, authentication systems adopting the grid based features of recognition based systems generally do not have large password spaces. Like in the passfaces scheme, the password space for property based systems is M^N, where M is the number of images in the selection grid and N is the number of authentication steps. In property based systems, however, neither M nor N are constant.

Graphical Password Schemes	**Techniques**		**Possible Attack Methods**						**Security Feature on Graphical Password**					
	Recognition	Recall	Brute force	Dictionary	Guessing	Spyware	Shoulder-surfing	Social engineering	**Large password space**	**Randomly assign images**	**Hash function**	**Image variation**	**Decoy images**	**Repeat verification**
Jansen et al.	√		√	X	√	**X**	√	X	X	√	√		√	
Passfaces ™	√		√	√	√	**X**	√	X	X	√			√	
Triangle	√		√	X	√	**X**	X	X	√	√			√	
Movable Frame	√		√	X	√	**X**	X	X	√	√			√	
Intersection	√		√	X	√	**X**	**X**	X	√	√			√	
Pict-O-Lock	√		√	√	**X**	√	**X**	X	√	√		√	√	√
Déjà Vu	√		√	X	√	**X**	√	X	X	√	√		√	
Blonder		√	√	X	√	**X**	√	X	√					
VisKey SFR		√	√	X	√	**X**	√	X	X					
Passlogix v-Go		√	√	X	√	**X**	√	X	**X**					
PassPoints		√	√	X	√	**X**	√	X	√		√			
DAS		√	**X**	√	√	**X**	√	X	√		√			
Property Based	√	√	**X**	**X**	**X**	**X**	**X**	√				√	√	

Table 7.4: Authentication systems' security features and vulnerability [31].

Property based systems have randomly assigned images, that is, both the pass and decoy images are changed across authentication sessions. During each authentication round, the image grid submits the user with a different set of both the authentication image as well as the decoy images. They are not associated with harsh functions, but are associated with image variation as the portfolio and decoy images are changed with each authentication session. Property based systems do not have a function for repeat verification.

When all the security items to which property based systems are vulnerable are checked, and those to which they are secure are marked with 'X', one will realize that property based systems are the only ones to which more than four security related features are marked with an ‘X’. This is a strong indication of the strong resilience of property based systems to security breaches on the user side.

7.4 More Critical Analysis

This section considers more critical comparison of usability and security in existing graphical authentication systems. The section is also used to compare the usability and security of existing with selected implementations of the property based paradigm. In the first part of the section the researcher provides an example of more critical security and usability evaluation from the literature, and in the second part of the section, the researcher makes his own critical comparisons based on existing literature and the compares these results to those of selected property based system implementations. The researcher does the comparison using two tables, table 7.6 (for usability) and table 7.7 (for security).

7.4.1 Previous Study

A number of researchers have extensively compared the usability and security of existing graphical authentication systems. One of these is the work conducted by the researchers in [130] They created three tables for their evaluations, one for recognition based systems, one for recall based systems, and one for cued recall based systems. Since property based systems are grid based systems, it was seen to be more accurate to evaluate their performances based on the table designated for recognition based systems. Their findings for recognition based systems are organised into table 7.5

The researchers used a set of symbols as measures of performance based metrics. The performance and data metrics include theoretical space (bits), user choice resilience, variant response, server probes, paper study, lab study, field study, web study, login time, success rate and interference studied. The researchers used the abbreviation *i.d.,* meaning ‘insufficient detail’ to designate that there was no sufficient detail available to then from the literature to help them in categorising that system on that aspect of the information they needed. The (*) was used to indicate their best estimates from the data available to them and the dagger (†) to indicate approximations based on reported figures. They used the dash (-) to indicate that to the best of their knowledge there was no published data in relation to a piece of information for that system. The researchers used a number of measures to categorise security, such that they categorized password space into three ranges according to the number of binary digits (bits) used. This is in line with configurations mostly reported in the literature. They used icons to categorise the ranges as: under 20 bits (*PIN-level,* ○), 20 to 60 bits (*password-level,* ◉), and over 60 bits (*crypto-level,* ●). They then categorised the systems based on the degree to which the issue of user choice can weaken security. Schemes that were affected by predictability due to user choice were seen as the weakest and rated (◇), those with system-assigned passwords were rated the strongest (◆), while those that are trying to influence user choice to support usability and security gains are rated❖. In schemes that provided two options for user chosen images and for system generated images, the table was designed to provide a rating for each. Thus in the “variant response" row, a ‘yes’ indicated a non-static response (i.e., each authentication session provided a different set of authenticators) such that a simply recorded observation that is played later is likely to fail. Systems such as the passfaces scheme in which a constant set of images is selected for each step in each login session, a ‘no’ is marked against it on the ‘variant response’ item. Another parameter they captured was the number of server probes an attacker will need to carry out a phishing attack (without any interaction with the user). A probe means a single login instance. For schemes like the DAS scheme, no probes are needed as the attacker only needs to display an empty grid on his phishing site. For the passpoints scheme, one probe is needed to retrieve the password for any particular userid.

For the usability study, the researchers compared if multiple password memory interference has been studied, i.e., the use of multiple passwords. They also compared measures such as the login time, login success rates and the duration within which the user studies had been conducted from what is obtained in available literature.

Scheme	Cognitive Authentication	Use Your Illusion	Story	Passfaces / Face	VIP (type 1)	D´ej`a Vu	Photographic Authentication	Convex Hull Click	GPI / GPIS	Property based schemes
Theoretical space (bits)	○/● 10/73	○ 11	○ 12	○ 13	○ 13	○ 16	◉ 20	◉ 32	◉ 43	○ 18
User choice resilience	◆	*i.d.*	◇	◇ / ◆	◆	*◇	*◇	*◇	*◇/*◈	◆
Variant response	yes	no	no	no	no	no	yes	yes	no	yes
Server probes	many	1	1	1	1	1	many	many	1	many
Paper study	-	-	-	-	-	-	-	-	-	-
Lab study	13×/ 10wk	4×/4 wk	-	-	2×/1wk 3×/4wk	2×/1 wk	1×	2×/1 wk	2×/1wk	≥16wk
Field study	-	-	≥16 wk	≥16wk 10wk	≥16wk	-	-	-	-	-
Web study	-	-	-	1-5mth 5wk	-	-	-	-	-	-
Login time	90-180s	12-26s	-	14-88s	5-†6s	32-36s	†40s	72s	†18s/†19s	20 - 26s
Success rate	>95%	89-100%	†85%	72-100%	†11-95%	90-100%	†95-100%	90%	83%/74%	85%-100%
Interference studied	-	-	-	yes	yes	-	-	-	-	-

Table 7.5: Security and Usability Comparisons for Recognition Based Systems [130]

Comparing the performance of property based systems with those of other systems in the table, one will realize that the systems maintain an average to high performance in every usability or security metric used in the study. From this, one will realize that in this comparative study too, property based system demonstrate to possess both good usability and good security in line with the research objectives.

7.4.2 Usability Analysis of Existing Systems

Usable security researchers find it exceptionally difficult to efficiently compare studies conducted on the design and evaluation of existing graphical authentication systems for many reasons. Some of these reasons include the fact that many designs are never evaluated. Other reasons include the fact that researchers evaluate new systems using different metrics, sample sizes or different study designs. Even when the system or study designs are similar, there may be disparity in the data analysis techniques [16, 124].

The evaluation summarised in table 7.6 looks into existing literature to compare the design and performance of existing graphical authentication algorithms based on a number of metrics. Three models of the property based system have been randomly selected and compared alongside the existing systems using a set of metrics. The metrics include:

- **Memory Type:** Memory type denotes the type of memory process involved the retrieval of the image from memory. This is categorised into; recognition, recall and cued recall.

- **Image Type:** This denotes the exact type of images used by the authentication system such as pictures, icons or doodles.

- **Image Selection:** Image selection denotes the way authentication images (passwords) are assigned on the system, that is, whether they are system assigned or user selected.

- **Registration Time:** This is the time it takes a new user to create a password on the system as reported by documented user studies. It is an important measure of the efficiency of the system.

- **Login Time:** This is the time it takes a user to login on the system as reported by user studies. It is also an important measure of the efficiency of the system.

- **Login Success Rate:** This is the percentage of successful logins among all login attempts of system users as reported by documented user studies. It is an important measure of the effectiveness of an authentication system.

- **Number of Images Needed:** This is the minimum number of images required for the creation of the system as reported by previous user studies.

- **Target/Decoy Images:** These are the numbers of password images selected by the user in each authentication round compared to the number of distractor images presented together with the user's password.

- **Constant Decoys:** This indicates if the same decoys (distractor images) are presented with the user's chosen password each time he comes to authenticate or if such images are constantly changed.

- **Ordered login:** This is an indication of whether the user's selection has to be done in a definite order to create his password and if that order has to be strictly followed whenever the user comes to authenticate.

- **Type of User Study:** This indicates the type of user study conducted by the researchers on the system. This are categorised are lab, field or web studies.

In this comparative study, effort is made to obtain and report values from current literature. This may sometimes not be possible due to lack of reported work and the value has be considered from an informed guess such as the availability of data for very similar designs or estimated from non-numerical contexts such as graphs. This is designated by an asterisk (*). A system that does not entirely fit a given metric due to some exceptions or design characteristics is appended with a cross (†). An example is in the 'image selection' option for property based systems in the usability table (table 7.6) to designate that the images are neither entirely user selected nor system assigned.

7.4.4 Discussions on Usability Analysis

For ease of understanding, a summary of the findings of the usability analysis of graphical authentication systems is presented in table 7.6. The table has been used to compare the implementation and performances of thirteen existing authentication systems and three property based implementations randomly selected. The table is made up of twelve columns. The first column is used to specify the name of the model. The next column 'Memory Type' denotes the type of information retrieval method adopted in remembering the password from memory. There are basically three categories of authentication systems based on the information retrieval method; recall based, recognition based and cued recall based systems. In this classification, property based systems can best be classified as a form of cued recall based authentication systems. The third column contains the 'Image Type' or the type of image used by the authentication method. Various authentication systems have used different image types in their respective implementations. The passdoodle scheme, for example, uses images of hand-drawn doodles, the passfaces scheme uses pictures of human faces, the déjà vu scheme uses pictures, art images and system generated abstract images, the convex hull scheme uses icons of logos, while the story scheme uses random object images. The cognitive authentication scheme uses pictures and pseudo-word images. Click based authentication schemes such as Blonder's scheme [63], the passpoints scheme [69] and Cued Click points (CCP) [71] use picture type images. The CDS scheme proposed in [74] also uses picture and object based images like the story scheme. The DAS scheme [58] and the signature scheme [62] do not provide images, but present users with empty grids upon which the user writes down his password. Hence in the 'Image Type' column, the letters 'NA' are written, which stands for 'Not Applicable' to indicate that this property (images) do not apply to the implementation of these systems. For property based systems, the 'Image type' depends entirely on the implementation of the particular model. For the three models presented in the table, the Colour Model uses art images of common shapes, the Mixed Model also uses art images of basic shapes and the Word Model uses pictures and object based images as well as written English words. The diversity of the 'Image Type' feature is a unique advantage for property based systems. Although the passpoints scheme [67] claims to be able to adopt a wide variety of images, many images have proven to be difficult to use in the implementation of this system [68]. The next column, the fourth, contains the image selection styles. This indicates the method by which the selection of images takes place on the system, whether or not images are 'User Selected', which means that the user has the free will to choose password images of his choice in the system's image pool, or if the images are 'System Assigned', in which the system randomly assigns images to the user, in which case the user has no control over the choice of images to use for his password. The main advantage of use selected images is increased memorability, while the main advantage of system assigned images is increased security [130]. Except for the DAS and BDAS passwords in which the image selection style is 'image drawn by user' and the signature based scheme in which the selection style is 'signature drawn by user', all other systems have either user selected or system assigned images. In property based systems, however, the 'properties' are user selected during the registration phase, but authentication images are presented by the system and may be different from the exact image the user selected during his/her registration. This is also a unique feature of property based authentication systems. The next column (the fifth column) contains the ‘Registration Time’. This is the amount of time in seconds which a user spends during password creation and is a measure of the efficiency of an authentication system (table 5.1). In cases where no report of this value is found in the literature, the phrase ‘Not Reported’ is entered into the column. As one can observe, except for the Cued Click Points (CCP) scheme which reports a 24.7s password creation time, all other systems reported have a password creation time of more than 40 seconds. In the property based schemes presented in the table, although the Colour Model and Mixed Model have registration times of 79.8s and 78.9s respectively, the word based model has a registration time of just 37s. The sixth column ‘Login Time’ is the time it takes a system user to use his password to get authenticated onto the system and is also a measure of system efficiency (table 5.1). As in the case of registration times, the phrase ‘Not reported’ has been used in cases where the user studies contained in the literature have not provided values for the login time for a system implementation. As can be observed, for most systems, it takes far less time to login than to create the password. Except for the cognitive authentication system that records a login time of 90-180s, among the seven systems in which the studies have been conducted and values reported, only four systems record a login time of less than 20 seconds, three systems record a login time of less than 30 seconds, and one system records less than 40 seconds, considering extreme values. All property based systems in the analysis record a login time of less than 40 seconds. In fact, the Colour Model records a 19.7s which is considerably better than the average. The seventh column is the ‘Login Success Rate’ which the denotes the percentage login success for an authentication system, that is, the proportion of successful login attempts in relation to the total login attempts made in a given login session. Login success rate is a measure of the memorability and effectiveness of a system (table 5.1). In systems with very good memorability, the login success rate is very high and are seen to be very effective. The déjà vu scheme, for example has a login success rate of between 90 and 100 percent. This is far better than the passfaces scheme that reports between 72 and 100 percent. The variation of percentage for a system is indicative of variation in results between several experiments and user studies conducted in which some of the experiments reported the lower bound, and others reported the upper bound, exact values are mostly obtained from single experiments and analysis. Other systems, such as the DAS and BDAS schemes, still reported lower values of 57-80% and 50-80% respectively. The property based systems analysed in the table reported average to high values with the Colour Model having 90-100%, the Word Model having 85-95% and the Mixed Model having 60-80%. The eighth column contains the ‘Number of Images Needed’ to form an image pool from which a user can select his password images or the number images that form an image panel in a grid based authentication scheme. For most click based authentication systems, the number of images needed is only 1, while the number of images per panel is provided especially in relation to systems in which the exact number of panels needed for a successful authentication has not been specified. For property based systems, 200 images is designated as the number of images that forms the image pool from which all passwords for a model can be drawn. The ninth column is designated as ‘Target/Decoy Images’ and specifies the number of images needed by the user to create his passwords compared to the number of non-password (decoy) images presented in each authentication grid. For property based systems, the user’s password consists of 1-4 images depending on the number of steps, while the number of decoy images ranges from 3-96 depending on the selected grid size. The tenth column is designated as ‘Constant Decoys’ and is used to show that decoys (distractor images) used alongside user password images in a grid are never changed. For most systems, there is a variation of decoy images in every authentication round, except for systems that do not use decoy images. For all property based systems, decoy images are randomly changed in each authentication cycle. The eleventh column is designated as ‘Ordered Login’ and is used to specify if the user’s login credential have to be entered in a definite order whenever he/she comes to authenticate. While for some systems the order in which password are entered is insignificant such as with the déjà vu and passfaces schemes, in other systems such as Blonder’s and passpoints schemes, images or click point selection must be done in a definite order. In all property based schemes, password image selection must be done in a definite order. The last column specifies the ‘Type of User Studies’ and holds information on the type of user studies conducted for the model. There are various options for the type of user studies conducted to a system which include; lab studies, which indicate if the studies were conducted in a single session in a lab or other controlled environment, field study if the system is deployed in an uncontrolled environment such as the web, lab – multiple, if the studies are conducted through multiple lab studies, or paper based if a paper based study was conducted. All experiments for property based systems were conducted in controlled laboratories.

7.4.5 Security Analysis of Existing Systems

The security analysis conducted as part of this research work looks into the issue of security with regards to a list of security related items as presented in table 7.7. These items include:

Theoretical Password space: This is the set of all possible passwords that a password system can accept. For example, the theoretical password space of all 8-character passwords is 95^8 since there are 95 printable characters in a standard keyboard.

- **Selection Patterns:** This indicates the possibility of observable patterns in the selection of user passwords in a given password system. These selection patterns increase the guessability of user passwords.

- **Offline Attack:** This is the tendency that an attacker can launch an attack on the systems when the attacker is not online.

- **Shoulder Surfing:** This is the amount of effort that an attacker can exert to learn a user's password by merely spying over his shoulders.

- **Guessability:** This is the tendency that a user's password is easily guessed to due to noticeable password selection patterns or due to some design issues associated with the system.

- **Social Engineering:** This is the possibility that a system user can intentionally or unintentionally divulge his password to someone with malicious intent.

- **Main Security Concern:** This is a means that can be exploited by attackers to gain access to the system.

7.4.6 Discussions on Security Analysis

As in the usability analysis the researcher's security analysis also looks into thirteen existing graphical authentication systems and analyses these systems based on seven security parameters as presented in table 7.7. As in table 7.6, the first column of this table also holds the name of the authentication system being analysed. The second column specifies the 'Theoretical Password Space' which is viewed as the number of binary digits (bits) that are utilised in the storage of the password into system memory. It is a measure of the resilience of the password against common attacks. The higher the amount of memory needed to store a password, the more difficult it is for an attacker to infiltrate [130]. From the table, one can observe that among the systems for which this parameter is reported, the BDAS scheme has the highest theoretical password space of 61.8 bits followed by the DAS with 58 bits. Data from the table generally indicates that draw based passwords (such as BDAS and DAS with 61.8 and 58 bits respectively) have the highest theoretical password spaces and hence the highest resilience followed by the click based systems (such as passpoints with 44 bits). Grid based passwords are the weakest with passdoodle and passfaces schemes having 16 bits each and the story scheme having 12 bits. For grid based systems, the theoretical password space is computed as N^M where N is the number of images in the challenge set (size of the grid) and M is the number of authentication steps. Hence for the passfaces scheme with a grid size of 9 and 4 authentication steps, the theoretical space is 9^4 which is $\approx$ 16 bits. For property based systems, a grid size of 25 and 4 steps gives a theoretical space of 25^4 which is $\approx$ 18 bits. The third column in the table is the 'Selection Pattern' which specifies if there are any definite selection patterns used by users in the selection of their passwords. Selection patterns are normally a giveaway for attackers as they provide helpful means by which they can attack. For the passfaces scheme, for example, research has proven that users tend to select attractive faces, faces of the opposite sex, or faces of members of their own race. This is a selection pattern that can be easily exploited. Property based authentication systems have no selection pattern as the user does not select 'definite' password images and portfolio images are randomly presented for authentication by the system. The next column 'Offline Attack' specifies the possibility of launching an offline attack on the system. For most systems, the attack is only possible if the password images or 'system' is on the computer system. However, many systems can be hashed. Hashing is the process of encoding a password using a cryptographic hashing algorithm. If a system is hashed, only the result of the hashing operation is stored on the computer. To verify the success of an attack, the attacker only needs to compare the results with the stored password hash. The next column 'Shoulder Surfing' designates the possibility of launching an observational attack on the system. An observational attack is an attack that is mainly based on the attacker's ability to observe the actions of the system user when he enters his password. Shoulder surfing attacks are among the greatest security challenges of graphical and text based password systems. The column contains the intensity of the work (i.e. number of observations) needed by an attacker to effectively learn password data entry from an unsuspecting user from mere observation. The data entered here is categorised into 1 login, a few logins, several logins or none, indicating that observational attacks are not possible for this system. As shown from the research findings, observational attacks are very difficult for property based systems and in order to succeed, an attacker must observe several login entries. The sixth column 'Guessability' denotes if the system is susceptible to guessing attacks, that is, random guesses. Random guessing attacks are only possible where system users display predictable patterns in password selection. Except for some systems like the passfaces scheme that has obvious selection patterns, guessing are difficult to perform on most authentication systems. Hence in property based authentication systems, it is not possible to launch random guessing attacks due to lack of predictable patterns in user image selection. The seventh column in the table 'Social Engineering' denotes if social engineering attack can be launched on a system. Social engineering is that act of convincing a system user to divulge sensitive login data to help the attacker launch his attack. Social engineering is, however, not possible, unless the password system can be described. Hence the systems in table that can all be described are susceptible to social engineering attacks such as the passfaces scheme and the story scheme. Interestingly, of the three property based systems selected for security analysis, the Colour Model ‘Can be described’, as the images are mainly composed of coloured images of basic shapes, the Word Model is ‘Difficult to describe’ as it uses the relative positions of alphabetic letters within English words, and the Mixed Model ‘cannot be described’ as the properties in this model are composed of a mixture of patterns and colours that are difficult to understand. This is an amazing feature of the property based implementation and a proof that the significance of the property based authentication factor in the security of the system. The last column is designated as the ‘Main Security Concern’ and highlights security vulnerabilities of the system that can be exploited by attackers to gain access to the system. For click based graphical passwords such as passpoints and Blonder’s scheme, the problem of hotpots is the most compelling problem. For the passfaces scheme, the predictable patterns in image selection present the most compelling security problem. For the DAS passwords the appearance of symmetry and image centralization within the drawing grid present the most compelling issues, and in most other systems, the tendency that password login activity can be recorded remains of utmost concern. In spite of the tendency of most of the implementations of the property based concept to resist observational attacks, the tendency that screen activity can be recorded by either software, hardware or malware remains a disturbing issue. From the analysis of usability, the variation in security and usability of property based authentication systems is very glaring. In spite of their seeming similarity the variation in authentication factor has meant that property based systems are entirely different in both their usability characteristics and resilience to common attacks making them a unique variety of authentication systems with common and uncommon characteristics.

Scheme Name	Memory Type	Image Type	Image Selection	Registration Time	Login Time	Login Success Rate	Number of Images Needed	Target/Decoy Images	Constant Decoys	Ordered Login	Type of User Study
Draw a secret (DAS) [58,59, 61]	Recall	NA	Image Drawn by User	Not Reported	Not Reported	57-80%	None	None	None	NA	Paper Based
Signature [62]	Recall	NA	Signature Drawn by User	Not Reported	Not Reported	93%	None	None	None	NA	Lab
Passdoodle [60]	Recall	Doodle	Image Drawn by User	Not Reported	Not Reported	Not Reported	None	None	None	Yes	Paper Based
Passfaces [49]	Recognition	Face Images	System Assigned	180-300s	Not Reported	72-100%	9 per round, 4 rounds	1/8	No	No	Field
Déjà vu [7]	Recognition	Art, Picture, Abstract	User Selected	45s	32-36s	90-100%	100 Images	5/20	No	No	Lab – Multiple
Convex Hull [34,36]	Recognition	Icons	User Selected	Not Reported	24-150s	90.35%	112	5/43-112	No	NA	Lab – Multiple
Story [49,74]	Recognition	Picture Object	User Selected	42.9s	9.2-23.1	*85%	9 Images per Panel	4/5	No	Yes	Field
Cognitive [39]	Recognition	Picture Pseuso-word	System Assigned	2–3 Sessions	90-180s	>95%	*200	30-60/40-50	No	No	Not Specified
Blonder's Scheme [63]	Cued Recall	Picture	User Selected	No Study	No Study	No Study	1	NA	NA	Yes	No Study
Passpoints Scheme [67,69]	Cued Recall	Picture Object	User Selected	64.6s	8.78-24.25s	Not Reported	1	NA	NA	Yes	Lab – Multiple

Cued Click Points (CCP) [71]	Cued Recall	Picture	User Selected	24.7s	10.9s	83-98%	1	NA	NA	Yes	Lab
CDS [74]	Cued Recall	Picture Object	User Selected	49.5	13.7-19.8s	80%	24 images per Panel	5/19	No	Yes	Lab
BDAS [59]	Cued recall	Object	Image drawn by user	Not reported	Not reported	50-80%	None	None	None	Not Reported	Paper Based
Property Based Colour Model	Cued Recall	Art	†User Selected	79.8s	19.7	90-100%	200	1-4/3-96	No	Yes	Lab
Property Based Mixed Model	Cued Recall	Art	†User Selected	78.9s	37.8s	60-80%	200	1-4/3-96	No	Yes	Lab
Property Based Word Model	Cued Recall	Object Picture Word	†User Selected	37s	35.2s	85-95%	200	1-4/3-96	No	Yes	Lab

Table 7.6: Critical Usability Analysis of Existing Graphical Systems

Scheme Name	**Theoretical Password Space**	**Selection Patterns**	**Offline Attack**	**Shoulder Surfing**	**Guessability**	**Social Engineering**	**Main Security Concern**
Draw a secret (DAS) [56,59,61]	58 bits	None	Can be hashed	* One login	No	Can be sketched, difficult to verbally describe	*Image symmetry, stroking pattern, screen shot
Signature [62]	*Not Reported	None	Can be hashed	*Few login sessions	No	No	Screen shot
Passdoodle [60]	16 bits	Doodle may be personally identifiable	Doodle image must be available on system	*One login	*No	Can be sketched, difficult to verbally describe	Screen shots
Passfaces [49]	16 bits	Tends towards attractive and user’s race	Portfolio must be on system	*One login	Guessable due to unsafe selection trends	Images could be described	*Image selection tends towards attractive faces, members of the opposite sex and the user’s own race
Déjà vu [7]	15.6 bits	*Tend towards attractive images	Portfolio must be on system	*A few login sessions	No	*Abstract images cannot be described	*Recording of screen activity
Convex Hull [34,36]	32 bits	*None	Portfolio must be on system	*Several login sessions	No	No	Screen recording

Story [49]	12 bits	No	Portfolio must be on system	No	Difficult to guess	Images could be described	*Recording of screen activity
Cognitive [39]	10-73 bits	None	Portfolio must be on system	*A few logins	No	*Difficult to describe	*None
Blonder's Scheme [63]	Dependent on click point size.	Click points create hotspots	Can be hashed if system is offline	*One login	*Difficult to guess	*Difficult to describe	Problem of hotspots
Passpoints Scheme [67,68,69,72]	44 bits	Click points create hotspots	Can be hashed if system is offline	*One login	*Difficult to guess	*Difficult to describe	Hotspots problem
Cued Click Points (CCP) [71]	*Not reported	None	Can be hashed if system is offline	*Several logins	*Difficult to guess	*Difficult to describe	*Screen recording
CDS [74]	*Not reported	None	*None	Several logins	No	Images and system could be described	*None
BDAS [59]	61.8 bits	None	Can be hashed if system is offline	*Few logins	No	Can be sketched, difficult to verbally describe	Screen shot
Property Based Colour Model	18 bits	Non	Portfolio must be on system	Several logins	No	Can be described	*Screen recording
Property Based Mixed Model	18 bits	Non	Portfolio must be on system	Several logins	No	No	*Screen recording
Property Based Word Model	18 bits	Non	Portfolio must be on system	Several logins	No	Difficult to describe	*Screen recording

Table 7.7: Critical Security Analysis of Existing Graphical Systems

7.6 Conclusion

Considerable work has been conducted to compare the usability and security capabilities of graphical authentications systems. While the approach and metrics utilised in each of the studies differs significantly, most of the studies have considered the investigation of system vulnerabilities from the user side. Such vulnerabilities as brute force attack, dictionary attack, guessing attack, spyware attack, shoulder surfing attack as well as social engineering attack have been important security considerations for most of these studies. From the usability perspective, metrics such as the size of password space, the random assignment of images and image variation have been important security considerations.

The tendency to compare property based systems with other graphical password systems in these studies has made clear the security and usability advantages of the design and implementation of property based systems compared to other methods. Since these strengths are observed both on the security and usability aspects of authentication system design, one is tempted to believe that property based systems can finally bridge the gap in usability and security that has continued to frustrate usability and security practitioners since the commencement and advancement of research in graphical authentication systems. The disparity in these results as they relate to different implementations of the property based system in both usability and security is also a clear indication of the diversity in terms of usability and security in the vast implementation options available for these systems.

Chapter Eight – Conclusion and Future Work

8.1 Background

Security and usability are among the most important considerations in the development of computing systems, most especially the design of security systems for human users. Authentication is a part of usable security that deals with the access of computing systems and devices to legitimate users and deny such access to intruders. The most popular authentication systems to date are text based systems that use alphabetic letters, numbers, and special symbols to grant users access to computing devices.

Due to their vulnerabilities, however, security researchers continue to search for alternatives to replace alphanumeric passwords and PINs in granting access into computing systems and devices. Some of the alternative solutions considered are graphical authentications systems. These are systems by which access to computing systems is granted through the use of images and not alphanumeric text. Many graphical password systems have been proposed, some implemented, and some even commercialized. None of these systems, however, has been able to fully mitigate the usability and security issues that had plagued alphanumeric passwords and driven research interests into graphical passwords. In tackling these issues, however, researchers have focused more on the optimization of existing systems, merging old systems and multifactor authentication, among others, each with its merits and demerits, rather than concentrate on the development of newer and more efficient systems. The lingering contentions between usability and security in the provision of effective, efficient and secure systems are yet to be fully understood or fully addressed.

It is in the light of these prevailing issues that this work is focused towards an entirely new direction. Property based authentication is a novel hybrid authentication technique in which the characteristics of images are used as a factor for graphical authentication and not specific subsets of large image sets as used in existing recognition based authentication systems. In this work, the idea of property based authentication has been consistently studied, several versions of the system have been proposed and implemented. Several researchers have worked towards the provision of improvements to existing systems or making suggestions for better designs towards upgrading either usability or security features, normally to the detriment of the other, or to emphasize the need to allow multiple systems work together in the form of multifactor authentication systems, normally decreasing usability or introducing the need for additional devices, these works normally provide single alternatives or implementations. The idea of property based authentication can be seen as the introduction of a technique rather than a model, which will foster the development of newer and highly secure and highly usable systems.

The idea of the use of image properties for user authentication has enabled this work to provide fertile grounds for research and development into a novel class of authentications systems that hold substantial promise in the development and implementation of secure and usable systems. From the work conducted in this research, it is obvious that this systems can effectively mitigate the usability and security issues prevalent in existing systems as well as essentially combine usability and security features as never seen before in existing work.

8.2 Thesis Summary

This research is focused towards the design and development of a novel hybrid authentication system that could help mitigate problems associated with the usability and security of existing systems. In achieving this, a novel system referred to as ‘property based authentication’ has been proposed. It is a systems in which images are created and grouped based on common characteristics and the characteristics are then used in defining the factor for user authentication instead of picking individual images as has always been a tradition in existing recognition based graphical authentication systems. The work is implicitly divided into six parts, the first part being the introduction and conclusion (chapters 1 and 8) serving as gateways into and out of the presentation of the thesis, a literature review (chapter 2), provides details of existing research, and is the second part of the work. The third part (chapter 3) explains the principles and concepts of the design and implementation of property based authentication systems. The fourth part is the prototype design (chapter 4), explaining how the prototypes are constructed. The experimentation and results (chapters 5 and 6), represent the fourth part, detailing the format and findings of experiments conducted as part of the research work, and the comparative studies (chapter 7), makes a critical comparison of the performances of property based systems with those of existing systems and is the sixth part of the thesis.

The introductory part on the one hand provides a short introduction and overview of the thesis in relation to the aims and objectives of the study. It provides a highlight of the research question, states the main motivations for conducting the research, and provides an explanation of the research approach and methodology. The introduction also discusses the thesis structure, that is, how the chapters within the thesis are organised as well as the contributions of the project to existing knowledge. The conclusion on the other hand provides some background information about the reasons and motivations behind the introduction and development of property based authentication systems, a summary of the research thesis, as well as a summary of the research findings and their significance in relation to the objectives of the research. Other topics within the conclusion include demonstrations of how the research question has been answered and how the research objectives have been met. This part also provide a conclusion to the thesis and what future direction the idea of property base graphical authentication may likely take.

The part on literature review, the second part, is meant to provide a detailed review of existing authentication systems and research findings in the field of usable security to date. The chapter is explicitly divided into two parts, the literature review and the research review. The section on literature review discusses a number of topics which include a review of current authentication system methodologies, with details of their specific authentication factors; recognition, recall based or hybrid systems, their specific designs, and usability and security strengths and weaknesses. The section also provides an overview of common security attacks and then provides details of some of the attacks that have been considered and investigated in the course of the research work, such as the guessing attacks, shoulder surfing attacks and vulnerability to verbal and written descriptions. The section also discusses the significance of merging usability and security. The second section of the literature review provides a more detailed analysis of some of the authentication algorithms previously highlighted in the literature review.

The fourth part of the thesis, mainly the fourth chapter, discusses the operational procedure for each of the ten software prototypes or implementations of the property based algorithm studied in this research work. The main function of the chapter is to provide a glimpse into how the authentication systems studied in the project were designed. Thus, it provides pictorial representations, mainly screenshots, of the registration and authentication processes as they are conducted in each of the authentication system prototypes. A comprehensive overview of the idea of property based authentication, including the various modalities of implementation, various ideas, design concepts and principles, as well as possible extensions is provided in chapter 3.

The fifth part of the thesis comprises of chapters five and six that are used to provide details of the various experiments conducted as part of the research work. While chapter five discuss usability, chapter six discusses security. Chapter five starts with a brief overview of HCI usability evaluation and usability metrics, explaining the various metrics used in usability and memorability evaluations. In the case of each of the usability experiments conducted, the chapter provides sections that discuss the experimental hypotheses, research participants, experimental variables, materials and methods, experimental procedure as well as a detailed discussion of the results. The experiments were conducted to study main usability issues such as effectiveness, efficiency and user satisfaction, through usability measures such as login success rates, registration and login time collected from systems logs and qualitative data collected from survey questionnaires. Result analysis was made using Microsoft Excel and SPSS Statistics through the use of tables, charts, ANOVA, chi-square and Kruskal-Wallis tests. The chapter also analysed other concepts peculiar to property based systems such as the ordering of magnitude based systems and organised image selection. Chapter five deals with security issues and security experiments conducted in the course of the research work. The main issues investigated are those that have a direct bearing on the system user, such as vulnerability to guessing attacks, shoulder surfing and verbal and written descriptions.

The last part of the thesis consists of the chapter seven, used to conduct usability and security comparisons between property based systems and well known existing systems. The comparisons focus on usability issues such as recall rate, learnability and usability, and security issues such as password space and password image assignment as well as susceptibility to common attacks such as brute force attack, dictionary attack, guessing attack, spyware, shoulder surfing and social engineering. Tables have also been provided in this section which summarise the researcher’s critical comparison of property based systems against existing models.

8.3 Summary of Research Findings

A number of experiments were performed over several months to help ascertain the usability and security strengths and weaknesses of property based graphical authentication systems. Having developed the needed prototypes, it was paramount that the necessary experiments are performed to evaluate the extent to which these systems meet the research objectives and effectively answer the research questions.

In doing this, eight usability experiments were performed, four of the experiments were conducted to determine the variation in effectiveness, efficiency and user satisfaction among the various implementations of the property based graphical authentication paradigm. In order to capture and understand these metrics, researchers have to obtain data for login failure and success rates from the systems, as well as data pertaining to registration and authentication times, that is, data that shows the amount of time it takes for an average user to register onto the systems and to login to it. In both the quantification of effectiveness and efficiency also, subjective data on ease of use and ease to remember must be collected and analysed through well designed survey questionnaires.

It is in this regard that the first three experiments are designed to compare the relative effectiveness, efficiency and user satisfaction of the implementations of property based paradigm. The first experiment examined the variation in registration and authentication times between three implementations of property based systems. Two were fill based models, called the colour and pattern based models, while the third was a magnitude based model. The results suggests statistically significant variation in both the registration and login times between the colour based model and the pattern based model. The colour based model recorded lowest times in both registration and authentication, while the pattern based model recorded the highest.

Although experiments 2 and 3 were designed to evaluate the same set of parameters, being that the number of participants was not the same for the two experiments and a training session was introduced to experiment 3, it was not worthwhile to make a direct comparison between the two experiments. Experiment 2 used 15 participants for each authentication system, while experiment 3 used 20 participants for each authentication system. Experiment 2 compared the registration and authentication times of the first five models which include the colour, pattern, mixed, magnitude and butterfly models. Results for experiment 2 indicate that statistically significant mean variation did not exist between the groups in registration time, but statistically significant variation exists between the groups in terms of authentication time. Results showed that the mixed model (condition 3, M = 37862, SD = 17740), p=0.001 had the highest mean authentication time and had a statistically significant mean variation as compared to all the other models evaluated in the experiment.

The models evaluated in experiment 3 included the digit based model, the character based model, the form based model, the number representation based model and the word based model. Results for experiment 3 indicated that statistically significant mean variation existed between groups for both the registration and authentication times. In terms of the registration time, statistically significant mean variation occurred between the character based model (condition 6, M = 53165.25, SD = 13864.348) and the word based model (condition 10, M = 37023.70, SD = 14923.471), p =0.47 and between the digit based model (condition 10, M = 37023.70, SD = 14923.471), p =0.47 and the word based model (condition 10, M = 37023.70, SD = 14923.471), p =0.47, and in the authentication time the variation occurred between character base model (condition 6, M = 18054.60, SD = 9383.247) and the form based model (condition 9 M = 49785.00, SD = 32344.921), p = 0.007 and between the digit based model (condition 7, M = 27809.00, SD = 18517.177), p=0.007 and the form based model (condition 9 M = 49785.00, SD = 32344.921), p = 0..

Qualitative data for both experiments suggests that the all the models have enjoyed significant acceptance from the participants. The results show an above average performance for each of the metrics investigated, which include ease of use, ease of learning, security, registration time, authentication (or login) time and user satisfaction.

Experiment 4 is one of the experiment performed to evaluate the usability of property based systems alongside existing systems. It is a longitudinal experiment conducted to analyse the memorability of property based systems by use of login success rates. Four login sessions were organised for each participant within a period of four weeks. The models evaluated included the colour based model, the mixed model, the digit based model and the word based model. The results of the experiment showed that even at the fourth login session, each of the systems had a success rate of at least 60%. The login success rate had, however, reduced significantly between successive login sessions. A chi-square test indicated significant mean variation between the models, with the significance value decreasing steadily from p = 0.27 to p = 0.002, depicting an increased significance in variation across login sessions.

Experiment 5 is one of the experiments that seek to compare the performances of property based systems in terms of usability or the testing of ideas directly related to the design and implementation of property based systems. Experiment 5 is used to evaluate and compare mean login times when the size of the authentication grid is altered. Hence in the experiment, users logged onto computing systems using four grid sizes. Results of the experiment showed statistically significant mean variation between the grid size of 2, n=2 (condition 2, M = 17637.60, SD = 15851.669) and the grid size of 5, n=5 (condition 5, M = 36196.23, SD = 27092.755), with p = 0.038. Although there was a variation in mean login time between all grid sizes, which showed that mean login time increased with grid size, the variation was not statistically significant.

Experiment 6 was used to investigate the impact of object based ordering in magnitude based models. In the experiment, three implementations of the magnitude based model were used; an ordered model, an unordered model and a standard model. The essence was to investigate if significant variation will exist between the models with respect to login times. The experimental results indicated statistically significant mean variation in login times between the ordered model (model 11, M = 25086.03, SD = 18093.535) and the unordered (model 12, M = 37277.15, SD = 23347.476), p = 0.047. This result proved the usefulness of ordering as a concept.

Experiments 7 and 8 were designed to investigate the effects ‘organised image selection’ on two of the models. Experiment 7 investigates variation in login time between various image selection styles in the word based model, while experiment 8 investigates organised image selection in the colour based model. Although the results for experiment 7 showed some variation in mean login time between the various styles, the results were not statistically significant. In experiment 8, some statistically significant variation was recorded between the random painting style (condition 4, M = 25634.47, SD = 6598.242) and two other conditions. These were the outward painting style (condition 2, M = 15270.53, SD = 5450.910), p=0.003, and fixed painting style (condition 3, M = 15363.13, SD = 8314.870), p=0.004. This indicated significant time saving for organised image selection compared to random selection in concentric fill based models.

Seven (7) security related experiments were conducted in the course of the research. The first three experiments were to determine the vulnerability of the first set of property based systems developed to the shoulder surfing attack. The first experiment considers vulnerability of the authentication systems to shoulder surfing attacks considering a login session with only one authentication step. The second experiment considers their vulnerabilities to the shoulder surfing attacks for a login session with two authentication steps. The third experiment considers their vulnerabilities to shoulder surfing attacks for two login sessions of two authentication steps each. Seventy five (75) participants participated in each of the experiments.

The results for the experiment on the one step login indicated high login failure rate for the attackers. The system with the lowest login failure rate scored 73%, while the system with the highest login failure rate scored 100%. For the two step single login, four of the five models had a 100% login failure rate, while one of the systems had a 93% login failure rate. In the dual login observation experiment, results indicated two of the systems had 2 successful observation successes in their 15 trials giving them an 87% score. The other three systems all scored 100% failure rates. A chi-square test conducted on the results showed no correlation between the authentication systems investigated and the login failure rate.

The next experiment was performed to compare the guessability of five property based authentication systems on the basis that the user gives out a secret, either his favourite colour or favourite number, with which he had authenticated, depending on the implementation. One hundred (100) participants, twenty for each system, conducted the experiment. The results for the experiment showed that two (colour and mixed models) of the systems recorded three successful logins out of the total twenty for the trial giving each an 85% login failure rate, one of the systems (digit) had two login successes (90%), one (number representation) had one login success (95%), while one (magnitude model) recorded no login success (100%). The results showed that even giving out a user's favourite colour or number does not make property based systems vulnerable to guessing attacks.

The vulnerability of the second set (set 2) of developed prototypes to observational attacks (shoulder surfing) were conducted in the next experiment. Five property based models were evaluated which included the digit based, representation based, the form based, the text based and the word based models. The experiment had two parts, the first part of the experiment evaluated the vulnerabilities of the systems to observation on a single login session, while the second part of the experiment evaluated their vulnerabilities on dual login sessions. The results for the first part of the experiment recorded no login success (100% login failure rate) for four of the models (representation, form, character and word) and a single login success for the digit based model (95% login failure rate). The results for the second part of the experiment recorded no login success for two (representation and word based models) of the models evaluated. Two other models (the character and the form) recorded two login successes each (95% login failure rate) and one model (the digit based model) recorded two login successes (90% login failure rate).

Two experiments were then performed to ascertain the vulnerabilities of the systems to the verbal and written description of the users' passwords. The results indicated a high degree of vulnerability to descriptive attacks among various implementations. In the vulnerability evaluation for verbal descriptions, one of the models (the mixed model) recorded 40% login success rate, the magnitude model recorded 50% login success rate, while the rest four models scored 60% and above. The most vulnerable to verbal descriptions was the digit based model that scored 75% success. The results for written description was slightly better than that for verbal descriptions. In the vulnerability test for written descriptions, the mixed model scored 35% login success rate, the magnitude model scored 45%, pattern based model scored 50%, the representation model scored 55%, and two models (digit and colour based models) each scored 65% login success rates.

8.4 Significance of Research Findings

The experiments have looked into usability and security issues that are of the greatest interest in the design and use of authentication systems in general, but specifically to graphical authentication systems. In terms of usability, probably the most important achievement of these systems from empirical results is that the idea of property based authentication (the use of image properties for user authentication) is a feasible concept. All five schemes proposed for the system have been implemented and evaluated. The different implementations (sub-classes) suggested for the schemes have also been implemented and evaluated. The fill based scheme alone has been evaluated with four models, the number based scheme with two, the text based scheme with two models, and the magnitude and form based schemes with one model each. The introduction of yet another *class* of authentication systems alone is a great achievement in graphical authentication systems research.

The usability experiments conducted have demonstrated strong usability for property based authentication systems in all the experiments performed. The usability experiments that have compared property based systems have proven that although the systems showed significant mean variation among the different implementations in registration and authentication times in some of the experiments, all systems recorded satisfactory registration and authentication times. From the data, experiment 1 had a mean registration time as 80s, and mean login time as 26s, while experiment 2 shows mean registration time as 57s and mean login time as 33s, from this it can be deduced that on the average, a user can register and authenticate on a property based system in about 1½ minutes. As compared to other models in section 6.5, property based models have better login times when compared to most other models. The participants enjoyed using the system. This was very obvious from the interaction in the lab to their scores on the questionnaire. From the questionnaire, the various usability parameters were each scored more than 80% in experiment 2. The memorability for property based models has also proven to be very high, with lowest in recall rate tested in experiment 4 scoring 60%, the rest scoring above 80% (≥ 85%).

A significant improvement to existing systems is that in property based systems, a user can choose his preferred grid size among several grid sizes. Experiment 5 was a usability experiment that compared mean login times among the various grid sizes. It recorded statistically significant variation among grid sizes. Also, as expected, the results showed that the larger the grid size, the more time it takes to identify a user's pass images. It is also expected that larger grid sizes will provide higher security. This, however, is subject to future research.

Property based systems also allow users to make their own choices of authenticator images. Since the images are not definite images of objects, and hence the user depends on both recognition and recall, the idea of '*organised image selection'* may give users some support in terms of the memorability of password images. Experiments 7 and 8 both evaluated the effects of organised image selection on the login times of word based and a fill based (colour based) models. Experiment 7, on the one hand, showed slight variation in login times between the different image selection styles, but the results were not statistically significant. Experiment 8, on the other hand, found statistically significant mean variation between the fixed painting style and random painting style, supporting the idea of time saving in organised image selection.

The security experiments conducted as part of this work have proven the strength of property based systems against common attacks. The first set of experiments evaluated the performances of property based systems against observational attacks. Three login scenarios were investigated; one step login, 2 steps login and dual login scenarios. The results indicated that even for the one step login scenario, the lowest (most vulnerable to observational attacks) scored a failure login rate of 73%. This is a very exciting performance, suggesting that even for one step login, property based systems will display a resilience to observational attacks. Total login failure (100%) was recorded for four out of the five systems evaluated in the single two-step login. This is proof to extraordinary resilience of property based systems to observational attacks. To provide better chances for observational attacks, the dual login test was conducted. This was to increase the chances of the attacker since he focusses on the interface twice. Yet, three out of five systems recorded 100 failure rate.

The guessability experiment also proved the resilience of property based systems to guessing attacks even when the attackers were armed with some advantaged information about the user's chosen image. The information shared in the experiment were the user's favourite colour or favourite number with which each user was asked to register. Armed with this information, yet the attackers' login failure rates among the five systems evaluated was ≥ 85%.

Amazingly, the observational experiments for the second set of property based systems conducted also recorded an extraordinary performance with four of the five systems tested scoring a 100% login failure rate, with a single system being the lowest, scoring a 95% login failure rate. The dual login sessions for the same set of models indicate a 100% login failure rate for two models, a 95% login failure rate for two other models, and 90% login failure rate for the fifth and lowest model. This was also an amazingly high performance.

The experiments for vulnerability to verbal and written descriptions bring to light the tendency that property based systems may be vulnerable to attacks due to verbal and written descriptions. Vulnerability to description is the key ingredient for vulnerability to social engineering attacks. By its nature, social engineering cannot take place unless passwords can be effectively described. The results for the verbal description experiment showed that one of the models (the mixed model) scored a 40% guess success rate. The remaining models scored 50% and above. In the experiment for written descriptions, the mixed model had 35% login success rate, and the magnitude based model had 45% login success rate. The remaining had success rates of 50% and above. This shows that a *majority* of the systems were vulnerable to attacks due to verbal and written descriptions. It is significant not to forget, however, that a 35% guess success rate, as in the case of the mixed model for written descriptions, is also a 65% guess failure rate. Hence the results clearly show that depending on the implementation, some property based models may not be susceptible to social engineering attacks.

Experiments on usability have proven the strength of property based systems. From the mean registration times and the mean login times to other aspects of usability such as memorability and interpretation of qualitative data. This is also proven by the comparisons on chapter 6. The security experiments conducted have also displayed the strength of property based systems in terms of security. Hence it only seems plausible to conclude that property based authentication is the ideal concept that bridges the usability and security gap that has existed since the inception of existing graphical and non-graphical authentication systems.

8.5 Answering the Research Question

In the first chapter, the research question was stated as:

"Can images, assigned properties and associated variants, be used in user authentication as hybrid graphical authentication systems to effectively combine usability and security"?

This question is made up of two parts. The first part of this question is concerned with the tendency that properties can be used for user authentication. The second part is concerned with the tendency that such systems can combine usability with security.

The experiments conducted have very strongly suggest that property based authentication is indeed a very effective method for user authentication. Hence the part of the question doubting the use of image properties and variants for user authentication is answered. They definitely can be used for user authentication. Concerning the second part, since property based systems have proven to be both highly usable and highly secure, the second part of the question that shows a reservation for the ability of property based systems to effectively combine usability and security has also been answered. These system can effectively combine usability and security as expected of an 'ideal' authentication system.

8.6 Meeting the Research Objectives

From chapter 1, the aim of the research is stated as “to develop a more efficient hybrid graphical authentication technique that can utilize both recognition and recall as an effective means of combining usability and security as well as to build a concise conceptual model of the system”.

This aim is broken into a number of objectives. These include:

1. To investigate usability and security issues in relation to currently developed (existing) graphical authentication systems.
2. To develop alternative novel system towards improving usability and security.
3. To identify the various possible approaches towards the implementation of the new system
4. To empirically evaluate the performances of the new system
5. To evaluate novel ideas developed in the course of objective 2 so as to determine their effects on system performance
6. To develop a concise conceptual model for the implementation of the system.

Each of the above objective has been addressed in the course of the research work. To ascertain the extent to which each of the objectives is addressed, it is important to review them one after the other.

The first objective has been addressed through an extensive literature search. Chapter two provides a comprehensive overview of graphical authentication systems from existing literature. The trend in the development of authentication systems had been outlined, stating the usability and security strengths and weaknesses of each of the models.

For the second objectives, the researchers have looked into the concept of property based authentication, a hybrid graphical authentication system that seeks to combine the potentialities of recognition and recall. It is a system whereby a set of properties is identified and images are built based on these properties. Each image in a property based system is unique.

In identifying the various possible approaches towards the implementation of the new system, the various classes by which property based systems could be implemented have been identified. Twelve versions in all have been implemented and evaluated in the course of the numerous experiments conducted in the research work.

For the fourth objective, numerous usability and security evaluations have been conducted on each of the authentication models. These has helped the researchers in understanding the relative performances of the systems. The results shall go a long in helping users make better choices in the actual implementations of the systems as well as providing fertile grounds for future and more in-depth research.

For the fifth objective, a number of ideas and concepts that have been evolved in the course of the research have been evaluated. The effects of grid size on mean authentication time has been evaluated, the effect of object based ordering on the magnitude based model has been evaluated. The effects of organised image selection on the word and fill based models has also been evaluated.

For the sixth objective, a concise conceptual model and overview has been provided and is presented in appendix 1. The overview will help anyone interested in the ideas of property based authentication to have a better hold of the basic and fundamental concepts.

8.7 Limitations

The PhD is a highly constrained endeavor and arguably the most important of these constraints is the time factor. Whatever one has in mind must be organised and conducted within a specific period of time. Hence all work has to be contained, managed and organised to meet stringent deadlines. The stringent deadline does not give room for delays and hence sometimes the researcher has to make do with whatever he can lay his hands on. This puts one in a particularly difficult situation when a decision has to be made that can affect the integrity or accuracy of your results. A particular instance of this is in getting the right participant population for research. Recruiting an adequate participant population is a difficult task. This is further worsened by students' busy schedules as some of them abandon the work halfway into it. Ethical issues further tighten the situation as they must be informed of their rights to voluntary withdrawal.

As a common problem with research using study participants, many of the participants drop out of the experiment at the middle and sometimes even approaching the end of the experiments. At time an entire experiment has to be repeated. Organizing many students in lab based experiments may sometimes be difficult and tedious.

Although a lot of effort was made to ensure that as much is covered as possible in the implementation and of these systems as well as the evaluation of concepts and ideas that have evolved in the course of the work, the timing constraint associated with doctoral work meant a considerable amount of work initially planned will have to be moved to future work, to be conducted at a later time. The possibility of conducing field and web based trials was also not possible due to the same constraints.

As there are many parameters to work with, some of the variables have to be contained and used only as control variables if they have to be used. Else they become confounding variables and alter the validity of the results. Hence, except for the purpose of furthering research, the researchers have consistently used 2 as the number of steps for each user password, and have also consistently used a grid size of 9. Also in all implementations of the property based model, the number of properties provided for user password creation is three.

8.8 Future Work

Although this work set out to develop and investigate some advanced models of the property based implementation, this has not been possible due to timing constraints. Two advanced models had initially been selected for development and evaluation; the net based models and the directional model (both in appendix 1). This work is has been left as a future course.

Due to the nature of the work and the timing constraints, all experiments conducted have been lab based. It is significant that field and web based tests of these systems be conducted with larger user populations. Field and web trials are good for data analysis due to the large populations involved, this is although, is at the expense of control.

There is great likelihood that several classes, models or advanced versions of the systems be developed in the future, the behaviour of these systems is highly uncertain and must be subject to whole new set of evaluations. Even with the experiments conducted in this research, only selected systems were tested in most of the experiments due to timing constraints. It will be interesting to discover the outcomes of the evaluations of those systems that have not been evaluated.

8.8 Conclusion

This research work has been focused on the development and evaluation of a hybrid property based graphical authentication system. Essentially, the system combines the elements of recognition and recall as recall based systems are believed to be more secure, while recognition based systems are believed to be more usable. A bridge between the two systems is likely to yield good usability as well as good security. In developing this idea, a conceptual model for the systems has been built and several models of the system have been developed and implemented. Significant usability and security evaluations on the systems have also been conducted.

From the results of usability experiments conducted, it is obvious that property based systems have very high usability. The registration and authentication times of the systems were considerably better than those of most existing graphical authentication systems. They also have good memorability and are scored very high by research participants in the qualitative data collected through research questionnaires. Property based systems have also proven to be exceptionally good in security. The systems displayed very high resilience to all form of guessing and observational attacks. Even for observational experiments with two login sessions, they maintained a login failure rate of more than eighty percent. Their main weakness discovered from the results is their susceptibility to description based attacks, and hence a tendency to be vulnerability to social engineering attack.

From the results, there is much hope that these systems will very much be able to mitigate the usability and security contention that has existed and continues to exist in the design and implementation of authentication techniques and to provide ideal systems that can be used easily, efficiently, securely. Considerable field and web based evaluations still need to be conducted though, with much larger populations to be able to evaluate the actual and comparative potentialities of these systems.

References

[1]. Y. Rogers, H. Sharp and J. Preece. Interaction Design. Beyond Human Computer Interaction. (3rd Ed). John Wiley and Sons; 2011

[2]. D. Benyon. Designing Interactive Systems. (2nd Ed) Pearson Educational. Essex; 2010.

[3]. A. J. M. Carroll. Human Computer Interaction - brief intro. In: Soegaard, Mads and Dam, Rikke Friis (Eds.). "The Encyclopedia of Human-Computer Interaction, 2nd Ed." Aarhus, Denmark, 2014, The Interaction Design Foundation. [Available online] at https://www.interaction-design.org/encyclopedia/human_computer_ interaction_hci.html [Accessed 5 August, 2015]

[4]. S. Patrick, A. C. Long and S. Flinn "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[5]. A. Adams, and M. A. Sasse, "Users are not the enemy". *Communications of the ACM, 42*(12), 40-46, 1999.

[6]. M. A. F. Al-Husainy and R. A. Malih "Using Emoji Pictures to Strengthen the Immunity of Passwords against Attackers" European Scientific Journal vol.11, No.30 October 2015

[7]. R. Dhamija and A Perrig "Déjà Vu-A User Study: Using Images for Authentication" In *USENIX Security Symposium* vol. 9, August, 2000.

[8]. W. C. Summers and E. Bosworth, "Password policy: the good, the bad, and the ugly," In *Proceedings of the winter international symposium on Information and communication technologies,* Cancun, Mexico, 2004.

[9]. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes". In *IEEE Symposium on Security and Privacy*, 2012

[10]. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33, pp. 168-176, 2000.

[11]. R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

[12]. S. Saeed and M. S. Umar. "A hybrid graphical user authentication scheme." In *Communication, Control and Intelligent Systems (CCIS),* (pp. 411-415). IEEE. November, 2015.

[13]. P. Dunphy, A. P Heiner, and N Asokan. "A closer look at recognition based graphical passwords on mobile devices". In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 3). ACM, July, 2010.

[14]. C. Singh and L. Singh "Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience". *International Journal of Network Security & Its Applications (IJNSA), 3*(2), March 2011.

[15]. M. Z. Jali "A Study of Graphical Alternatives for User Authentication." PhD Thesis, University of Plymouth. 2011.

[16]. S. Chowdhury "Exploring the Memorability of Multiple Recognition-Based Graphical Passwords and their Resistance to Guessability Attacks." PhD diss., University of Glasgow, 2015.

[17]. S. Chowdhury, R. Poet and L. Mackenzie. "A study of mnemonic image passwords." In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*, pp. 207-214. IEEE, 2014.

[18]. P. Dunphy "Usable, Secure and Deployable Graphical Passwords." PhD Thesis, School of Computing Science, Newcastle University, 2012.

[19]. S. Chiasson "Usable authentication and click-based graphical passwords." PhD Thesis, School of Computer Science, Carleton University, 2008.

[20]. A. H. Lashkari, D Saleh, S Farmand, D Zakaria, and O. Bin. "A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns". *arXiv preprint arXiv:1001.1962.*, 2010

[21]. E. Hayashi, R Dhamija, N. Christin, and A. Perrig. "Use your illusion: secure authentication usable anywhere". In *Proceedings of the 4th Symposium on Usable Privacy and Security* (pp. 35-45). ACM, July, 2008.

[22]. R. C. Atkinson and R. M. Shiffrin "Human memory: A proposed system and its control processes". In *Psychology of learning and motivation* (Vol. 2, pp. 89-195). Academic Press. 1968.

[23]. H. P. Bahrick "Semantic memory content in permastore: Fifty years of memory for Spanish learned in school". In *Journal of Verbal Learning and Verbal Behavior* 14 1-24. 1984.

[24]. T. J. Wixted "The psychology and neuroscience of forgetting". *Annual Review of Psychology* 55 235-269, 2004.

[25]. D. J. Rundus "Analysis of rehearsal processes in free recall". *Journal of Experimental Psychology* 89, 63-77, 1971.

[26]. B. Coskun and C. Herley "Can "Something You Know" Be Saved?" In *ISC* (Vol. 8, pp. 421-440). September, 2008.

[27]. A. De Luca, M. Denzel and H. Hussmann “Look into my eyes!: Can you guess my password?.” In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 7). ACM. July, 2009.

[28]. D. Gafurov, E. Snekkenes and P. Bours “Spoof attacks on gait authentication system”. IEEE Transactions on Information Forensics and Security, 2(3), Special Issue on Human Detection and Recognition. 2007

[29]. M. Babaeizadeh, M. Bakhtiari and A. M. Mohammed “Authentication Methods in Cloud Computing: A Survey” Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015

[30]. E. Hayashi and J. I. Hong, “A Diary Study of Password Usage in Daily Life,” In *Proceedings of the 29th Annual Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada, May 2011.

[31]. M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, “Towards identifying usability and security features of graphical password in knowledge based authentication technique”. In *Modeling & Simulation. AICMS 08. Second Asia International Conference on* (pp. 396-403). IEEE, May 2008.

[32]. G. Devansh "A new approach of authentication in graphical systems using ASCII submission of values."*Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017.

[33]. H. Zhao and X. Li “S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme.” In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on* (Vol. 2, pp. 467-472). IEEE, May 2007.

[34]. S. Saeed and M. S. Umar. “A hybrid graphical user authentication scheme.” In *Communication, Control and Intelligent Systems (CCIS),* (pp. 411-415). IEEE. November, 2015.

[35]. A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.

[36]. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," In *Proceedings of Midwest Instruction and Computing Symposium*, 2004.

[37]. S. Chowdhury and R. Poet “Comparing the usability of doodle and Mikon images to be used as authenticators in graphical authentication systems”. In *Proceeding of Conference on User science and Engineering,* pp. 54-58, 2011

[38]. S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget “Design and evaluation of a shoulder-surfing resistant graphical password scheme.” In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184). ACM, May 2006.

[39]. D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, pp. 1399-1402., 2004

[40]. L. Sobrado and J. C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[41]. F. Tari, A. Ozok and S. H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords". In *Proceedings of the second symposium on Usable privacy and security* (pp. 56-66). ACM. July, 2006.

[42]. R. Poet and K. Renaud. “A Mechanism for Filtering Distractors for Graphical Passwords”. In 13th Conference of the International Graphonomics Society Melbourne, Australia, volume 11, pg 14, 2007

[43]. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme – WIW" in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[44]. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2004.

[45]. Passfaces: Two factor authentication for the enterprise". [Available online] at www.realuser.com, (Accessed July 2015)

[46]. T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London, 1998.

[47]. T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London, 1999.

[48]. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in *People and Computers XIV - Usability or Else: Proceedings of HCI*. Sunderland, UK: Springer-Verlag, 2000.

[49]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Usenix Security Symposium*. San Diego, CA, 2004.

[50]. P. Dunphy, J. Nicholson, and P. Olivier. "Securing passfaces for description." In *Proceedings of the 4th symposium on Usable privacy and security*, pp. 24-35. ACM, 2008.

[51]. W. Jansen, "Authenticating Mobile Device Users through Image Selection," in *Data Security*, 2004.

[52]. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[53]. W. A. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[54]. T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," In *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[55]. X. Suo, Y. Zhu and G. S. Owen Graphical passwords: A survey. In *21st annual Computer security applications conference* (pp. 10-pp). IEEE, 2005.

[56]. I. H. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," In *Proceedings of the 8th USENIX Security Symposium*, 1999.

[57]. J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," In *Proceedings of the 13th USENIX Security Symposium*. San Deigo, USA: USENIX, 2004.

[58]. J. Thorpe and P. C. van Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *20th Annual Computer Security Applications Conference (ACSAC)*. Tucson, USA. IEEE, 2004.

[59]. P. Dunphy, and J. Yan. "Do background images improve Draw a Secret graphical passwords?" In *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 36-47. ACM, 2007.

[60]. J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," In *Proceedings of Human Factors in Computing Systems (CHI)*, Minneapolis, Minnesota, USA, 2002.

[61]. D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada, May 2004.

[62]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," In *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer- Verlag Lecture Notes in Computer Science (1438), pp. 403441, 1998

[63]. G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ,* U. S. Patent, Ed. United States, 16.

[64]. M. R. Albayati and A. H. Lashkari. “A New Graphical Password Based on Decoy Image Portions (GP-DIP). In *International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2014* (pp. 295-298). IEEE. September, 2014.

[65]. A. H Lashkari, A. Gani, L. G Sabet, & S. Farmand "A new algorithm on Graphical User Authentication (GUA) based on multi-line grids" In *Scientific Research and Essays, 5*(24), 3865-3875., 2010.

[66]. D. Paulson, "Taking a Graphical Approach to the Password," *Computer,* vol. 35, pp. 19, 2002.

[67]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," In *Human-Computer Interaction International (HCII 2005).* Las Vegas, NV, 2005.

[68]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," In *Symposium on Usable Privacy and Security (SOUPS).* Carnegie-Mellon University, Pittsburgh, 2005.

[69]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system, "*International Journal of Human Computer Studies 63*(1), 102-127, 2005 .

[70]. J. C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical passwords," *Cryptology ePrint archive,* 2003.

[71]. S Chiasson, van P. C. Oorschot, and R. Biddle. "Graphical password authentication using cued click points". In *Computer Security–ESORICS 2007* (pp. 359-374). Springer Berlin Heidelberg, 2007.

[72]. P. C. van Oorschot and J. Thorpe. "Exploiting predictability in click-based graphical passwords", *Journal of Computer Security:* 19(4):669–702, 2011.

[73]. W. Moncur, and G. Leplâtre. "Pictures at the ATM: exploring the usability of multiple graphical passwords". In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 887-894). ACM. April, 2007.

[74]. H. Gao, Z. Ren, X. Chang, X. Liu and U. Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing”, *International Conference on Cyberworlds*. 2010, IEEE: Singapore pp. 194 – 199, 2010.

[75]. A. Haque and B. Imam "A New Graphical Password: Combination of Recall and Recognition Based Approach" *International Journal of Computer, Electrical, Automation, Control and Information Engineering* Vol: 8, No:2, 2014

[76]. M. Sreelatha, M. Shashi, M. Anirudh, et al. "Authentication schemes for session passwords using color and images." In *International Journal of Network Security & Its Applications, 3*(3), 111-119. 2011.

[77]. S. Saeed and M. S. Umar "A hybrid graphical user authentication scheme". In *Communication, Control and Intelligent Systems (CCIS),* (pp. 411-415). IEEE, November 2015.

[78]. N. P. Sachin, D. V. Panjabi "An Overview: Passwords using Text, Color and Images Techniques Discussion, Implementation and Comparison". In *International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Computer Technology* NCETCT, 2014.

[79]. M. S. Tidke, M. N. Khan and M. S. Balpande "Password Authentication Using Text and Colors." *Computer Engneering, Rtm Nagpur University, Miet Bhandara*. 2015.

[80]. Z. Zheng, X. Liu, L. Yin and Z. Liu "A Hybrid Password Authentication Scheme Based on Shape and Text". *JCP, 5*(5), 765-772. 2010

[81]. P. C. Van Oorschot, and T. Wan "TwoStep: An Authentication Method Combining Text and Graphical Passwords". *MCETECH*, 233-239. 2009.

[82]. G. Yang, D. S. Wong, H. Wang and X. Deng "Two-factor mutual authentication based on smart cards and passwords" *Journal of Computer and System Sciences*, *74*(7), 1160-1172, 2008.

[83]. A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition, 37*(11), 2245-2255., 2004.

[84]. T. Hoang and D. Choi "Secure and privacy enhanced gait authentication on smart phone" *The Scientific World Journal*, 2014.

[85]. S. Abu-Nimeh, "Three-Factor Authentication." In *Encyclopedia of Cryptography and Security* (pp. 1287-1288), Springer, US. 2011.

[86]. J. Brainard, A. Juels, R. L Rivest, et al. "Fourth-factor authentication: somebody you know". In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 168-178). ACM. October, 2006.

[87]. E. von Zezschwitz, A. Koslow, A. De Luca and H. Hussmann. "Making graphic-based authentication secure against smudge attacks". In *Proceedings of the International Conference on Intelligent User Interfaces 277–286.*, 2013.

[88]. S. Chowdhury, R. Poet, and L. Mackenzie "Exploring the Guessability of Image Passwords Using Verbal Descriptions". In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 768-775). IEEE, July 2013.

[89]. A. De Angeli, L. Coventry, G. Johnson and K. Renaud "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems" *International journal of human-computer studies*, *63*(1), 128-152. 2005

[90]. M. E. Zurko and R. T. Simon "User-centered security". In *Proceedings of the 1996 workshop on new security paradigms* (pp. 27-33). ACM. September, 1996.

[91]. M. A. Sasse, S. Brostoff, and D. Weirich "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." *BT technology journal*, *19*(3), 122-131. 2001.

[92]. S. L. Pfleeger, M. A. Sasse and A. Furnham "From weakest link to security hero: Transforming staff security behavior." *Journal of Homeland Security and Emergency Management*, *11*(4), 489-510. 2014.

[93]. A. Adams and M. A. Sasse "Users are not the enemy". In *Communications of the ACM*, *42*(12), 40-46. 1999.

[94]. K. Renaud, P. Mayer, M. Volkamer, and J. Maguire "Are graphical authentication mechanisms as strong as passwords?" In *Federated Conference on Computer Science and Information Systems (FedCSIS),* (pp. 837-844). IEEE, September 2013.

[95]. S. Komanduri, R. Shay, P. G. Kelley et al. "Of passwords and people: measuring the effect of password-composition policies." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). ACM. May, 2011

[96]. L. Lamport "Password authentication with insecure communication" In *Communications of the ACM, 24* (11), 770-772. 1981.

[97]. W. C. Summers and E. Bosworth. "Password policy: the good, the bad, and the ugly." In *Proceedings of the winter international symposium on Information and communication technologies,* pp. 1-6. Trinity College Dublin, 2004.

[98]. J. Bonneau, S. Preibusch and R. J. Anderson "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs". In *Financial Cryptography* (Vol. 7397, pp. 25-40). March, 2012

[99]. B. Ives, K. R. Walsh and H. Schneider "The domino effect of password reuse." In *Communications of the ACM, 47*(4), 75-78. 2004.

[100]. M. Golla, D. V. Bailey and M. Dürmuth "I want my money back! Limiting Online Password-Guessing Financially." In *Symposium on Usable Privacy and Security (SOUPS).* July, 2017.

[101]. G. C. Kessler "Passwords – strengths and weaknesses" *Online Available at https://www.garykessler.net/library/password.html* Accessed October, 15th 2017.

[102]. L. Gong "Optimal Authentication Protocols Resistant to Password Guessing Attacks." In *Proceedings of the Computer Security Foundations Workshop, 1995. Eighth IEEE* (pp. 24-29). IEEE. June, 1995.

[103]. P. Biswas, M. M. Patil, and M. Biswas "Reduction of Password Guessing Attacks using Click Point". In *International Journal of Computer Applications (IJCA) (0975 – 8887) Proceedings on Emerging Trends in Electronics and Telecommunication Engineering (NCET).* 2013.

[104]. T. Kwon and J. Song "Efficient and secure password-based authentication protocols against guessing attacks" *Computer communications, 21*(9), 853-861, 1998.

[105]. S. M. Bellovin and M. Merritt "Encrypted key exchange: Password-based protocols secure against dictionary attacks" In *Research in Security and Privacy, 1992. Proceedings, 1992 IEEE Computer Society Symposium on*(pp. 72-84). IEEE. May, 1992.

[106]. H. K. Sarohi, and F. U. Khan "Graphical password authentication schemes: current status and key issues". *Int. Journal of Engineering and Innovative Technol. (IJEIT), 10*(2). 2013.

[107]. S. Chiasson, A. Forget, E. Stobert et al., "Multiple password interference in text passwords and click-based graphical passwords" In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 500-511). ACM. November, 2009.

[108]. K. Chalkias, A. Alexiadis, and G. Stephanides "A multi-grid graphical password scheme" In *Proceedings of the 6th International Conference on Artificial Intelligence and Digital Communications, Thessaloniki,* (pp. 1-11). *Greece,* August, 2006.

[109]. A. H. Lashkari, S. Farmand, D. Zakaria et al. "Shoulder surfing attack in graphical password authentication."*arXiv preprint arXiv:0912.0951*. 2009.

[110]. F. Aloul, S. Zahidi and W. El-Hajj "Two factor authentication using mobile phones." In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* (pp. 641-644). IEEE. May, 2009.

[111]. K. Krombholz, H. Hobel, M. Huber, and E. Weippl "Advanced social engineering attacks" In *Journal of Information Security and applications*, *22*, 113-122. 2015.

[112]. K. Ivaturi and L. Janczewski “A taxonomy for social engineering attacks.” In *International Conference on Information Resources Management*. Centre for Information Technology, Organizations, and People. June, 2011.

[113]. R. B. Basnet, S. Mukkamala, and A. H. Sung “Detection of Phishing Attacks: A Machine Learning Approach” In *Soft Computing Applications in Industry*, *226*, 373-383. 2008.

[114]. A. Ross et al. “Measuring the cost of cybercrime” In *11th Workshop on the Economics of Information Security*, Berlin, Germany. June, 2012.

[115]. S. Garera, N. Provos, M. Chew and A. D. Rubin “A framework for detection and measurement of phishing attacks.” In *Proceedings of the 2007 ACM workshop on Recurring malcode* (pp. 1-8). ACM. November, 2007.

[116]. J. Hong “The Current state of phishing attacks” In *Communications of the ACM*, *55*(1), 74-81. 2012.

[117]. Z. Ramzan, and C. Wüest “Phishing Attacks: Analyzing Trends in 2006” In *CEAS*. August, 2007.

[118]. A. Litan “Phishing attack victims likely targets for identity theft” Online available at https://www.social-engineer.org/wiki/archives/IdTheif/IdTheif-phishing_attack.pdf Accessed 15 November, 2017.

[119]. M. Jakobsson “Modeling and preventing phishing attacks” In *Financial Cryptography* (Vol. 5). February, 2005.

[120]. P. P. Ray “Ray’s scheme: Graphical password based hybrid authentication system for smart hand held devices.” In *Journal of Information engineering and Applications*, *2*(2), 1-12. 2012.

[121]. N. A. G. Arachchilage and S. Love “Security awareness of computer users: A phishing threat avoidance perspective” *Computers in Human Behavior, 38*, 304-312. 2014.

[122]. F. A. Aloul “Information security awareness in UAE: A survey paper.” In *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for* (pp. 1-6). IEEE. November, 2010

[123]. M. Masrom, F. Towhidi, and A. H Lashkari. "Pure and cued recall-based graphical user authentication". In *3rd International Conference on Application of Information and Communication Technologies, 2009. AICT 2009.* (pp. 1-6). IEEE, October 2009.

[124]. A. H. Lashkari, R. Saleh, F. Towhidi, and S. Farmand. "A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms". In *Second International Conference on Computer and Electrical Engineering*. 2009; Volume 1():527 - 542. IEEE., 2009

[125]. S. Chiasson, A. Forget, R. Biddle, and P. C van Oorschot. "User interface design affects security: Patterns in click-based graphical passwords". *International Journal of Information Security*, *8*(6), 387-398. 2009.

[126]. F. Towhidi, M. Masrom and A. A. Manaf. "An enhancement on Passface graphical password authentication". *Journal of Basic and Applied Scientific Research*, vol. 2, no. 2, 2013

[127]. R. English, "Modelling the security of recognition-based graphical password schemes," PhD Thesis, School of Computing Science, University of Glasgow., Glasgow, 2012.

[128]. J. W. Sparks, "The Impact of Image Synonyms in Graphical-Based Authentication Systems" PhD Thesis, College of Engineering and Computing, Nova Southeastern University, Florida, USA, March 2015.

[129]. Y. Meng, and L. Wenjuan. "Enhancing click-draw based graphical passwords using multi-touch on mobile phones." In *IFIP International Information Security Conference*, pp. 55-68. Springer, Berlin, Heidelberg, 2013.

[130]. R. Biddle, S. Chiasson and P. C. Van Oorschot "Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), 19. 2012

[131]. A. E. Dirik, N. Memon and J. C. Birget "Modeling user choice in the PassPoints graphical password scheme" In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 20-28). ACM. July, 2007

[132]. S. Chiasson, E. Stobert, A. Forget et al. "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism." In *IEEE Transactions on Dependable and Secure Computing*, *9*(2), 222-235., 2012.

[133]. J. Nicholson, L. Coventry and P. Briggs "Age-related performance issues for PIN and face-based authentication systems." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 323-332). ACM. April, 2013.

[134]. T. Naik and S. Koul "Multi-dimensional and Multi-level Authentication Techniques", International Journal of Computer Applications, Vol 75, 2013

[135]. V. K. Agrawa, "Multi-dimensional password generation technique for accessing cloud services." *arXiv preprint arXiv: 1207.3636*, 2012.

[136]. S. A. Pirayesh and A. Stavrou. "Universal multi-factor authentication using graphical passwords." International Conference on Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE, pp. 625-632. IEEE, 2008.

[137]. R. Gosavi, K. K. Mangalgire, N. P. Nandawadekar, K. P. Phadatare and A. Jajoo "Authentication System Using Sound Signature and Graphical Password". International

Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 2, Special Issue (NCRTIT 2015), January 2015.

[138]. N. Gunson, D. Marshall, H. Morton and M. Jack "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking" *Computers & Security, 30*(4), 208-220. 2011.

[139]. J. Kjeldskov, M. B. Skov and J. Stage "Instant data analysis: conducting usability evaluations in a day". In *Proceedings of the third Nordic conference on Human-computer interaction* (pp. 233-240) ACM, October 2004.

[140]. W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur and M. L. Mazurek "Usability and security of text passwords on mobile devices". In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 527-539). ACM. (May, 2016).

[141]. R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti and L. F. Cranor "Can long passwords be secure and usable?". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2927-2936). ACM. April, 2014.

[142]. K. Parsons, A. McCormac, M. Pattinson, M. Butavicius and C. Jerram, Phishing for the truth: "A scenario-based experiment of users' behavioural response to emails". In *IFIP International Information Security Conference* (pp. 366-378). Springer, Berlin, Heidelberg. July, 2013.

[143]. S. Lauesen and H. Younessi "Six Styles for Usability Requirements." In *REFSQ* (Vol. 98, pp. 155-166). June, 1998.

[144]. S. Chowdhury and R. Poet "Comparing the usability of doodle and Mikon images to be used as authenticators in graphical authentication systems". In *Proceeding of Conference on User science and Engineering,* pp. 54-58, 2011

[145]. F. Towhidi and M Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms" *International Journal of Computer Science and Information Security (IJCSIS),* Vol. 6, No. 2, 2009.

[146]. A. Dillon "The evaluation of software usability." In *Encyclopedia of human factors and ergonomics*. London: Taylor and Francis. 2001

[147]. F. Liu, B. S. Xiao, E. T. Lim and C. W. Tan "Searching for What I Want: Understanding the Impact of Anticipatory Search control on Search Efficiency." In *ECIS* (p. ResearchPaper22). June, 2016.

[148]. F. Tari, A. A. Ozok and S. H. Holden "A comparison of perceived and real shoulder surfing risks between alphanumeric and graphical passwords." In *Proceedings of the second symposium on Usable privacy and security*, pp. 56-66. ACM, 2006.

[149]. O. A. Olukayode, N. Ithnin, O. S. Ogunnusi "Memorability rates of graphical password schemes." In *Journal of Theoretical & Applied Information Technology*. 20;66 (1). August, 2014

[150]. X. Suo "A Design and Analysis of Graphical Password" "Master's Thesis" Department of Computer Science, Georgia State University, 2016.

Research Questionnaire

Please complete sections A and B of this questionnaire before undertaking the experiment and section D only when you have performed all needed tasks in the experiment. Section C is to be completed by the researcher.

SECTION A: PERSONAL DATA

Name …………………………………… Programme ………..…………… Level ……...............

1. What is your gender? Male □ Female □
2. What is your age group? (Please tick as appropriate)

Less than 18 □ 18 - 20 □ 21 - 23 □ 24 - 26 □ 27 - 29 □ 30 - 32 □ 33 - 35 □ More than 35 □

3. Do you have any seeing disability?

   Yes □ No □ (If answer is no, go to question 5)

4. If your answer to (3) is 'yes', please state the type of disability ....
5. Do you have any other disability that renders you incapable of performing a computer based experiment?

   Yes □ No □ (If answer is no, go to section B)

6. If your answer to (5) is 'yes', please state the type of disability ....

SECTION B: INTERNET/PASSWORD USE DATA

7. For how long have you used computers and or the internet?

   1 - 2 years □ 3 - 4 years □ 5 - 6 years □ 7 - 8 years □ 9 - 10 years □ More than 10 years □

8. How many online passwords do you have? (* this includes those of emails, social media, online bank accounts, professional forums, etc.)

   1 - 2 □ 3 - 4 □ 5 - 6 □ 7 - 8 □ 9 - 10 □ More than 10 □

9. What practice do you employ in keeping track of your numerous online passwords? (you can tick as many that apply to you)

   Writing p/w down □ Using same p/w for several accounts □ Sharing p/w with friends □ Using common words for p/w (such as towns) □ Using names of family members □ Using names of favourite things (such as pets and colours) □ Others □ (please specify) ....

10. How often do you request family members/friends to use your password to help you check emails and online bank and other accounts?

Always □ Often □ Sometimes □ Seldom □ Never □ Can't say □

11. How many ATM PINs do you have?

1 - 2 □ 3 - 4 □ 5 - 6 □ 7 - 8 □ 9 - 10 □ More than 10 □

12. What practice do you employ in keeping track of your numerous ATM PINs? (you can tick as many that apply to you)

Writing them down □ Using same PIN for several accounts □ Sharing them with friends □ Using dates of birth □ Using dates of known events □ Using parts of phone numbers □ Using parts of account numbers □ Using parts of other known numbers □ Others methods □ (please specify)

13. How often do you give ATM cards to family members/friends to help you withdraw funds from ATM machines?

Always □ Often □ Sometimes □ Seldom □ Never □ Can't say □

14. Have you ever heard of graphical/picture passwords?

Yes □ No □ (If your answer to (14) is ‘No’, go to section C)

15. Do you expect graphical/picture passwords to be a good alternative to be used in place of text based passwords?

Yes □ No □ Maybe □ Can't say □

16. Will you be willing to adopt/recommend a graphical/picture password as a replacement to a current text password?

Yes □ No □ Maybe □ Can't say □

SECTION C: EXPERIMENTAL DATA (To be completed by the researcher)

Participant Username .... Experiment type ....

Model name : .... System no/code: .... Grid size (NxN) .... Steps ....

Success Rate

Registration time

Test 1	**Test 2**	**Test 3**	**Test 4**	**Test 5**
Pass □ Fail □	Pass □ Fail □	Pass □ Fail □	Pass □ Fail □	Pass □ Fail □
Time	Time	Time	Time	Time ....

SECTION D: USER EXPERIENCE DATA

17. How can you rate your choice of this system in comparison to any other graphical systems you have used? (* answer this only if you have participated in a previous experiment)

□ Better □ Equal □ Worse (Please state your reason below)

....

For questions 18 to 24, please rate from 1 to 7, 1 being strongly disagree and 7 strongly agree, the scale is as follows:

Strongly Disagree	**Disagree**	**Somewhat Disagree**	**Neutral/Don't Know**	**Somewhat Agree**	**Agree**	**Strongly Agree**
1	**2**	**3**	**4**	**5**	**6**	**7**

18. Do you agree that the use of this system is easy to understand?

❶ ❷ ❸ ❹ ❺ ❻ ❼

19. Do you agree that this system is easy to use?

❶ ❷ ❸ ❹ ❺ ❻ ❼

Strongly Disagree	Disagree	Somewhat Disagree	Neutral/Don't Know	Somewhat Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

20. The time taken for a user to register on this system is adequate.

❶ ❷ ❸ ❹ ❺ ❻ ❼

21. The time taken for a user to authenticate on this system is adequate.

❶ ❷ ❸ ❹ ❺ ❻ ❼

22. It is difficult to guess a person's password when he uses this system.

❶ ❷ ❸ ❹ ❺ ❻ ❼

23. It is difficult for an observer to understand what a user selects as his password during an authentication round when he uses this system.

❶ ❷ ❸ ❹ ❺ ❻ ❼

24. The layout of the windows and buttons relative to the screen was adequate.

❶ ❷ ❸ ❹ ❺ ❻ ❼

25. The presentation of images in the authentication windows was adequate.

❶ ❷ ❸ ❹ ❺ ❻ ❼

26. The properties and variants provided for user authentication are adequate?

❶ ❷ ❸ ❹ ❺ ❻ ❼

27. If you are asked to score this system on a scale of 1 to 10, what will be your score?

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩

28. Are you satisfied with the layout (interface arrangement) of this system?

Yes □ No □ (if yes, please explain)

....

29. Are you satisfied with the various steps taken to register with this system?

Yes □ No □ (if yes, please explain)

....

30. Are you satisfied with the various steps taken to authenticate with this system?

Yes □ No □ (if yes, please explain)

....

31. Will you recommend this system to be accepted and introduced globally as an authentication system?

Yes □ No □

32. What is the reason for your answer in (30)?

....

33. What is your general opinion on the use of this system in relation to the following points:

	Strongly Disagree	**Disagree**	**Somewhat Disagree**	**Neutral/Don't Know**	**Somewhat Agree**	**Agree**	**Strongly Agree**
Good	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Interesting	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Challenging	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Confusing	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Difficult	**1**	**2**	**3**	**4**	**5**	**6**	**7**

34. Is there any weakness of this system that you have identified?

Yes □ No □

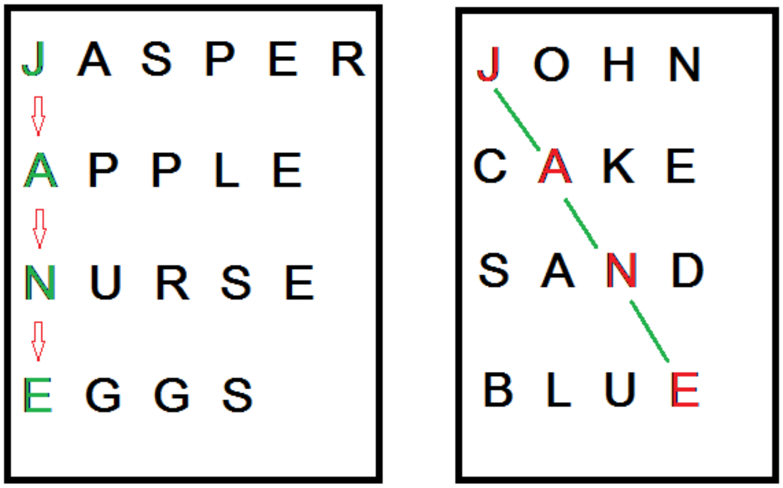
If (33) is 'Yes', what is the weakness ....

35. What useful suggestion can you offer for the improvement of the system?

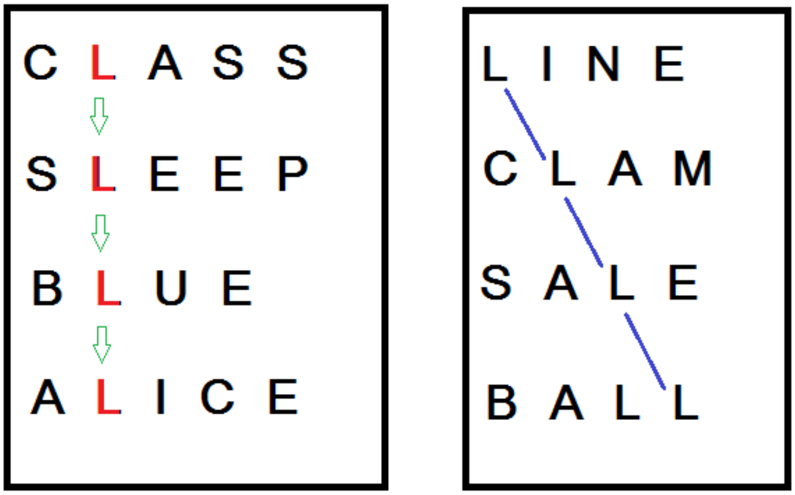
....

Appendix 1

A: Standard and ordinal spelling for the word “Jane”



B: Fixed Lettering and ordinal lettering for the letter L



APPENDIX 2 -- COMPARISON OF MEANS FOR EXPERIMENT 2

```
ONEWAY signup_time step_time_1 step_time_2 total_time avg_time BY user_auth_type
  /STATISTICS DESCRIPTIVES
  /MISSING ANALYSIS
  /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Regist. Time	1	18	79696.39	16227.320	3824.816	71626.73	87766.05	32532	98735
	2	18	70344.06	22544.122	5313.701	59133.13	81554.98	34447	102412
	3	18	78913.00	35025.055	8255.485	61495.45	96330.55	13198	127810
	4	18	86297.72	22690.594	5348.224	75013.96	97581.49	29763	127612
	5	18	83814.72	25365.345	5978.669	71200.83	96428.61	46408	135530
	Total	90	79813.18	25159.220	2652.015	74543.68	85082.67	13198	135530
Step Time 1	1	18	10742.56	4062.291	957.491	8722.43	12762.69	6438	22435
	2	18	10308.78	5715.408	1347.135	7466.57	13150.98	1908	26310
	3	18	14267.11	9975.103	2351.154	9306.61	19227.61	3080	38844
	4	18	14014.33	9661.172	2277.160	9209.95	18818.72	1036	44558
	5	18	12399.56	6867.141	1618.601	8984.61	15814.50	1976	28845
	Total	90	12346.47	7609.427	802.104	10752.70	13940.23	1036	44558
Step Time 2	1	18	8982.72	4424.603	1042.889	6782.42	11183.03	2345	22375
	2	18	11200.83	7032.219	1657.510	7703.79	14697.87	2171	26903
	3	18	23595.78	10496.933	2474.151	18375.78	28815.78	6007	39643
	4	18	10163.33	6294.455	1483.617	7033.17	13293.49	1143	25468

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
	5	18	11775.50	9381.641	2211.274	7110.12	16440.88	1968	29649
	Total	90	13143.63	9335.238	984.021	11188.41	15098.86	1143	39643
Authen. Time	1	18	19725.28	7956.387	1875.338	15768.66	23681.90	10999	44810
	2	18	21509.61	8440.916	1989.543	17312.04	25707.18	4079	35964
	3	18	37862.89	17740.558	4181.490	29040.72	46685.06	9087	71511
	4	18	24177.67	13981.533	3295.479	17224.81	31130.52	2893	63066
	5	18	24175.06	14485.296	3414.217	16971.69	31378.42	3944	51377
	Total	90	25490.10	14311.566	1508.572	22492.60	28487.60	2893	71511
Average Time	1	18	9862.83	3978.169	937.664	7884.54	11841.13	5500	22405
	2	18	10755.00	4220.409	994.760	8656.24	12853.76	2040	17982
	3	18	18931.67	8870.292	2090.748	14520.57	23342.76	4544	35756
	4	18	12089.06	6990.704	1647.725	8612.66	15565.45	1447	31533
	5	18	12087.78	7242.699	1707.120	8486.07	15689.49	1972	25689
	Total	90	12745.27	7155.780	754.285	11246.52	14244.02	1447	35756

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Regist. Time	Between Groups	2673898379	4	668474594.7	1.059	.382
	Within Groups	5.366E+10	85	631316326.7		
	Total	5.634E+10	89			
Step Time 1	Between Groups	237567232.6	4	59391808.16	1.027	.398
	Within Groups	4915833148	85	57833331.15		
	Total	5153400380	89			
Step Time 2	Between Groups	2539601163	4	634900290.8	10.345	.000
	Within Groups	5216452778	85	61370032.68		
	Total	7756053941	89			
Authen. Time	Between Groups	3701073511	4	925268377.9	5.414	.001
	Within Groups	1.453E+10	85	170917523.1		
	Total	1.823E+10	89			
Average Time	Between Groups	925272593.0	4	231318148.3	5.414	.001
	Within Groups	3631988481	85	42729276.24		
	Total	4557261074	89			

Post Hoc Tests

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Regist. Time	1	2	9352.333	8375.336	.797	-13991.40	32696.06
		3	783.389	8375.336	1.000	-22560.34	24127.12
		4	-6601.333	8375.336	.933	-29945.06	16742.40
		5	-4118.333	8375.336	.988	-27462.06	19225.40
	2	1	-9352.333	8375.336	.797	-32696.06	13991.40
		3	-8568.944	8375.336	.844	-31912.67	14774.79
		4	-15953.667	8375.336	.323	-39297.40	7390.06
		5	-13470.667	8375.336	.496	-36814.40	9873.06
	3	1	-783.389	8375.336	1.000	-24127.12	22560.34
		2	8568.944	8375.336	.844	-14774.79	31912.67
		4	-7384.722	8375.336	.903	-30728.45	15959.01
		5	-4901.722	8375.336	.977	-28245.45	18442.01
	4	1	6601.333	8375.336	.933	-16742.40	29945.06
		2	15953.667	8375.336	.323	-7390.06	39297.40
		3	7384.722	8375.336	.903	-15959.01	30728.45
		5	2483.000	8375.336	.998	-20860.73	25826.73
	5	1	4118.333	8375.336	.988	-19225.40	27462.06
		2	13470.667	8375.336	.496	-9873.06	36814.40
		3	4901.722	8375.336	.977	-18442.01	28245.45
		4	-2483.000	8375.336	.998	-25826.73	20860.73
Step Time 1	1	2	433.778	2534.941	1.000	-6631.61	7499.16
		3	-3524.556	2534.941	.635	-10589.94	3540.83
		4	-3271.778	2534.941	.698	-10337.16	3793.61
		5	-1657.000	2534.941	.966	-8722.39	5408.39

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	2	1	-433.778	2534.941	1.000	-7499.16	6631.61
		3	-3958.333	2534.941	.526	-11023.72	3107.05
		4	-3705.556	2534.941	.590	-10770.94	3359.83
		5	-2090.778	2534.941	.922	-9156.16	4974.61
	3	1	3524.556	2534.941	.635	-3540.83	10589.94
		2	3958.333	2534.941	.526	-3107.05	11023.72
		4	252.778	2534.941	1.000	-6812.61	7318.16
		5	1867.556	2534.941	.947	-5197.83	8932.94
	4	1	3271.778	2534.941	.698	-3793.61	10337.16
		2	3705.556	2534.941	.590	-3359.83	10770.94
		3	-252.778	2534.941	1.000	-7318.16	6812.61
		5	1614.778	2534.941	.969	-5450.61	8680.16
	5	1	1657.000	2534.941	.966	-5408.39	8722.39
		2	2090.778	2534.941	.922	-4974.61	9156.16
		3	-1867.556	2534.941	.947	-8932.94	5197.83
		4	-1614.778	2534.941	.969	-8680.16	5450.61
Step Time 2	1	2	-2218.111	2611.301	.914	-9496.33	5060.10
		3	-14613.056*	2611.301	.000	-21891.27	-7334.84
		4	-1180.611	2611.301	.991	-8458.83	6097.60
		5	-2792.778	2611.301	.822	-10070.99	4485.44
	2	1	2218.111	2611.301	.914	-5060.10	9496.33
		3	-12394.944*	2611.301	.000	-19673.16	-5116.73
		4	1037.500	2611.301	.995	-6240.72	8315.72
		5	-574.667	2611.301	.999	-7852.88	6703.55

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	3	1	14613.056*	2611.301	.000	7334.84	21891.27
		2	12394.944*	2611.301	.000	5116.73	19673.16
		4	13432.444*	2611.301	.000	6154.23	20710.66
		5	11820.278*	2611.301	.000	4542.06	19098.49
	4	1	1180.611	2611.301	.991	-6097.60	8458.83
		2	-1037.500	2611.301	.995	-8315.72	6240.72
		3	-13432.444*	2611.301	.000	-20710.66	-6154.23
		5	-1612.167	2611.301	.972	-8890.38	5666.05
	5	1	2792.778	2611.301	.822	-4485.44	10070.99
		2	574.667	2611.301	.999	-6703.55	7852.88
		3	-11820.278*	2611.301	.000	-19098.49	-4542.06
		4	1612.167	2611.301	.972	-5666.05	8890.38
Authen. Time	1	2	-1784.333	4357.848	.994	-13930.52	10361.86
		3	-18137.611*	4357.848	.001	-30283.80	-5991.42
		4	-4452.389	4357.848	.845	-16598.58	7693.80
		5	-4449.778	4357.848	.845	-16595.97	7696.41
	2	1	1784.333	4357.848	.994	-10361.86	13930.52
		3	-16353.278*	4357.848	.003	-28499.47	-4207.09
		4	-2668.056	4357.848	.973	-14814.24	9478.13
		5	-2665.444	4357.848	.973	-14811.63	9480.74
	3	1	18137.611*	4357.848	.001	5991.42	30283.80
		2	16353.278*	4357.848	.003	4207.09	28499.47
		4	13685.222*	4357.848	.019	1539.03	25831.41
		5	13687.833*	4357.848	.019	1541.64	25834.02

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	4	1	4452.389	4357.848	.845	-7693.80	16598.58
		2	2668.056	4357.848	.973	-9478.13	14814.24
		3	-13685.222*	4357.848	.019	-25831.41	-1539.03
		5	2.611	4357.848	1.000	-12143.58	12148.80
	5	1	4449.778	4357.848	.845	-7696.41	16595.97
		2	2665.444	4357.848	.973	-9480.74	14811.63
		3	-13687.833*	4357.848	.019	-25834.02	-1541.64
		4	-2.611	4357.848	1.000	-12148.80	12143.58
Average Time	1	2	-892.167	2178.921	.994	-6965.25	5180.92
		3	-9068.833*	2178.921	.001	-15141.92	-2995.75
		4	-2226.222	2178.921	.845	-8299.31	3846.86
		5	-2224.944	2178.921	.845	-8298.03	3848.14
	2	1	892.167	2178.921	.994	-5180.92	6965.25
		3	-8176.667*	2178.921	.003	-14249.75	-2103.58
		4	-1334.056	2178.921	.973	-7407.14	4739.03
		5	-1332.778	2178.921	.973	-7405.86	4740.31
	3	1	9068.833*	2178.921	.001	2995.75	15141.92
		2	8176.667*	2178.921	.003	2103.58	14249.75
		4	6842.611*	2178.921	.019	769.52	12915.70
		5	6843.889*	2178.921	.019	770.80	12916.98
	4	1	2226.222	2178.921	.845	-3846.86	8299.31
		2	1334.056	2178.921	.973	-4739.03	7407.14
		3	-6842.611*	2178.921	.019	-12915.70	-769.52
		5	1.278	2178.921	1.000	-6071.81	6074.36

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	5	1	2224.944	2178.921	.845	-3848.14	8298.03
		2	1332.778	2178.921	.973	-4740.31	7405.86
		3	-6843.889*	2178.921	.019	-12916.98	-770.80
		4	-1.278	2178.921	1.000	-6074.36	6071.81

*. The mean difference is significant at the 0.05 level.

Homogeneous Subsets

Regist. Time

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05
		1
2	18	70344.06
3	18	78913.00
1	18	79696.39
5	18	83814.72
4	18	86297.72
Sig.		.323

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 18.000.

Step Time 1

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05
		1
2	18	10308.78
1	18	10742.56
5	18	12399.56
4	18	14014.33
3	18	14267.11
Sig.		.526

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 18.000.

Step Time 2

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
1	18	8982.72	
4	18	10163.33	
2	18	11200.83	
5	18	11775.50	
3	18		23595.78
Sig.		.822	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 18.000.

Authen. Time

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
1	18	19725.28	
2	18	21509.61	
5	18	24175.06	
4	18	24177.67	
3	18		37862.89
Sig.		.845	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 18.000.

Average Time

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
1	18	9862.83	
2	18	10755.00	
5	18	12087.78	
4	18	12089.06	
3	18		18931.67
Sig.		.845	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 18.000.

APPENDIX 3 -- COMPARISON OF MEANS FOR EXPERMENT 3

```
ONEWAY signup_time step_time_1 step_time_2 total_time BY user_auth_type
  /STATISTICS DESCRIPTIVES
  /MISSING ANALYSIS
  /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Regist. Time	6	20	53165.25	13864.348	3100.162	46676.54	59653.96	34782	83461
	7	20	56732.75	32738.771	7320.612	41410.53	72054.97	32313	182180
	8	20	41312.65	8285.597	1852.716	37434.87	45190.43	23289	59075
	9	20	45033.85	9889.118	2211.274	40405.60	49662.10	30974	67890
	10	20	37023.70	14923.471	3336.990	30039.30	44008.10	12445	65473
	Total	100	46653.64	19271.678	1927.168	42829.72	50477.56	12445	182180
Step Time 1	6	20	6651.10	5465.659	1222.159	4093.09	9209.11	2235	24976
	7	20	10739.10	9989.373	2233.692	6063.93	15414.27	2265	42895
	8	20	13903.75	6807.051	1522.103	10717.95	17089.55	5641	30923
	9	20	20644.10	15501.655	3466.275	13389.10	27899.10	1609	59084
	10	20	13236.25	9768.878	2184.387	8664.27	17808.23	3781	41581
	Total	100	13034.86	10925.475	1092.547	10867.01	15202.71	1609	59084
Step Time 2	6	20	11403.50	4908.341	1097.538	9106.33	13700.67	6056	23820
	7	20	17069.90	10043.936	2245.892	12369.19	21770.61	6297	33237
	8	20	19634.45	7565.267	1691.645	16093.80	23175.10	9298	32345
	9	20	29140.90	17485.371	3909.848	20957.49	37324.31	7767	67584

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
	10	20	22037.65	10785.182	2411.640	16990.03	27085.27	8625	45880
	Total	100	19857.28	12262.088	1226.209	17424.22	22290.34	6056	67584
Authent. Time	6	20	18054.60	9383.247	2098.158	13663.11	22446.09	8291	48796
	7	20	27809.00	18517.177	4140.567	19142.69	36475.31	9187	74931
	8	20	33538.20	13411.634	2998.932	27261.36	39815.04	16158	63268
	9	20	49785.00	32344.921	7232.544	34647.11	64922.89	12313	126668
	10	20	35273.90	19247.992	4303.982	26265.56	44282.24	13750	76928
	Total	100	32892.14	22308.932	2230.893	28465.56	37318.72	8291	126668

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Regist. Time	Between Groups	5357503228	4	1339375807	4.051	.004
	Within Groups	3.141E+10	95	330640596.0		
	Total	3.677E+10	99			
Step Time 1	Between Groups	2094379337	4	523594834.3	5.116	.001
	Within Groups	9722855001	95	102345842.1		
	Total	1.182E+10	99			
Step Time 2	Between Groups	3404503008	4	851125752.0	7.043	.000
	Within Groups	1.148E+10	95	120852815.2		
	Total	1.489E+10	99			
Authent. Time	Between Groups	1.075E+10	4	2687248994	6.627	.000
	Within Groups	3.852E+10	95	405496439.0		
	Total	4.927E+10	99			

Post Hoc Tests

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Regist. Time	6	7	-3567.500	5750.136	.971	-19557.85	12422.85
		8	11852.600	5750.136	.246	-4137.75	27842.95
		9	8131.400	5750.136	.620	-7858.95	24121.75
		10	16141.550*	5750.136	.047	151.20	32131.90
	7	6	3567.500	5750.136	.971	-12422.85	19557.85
		8	15420.100	5750.136	.064	-570.25	31410.45
		9	11698.900	5750.136	.258	-4291.45	27689.25
		10	19709.050*	5750.136	.008	3718.70	35699.40
	8	6	-11852.600	5750.136	.246	-27842.95	4137.75
		7	-15420.100	5750.136	.064	-31410.45	570.25
		9	-3721.200	5750.136	.967	-19711.55	12269.15
		10	4288.950	5750.136	.945	-11701.40	20279.30
	9	6	-8131.400	5750.136	.620	-24121.75	7858.95
		7	-11698.900	5750.136	.258	-27689.25	4291.45
		8	3721.200	5750.136	.967	-12269.15	19711.55
		10	8010.150	5750.136	.634	-7980.20	24000.50
	10	6	-16141.550*	5750.136	.047	-32131.90	-151.20
		7	-19709.050*	5750.136	.008	-35699.40	-3718.70
		8	-4288.950	5750.136	.945	-20279.30	11701.40
		9	-8010.150	5750.136	.634	-24000.50	7980.20
Step Time 1	6	7	-4088.000	3199.154	.705	-12984.41	4808.41
		8	-7252.650	3199.154	.165	-16149.06	1643.76
		9	-13993.000*	3199.154	.000	-22889.41	-5096.59
		10	-6585.150	3199.154	.247	-15481.56	2311.26

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	7	6	4088.000	3199.154	.705	-4808.41	12984.41
		8	-3164.650	3199.154	.860	-12061.06	5731.76
		9	-9905.000*	3199.154	.021	-18801.41	-1008.59
		10	-2497.150	3199.154	.936	-11393.56	6399.26
	8	6	7252.650	3199.154	.165	-1643.76	16149.06
		7	3164.650	3199.154	.860	-5731.76	12061.06
		9	-6740.350	3199.154	.226	-15636.76	2156.06
		10	667.500	3199.154	1.000	-8228.91	9563.91
	9	6	13993.000*	3199.154	.000	5096.59	22889.41
		7	9905.000*	3199.154	.021	1008.59	18801.41
		8	6740.350	3199.154	.226	-2156.06	15636.76
		10	7407.850	3199.154	.149	-1488.56	16304.26
	10	6	6585.150	3199.154	.247	-2311.26	15481.56
		7	2497.150	3199.154	.936	-6399.26	11393.56
		8	-667.500	3199.154	1.000	-9563.91	8228.91
		9	-7407.850	3199.154	.149	-16304.26	1488.56
Step Time 2	6	7	-5666.400	3476.389	.482	-15333.77	4000.97
		8	-8230.950	3476.389	.133	-17898.32	1436.42
		9	-17737.400*	3476.389	.000	-27404.77	-8070.03
		10	-10634.150*	3476.389	.024	-20301.52	-966.78
	7	6	5666.400	3476.389	.482	-4000.97	15333.77
		8	-2564.550	3476.389	.947	-12231.92	7102.82
		9	-12071.000*	3476.389	.007	-21738.37	-2403.63
		10	-4967.750	3476.389	.611	-14635.12	4699.62

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	8	6	8230.950	3476.389	.133	-1436.42	17898.32
		7	2564.550	3476.389	.947	-7102.82	12231.92
		9	-9506.450	3476.389	.056	-19173.82	160.92
		10	-2403.200	3476.389	.958	-12070.57	7264.17
	9	6	17737.400*	3476.389	.000	8070.03	27404.77
		7	12071.000*	3476.389	.007	2403.63	21738.37
		8	9506.450	3476.389	.056	-160.92	19173.82
		10	7103.250	3476.389	.254	-2564.12	16770.62
	10	6	10634.150*	3476.389	.024	966.78	20301.52
		7	4967.750	3476.389	.611	-4699.62	14635.12
		8	2403.200	3476.389	.958	-7264.17	12070.57
		9	-7103.250	3476.389	.254	-16770.62	2564.12
Authent. Time	6	7	-9754.400	6367.860	.545	-27462.56	7953.76
		8	-15483.600	6367.860	.116	-33191.76	2224.56
		9	-31730.400*	6367.860	.000	-49438.56	-14022.24
		10	-17219.300	6367.860	.061	-34927.46	488.86
	7	6	9754.400	6367.860	.545	-7953.76	27462.56
		8	-5729.200	6367.860	.896	-23437.36	11978.96
		9	-21976.000*	6367.860	.007	-39684.16	-4267.84
		10	-7464.900	6367.860	.767	-25173.06	10243.26
	8	6	15483.600	6367.860	.116	-2224.56	33191.76
		7	5729.200	6367.860	.896	-11978.96	23437.36
		9	-16246.800	6367.860	.088	-33954.96	1461.36
		10	-1735.700	6367.860	.999	-19443.86	15972.46

Multiple Comparisons

Tukey HSD

Dependent Variable	(I) Model Number	(J) Model Number	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
	9	6	31730.400*	6367.860	.000	14022.24	49438.56
		7	21976.000*	6367.860	.007	4267.84	39684.16
		8	16246.800	6367.860	.088	-1461.36	33954.96
		10	14511.100	6367.860	.161	-3197.06	32219.26
	10	6	17219.300	6367.860	.061	-488.86	34927.46
		7	7464.900	6367.860	.767	-10243.26	25173.06
		8	1735.700	6367.860	.999	-15972.46	19443.86
		9	-14511.100	6367.860	.161	-32219.26	3197.06

*. The mean difference is significant at the 0.05 level.

Homogeneous Subsets

Regist. Time

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
10	20	37023.70	
8	20	41312.65	41312.65
9	20	45033.85	45033.85
6	20		53165.25
7	20		56732.75
Sig.		.634	.064

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 20.000.

Step Time 1

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
6	20	6651.10	
7	20	10739.10	
10	20	13236.25	13236.25
8	20	13903.75	13903.75
9	20		20644.10
Sig.		.165	.149

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 20.000.

Step Time 2

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05		
		1	2	3
6	20	11403.50		
7	20	17069.90	17069.90	
8	20	19634.45	19634.45	19634.45
10	20		22037.65	22037.65
9	20			29140.90
Sig.		.133	.611	.056

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 20.000.

Authent. Time

Tukey HSD[a]

Model Number	N	Subset for alpha = 0.05	
		1	2
6	20	18054.60	
7	20	27809.00	
8	20	33538.20	33538.20
10	20	35273.90	35273.90
9	20		49785.00
Sig.		.061	.088

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 20.000.

APPENDIX 4(B) -- CHI-SQUARE TEST FOR LOGIN SUCCESS RATE

```
CROSSTABS
  /TABLES=auth_type BY login_1 login_2 login_3 login_4
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Model Num. * 1st Login	80	100.0%	0	0.0%	80	100.0%
Model Num. * 2nd Login	80	100.0%	0	0.0%	80	100.0%
Model Num. * 3rd Login	80	100.0%	0	0.0%	80	100.0%
Model Num. * 4th Login	80	100.0%	0	0.0%	80	100.0%

Model Num. * 1st Login

Crosstab

			1st Login		Total
			0	1	
Model Num.	1	Count	0	20	20
		% within Model Num.	0.0%	100.0%	100.0%
		% within 1st Login	0.0%	26.7%	25.0%
		% of Total	0.0%	25.0%	25.0%
	3	Count	4	16	20
		% within Model Num.	20.0%	80.0%	100.0%
		% within 1st Login	80.0%	21.3%	25.0%
		% of Total	5.0%	20.0%	25.0%
	7	Count	0	20	20
		% within Model Num.	0.0%	100.0%	100.0%
		% within 1st Login	0.0%	26.7%	25.0%
		% of Total	0.0%	25.0%	25.0%
	10	Count	1	19	20
		% within Model Num.	5.0%	95.0%	100.0%
		% within 1st Login	20.0%	25.3%	25.0%
		% of Total	1.3%	23.8%	25.0%
Total		Count	5	75	80
		% within Model Num.	6.3%	93.8%	100.0%
		% within 1st Login	100.0%	100.0%	100.0%
		% of Total	6.3%	93.8%	100.0%

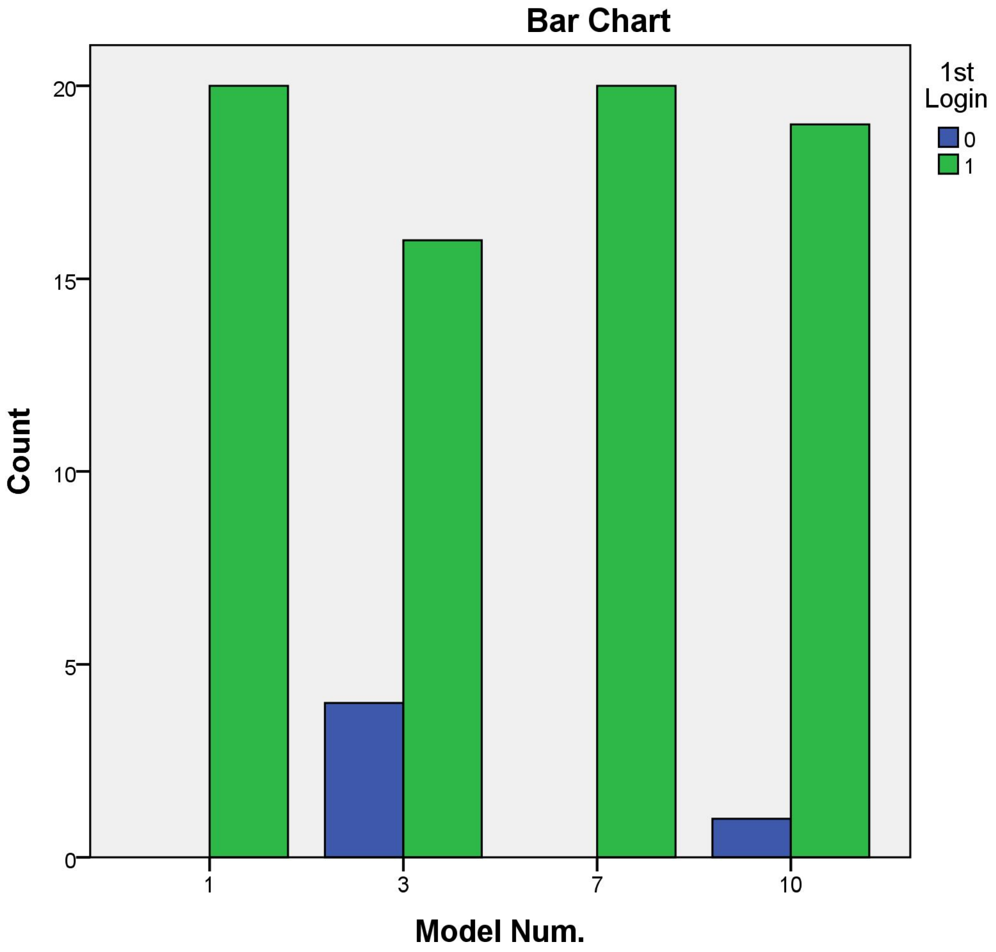
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.173[a]	3	.027
Likelihood Ratio	9.450	3	.024
Linear-by-Linear Association	.312	1	.576
N of Valid Cases	80		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 1.25.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.339	.027
	Cramer's V	.339	.027
N of Valid Cases		80	



Model Num. * 2nd Login

Crosstab

			2nd Login		Total
			0	1	
Model Num.	1	Count	1	19	20
		% within Model Num.	5.0%	95.0%	100.0%
		% within 2nd Login	10.0%	27.1%	25.0%
		% of Total	1.3%	23.8%	25.0%
	3	Count	6	14	20
		% within Model Num.	30.0%	70.0%	100.0%
		% within 2nd Login	60.0%	20.0%	25.0%
		% of Total	7.5%	17.5%	25.0%
	7	Count	0	20	20
		% within Model Num.	0.0%	100.0%	100.0%
		% within 2nd Login	0.0%	28.6%	25.0%
		% of Total	0.0%	25.0%	25.0%
	10	Count	3	17	20
		% within Model Num.	15.0%	85.0%	100.0%
		% within 2nd Login	30.0%	24.3%	25.0%
		% of Total	3.8%	21.3%	25.0%
Total		Count	10	70	80
		% within Model Num.	12.5%	87.5%	100.0%
		% within 2nd Login	100.0%	100.0%	100.0%
		% of Total	12.5%	87.5%	100.0%

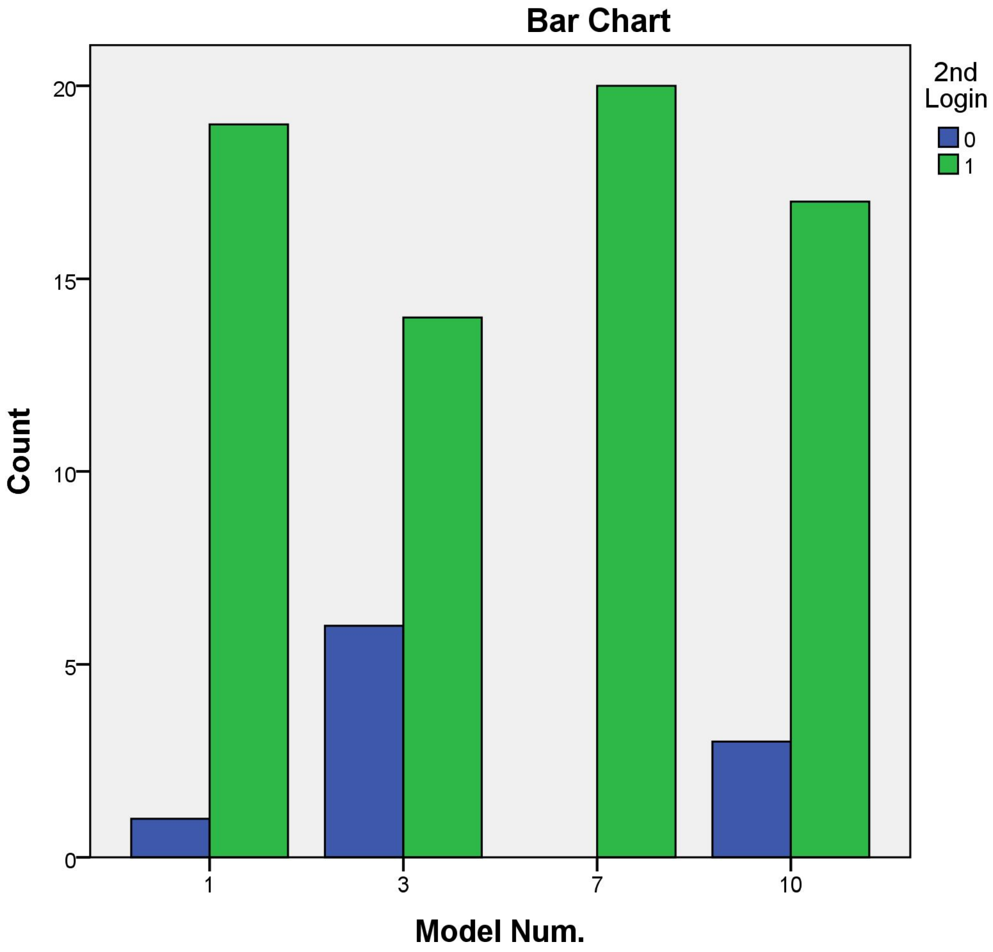
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.600[a]	3	.022
Likelihood Ratio	11.000	3	.012
Linear-by-Linear Association	.113	1	.736
N of Valid Cases	80		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 2.50.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.346	.022
	Cramer's V	.346	.022
N of Valid Cases		80	



Model Num. * 3rd Login

Crosstab

			3rd Login		Total
			0	1	
Model Num.	1	Count	2	18	20
		% within Model Num.	10.0%	90.0%	100.0%
		% within 3rd Login	16.7%	26.5%	25.0%
		% of Total	2.5%	22.5%	25.0%
	3	Count	7	13	20
		% within Model Num.	35.0%	65.0%	100.0%
		% within 3rd Login	58.3%	19.1%	25.0%
		% of Total	8.8%	16.3%	25.0%
	7	Count	0	20	20
		% within Model Num.	0.0%	100.0%	100.0%
		% within 3rd Login	0.0%	29.4%	25.0%
		% of Total	0.0%	25.0%	25.0%
	10	Count	3	17	20
		% within Model Num.	15.0%	85.0%	100.0%
		% within 3rd Login	25.0%	25.0%	25.0%
		% of Total	3.8%	21.3%	25.0%
Total		Count	12	68	80
		% within Model Num.	15.0%	85.0%	100.0%
		% within 3rd Login	100.0%	100.0%	100.0%
		% of Total	15.0%	85.0%	100.0%

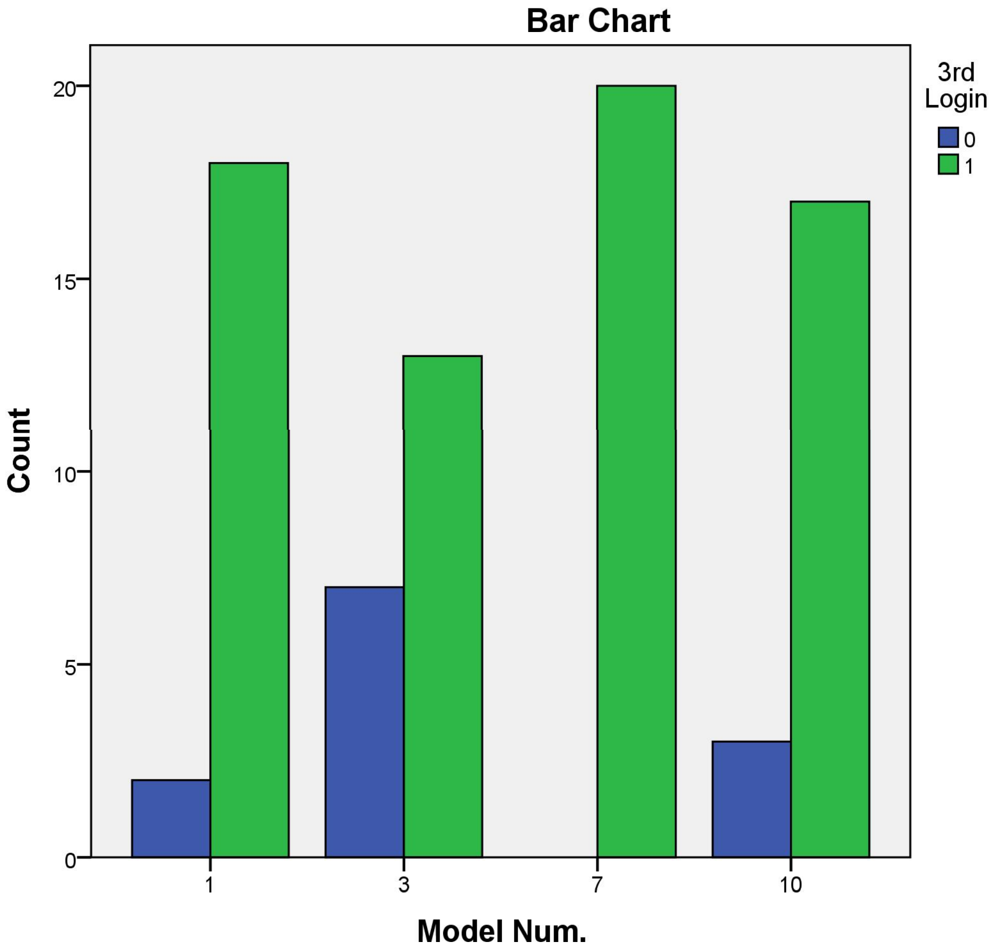
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.196[a]	3	.017
Likelihood Ratio	11.824	3	.008
Linear-by-Linear Association	.794	1	.373
N of Valid Cases	80		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 3.00.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.357	.017
	Cramer's V	.357	.017
N of Valid Cases		80	



Model Num. * 4th Login

Crosstab

			4th Login		
			0	1	Total
Model Num.	1	Count	1	19	20
		% within Model Num.	5.0%	95.0%	100.0%
		% within 4th Login	8.3%	27.9%	25.0%
		% of Total	1.3%	23.8%	25.0%
	3	Count	8	12	20
		% within Model Num.	40.0%	60.0%	100.0%
		% within 4th Login	66.7%	17.6%	25.0%
		% of Total	10.0%	15.0%	25.0%
	7	Count	0	20	20
		% within Model Num.	0.0%	100.0%	100.0%
		% within 4th Login	0.0%	29.4%	25.0%
		% of Total	0.0%	25.0%	25.0%
	10	Count	3	17	20
		% within Model Num.	15.0%	85.0%	100.0%
		% within 4th Login	25.0%	25.0%	25.0%
		% of Total	3.8%	21.3%	25.0%
Total		Count	12	68	80
		% within Model Num.	15.0%	85.0%	100.0%
		% within 4th Login	100.0%	100.0%	100.0%
		% of Total	15.0%	85.0%	100.0%

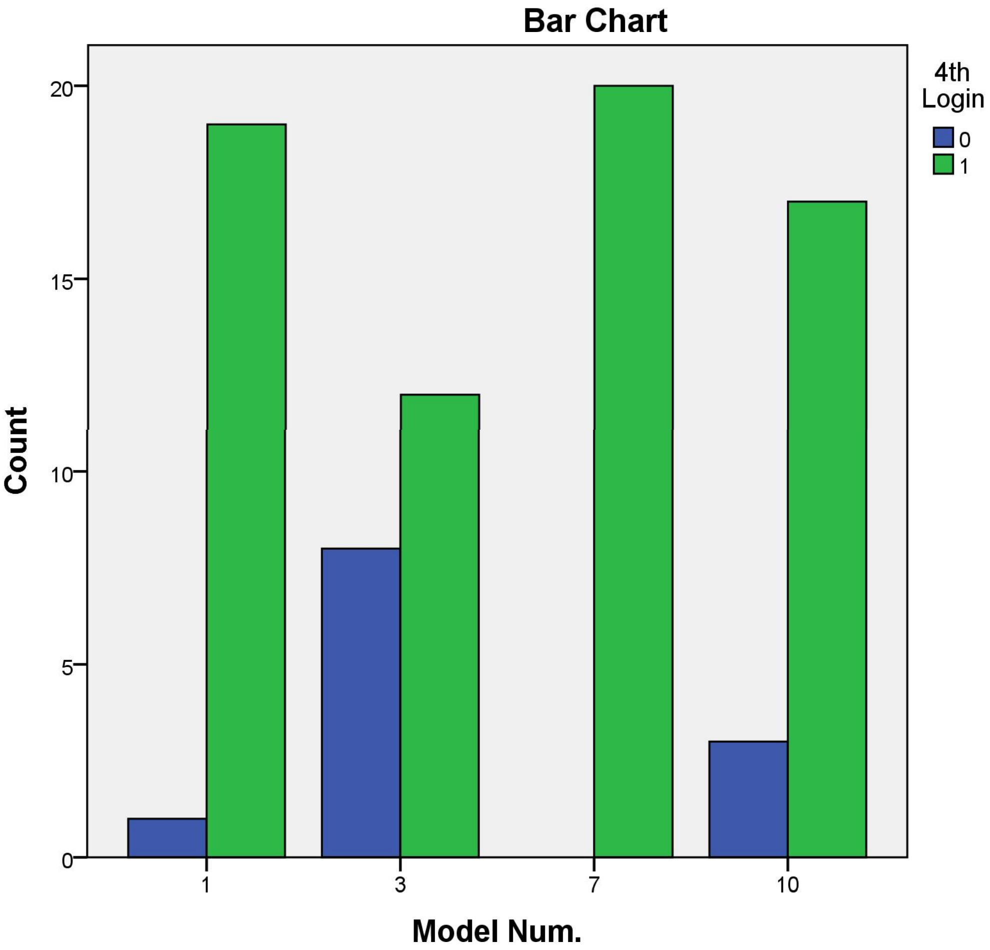
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14.902[a]	3	.002
Likelihood Ratio	15.864	3	.001
Linear-by-Linear Association	.508	1	.476
N of Valid Cases	80		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is 3.00.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.432	.002
	Cramer's V	.432	.002
N of Valid Cases		80	


Bar Chart
Count
0
5
10
15
20
Model Num.
1
3
7
10
4th Login
0
1

APPENDIX 5 -- COMPARISON FOR EXPERIEMNT 5 (GRID SIZES)

```
ONEWAY total_time avg_time BY grid_size
 /STATISTICS DESCRIPTIVES
 /MISSING ANALYSIS
 /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

Descriptives

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Login Time	2	30	17637.60	15851.669	2894.106	11718.49	23556.71	1883	57878
	3	30	31383.10	19616.713	3581.505	24058.10	38708.10	3546	71097
	4	30	31557.40	27687.115	5054.953	21218.86	41895.94	6360	102495
	5	30	36196.23	37546.263	6854.978	22176.23	50216.24	4084	179670
	Total	120	29193.58	27092.755	2473.219	24296.36	34090.80	1883	179670
Average Time	2	30	8819.10	7925.849	1447.056	5859.54	11778.66	942	28939
	3	30	15691.87	9808.444	1790.769	12029.33	19354.40	1773	35549
	4	30	15778.87	13843.596	2527.483	10609.58	20948.15	3180	51248
	5	30	18098.40	18773.146	3427.492	11088.39	25108.41	2042	89835
	Total	120	14597.06	13546.406	1236.612	12148.44	17045.67	942	89835

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Login Time	Between Groups	5788784109	3	1929594703	2.744	.046
	Within Groups	8.156E+10	116	703097258.7		
	Total	8.735E+10	119			
Average Time	Between Groups	1447184166	3	482394721.9	2.744	.046
	Within Groups	2.039E+10	116	175775203.5		
	Total	2.184E+10	119			

Post Hoc Tests

Multiple Comparisons

Tukey HSD

						95% Confidence Interval	
Dependent Variable	(I) Grid Size (NxN)	(J) Grid Size (NxN)	Mean Difference (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
Login Time	2	3	-13745.500	6846.397	.191	-31591.76	4100.76
		4	-13919.800	6846.397	.182	-31766.06	3926.46
		5	-18558.633*	6846.397	.038	-36404.90	-712.37
	3	2	13745.500	6846.397	.191	-4100.76	31591.76
		4	-174.300	6846.397	1.000	-18020.56	17671.96
		5	-4813.133	6846.397	.896	-22659.40	13033.13
	4	2	13919.800	6846.397	.182	-3926.46	31766.06
		3	174.300	6846.397	1.000	-17671.96	18020.56
		5	-4638.833	6846.397	.905	-22485.10	13207.43
	5	2	18558.633*	6846.397	.038	712.37	36404.90
		3	4813.133	6846.397	.896	-13033.13	22659.40
		4	4638.833	6846.397	.905	-13207.43	22485.10

Multiple Comparisons

Tukey HSD

			Mean			95% Confidence Interval	
Dependent Variable	(I) Grid Size (NxN)	(J) Grid Size (NxN)	Difference (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
Average Time	2	3	-6872.767	3423.207	.191	-15795.92	2050.39
		4	-6959.767	3423.207	.182	-15882.92	1963.39
		5	-9279.300*	3423.207	.038	-18202.45	-356.15
	3	2	6872.767	3423.207	.191	-2050.39	15795.92
		4	-87.000	3423.207	1.000	-9010.15	8836.15
		5	-2406.533	3423.207	.896	-11329.69	6516.62
	4	2	6959.767	3423.207	.182	-1963.39	15882.92
		3	87.000	3423.207	1.000	-8836.15	9010.15
		5	-2319.533	3423.207	.905	-11242.69	6603.62
	5	2	9279.300*	3423.207	.038	356.15	18202.45
		3	2406.533	3423.207	.896	-6516.62	11329.69
		4	2319.533	3423.207	.905	-6603.62	11242.69

*. The mean difference is significant at the 0.05 level.

Homogeneous Subsets

Login Time

Tukey HSD[a]

		Subset for alpha = 0.05	
Grid Size (NxN)	N	1	2
2	30	17637.60	
3	30	31383.10	31383.10
4	30	31557.40	31557.40
5	30		36196.23
Sig.		.182	.896

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 30.000.

Average Time

Tukey HSD[a]

		Subset for alpha = 0.05	
Grid Size (NxN)	N	1	2
2	30	8819.10	
3	30	15691.87	15691.87
4	30	15778.87	15778.87
5	30		18098.40
Sig.		.182	.896

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 30.000.

APPENDIX 6 -- COMPARISON OF MEANS FOR EXPERIMENT 6

COMPARISON OF STANDARD, ORDERED AND UNORDERED MAGNITUDE BASED SYSTEMS

4-STANDARD, 11-ORDERED, 12-UNORDERED MODELS

```
ONEWAY auth_time BY auth_type
  /STATISTICS DESCRIPTIVES
  /MISSING ANALYSIS
  /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

Descriptives

Login Time

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum
					Lower Bound	Upper Bound	
4	40	32592.33	25982.989	4108.271	24282.56	40902.09	4990
11	40	25086.03	18093.535	2860.839	19299.43	30872.62	4212
12	40	37277.15	23347.476	3691.560	29810.26	44744.04	6110
Total	120	31651.83	23078.565	2106.775	27480.21	35823.46	4212

Descriptives

Login Time

	Maximum
4	113417
11	75144
12	97336
Total	113417

ANOVA

Login Time

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3025542050	2	1512771025	2.932	.057
Within Groups	6.036E+10	117	515865448.1		
Total	6.338E+10	119			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: Login Time

Tukey HSD

(I) Model	(J) Model	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
4	11	7506.300	5078.708	.305	-4550.10	19562.70
	12	-4684.825	5078.708	.627	-16741.23	7371.58
11	4	-7506.300	5078.708	.305	-19562.70	4550.10
	12	-12191.125*	5078.708	.047	-24247.53	-134.72
12	4	4684.825	5078.708	.627	-7371.58	16741.23
	11	12191.125*	5078.708	.047	134.72	24247.53

*. The mean difference is significant at the 0.05 level.

Homogeneous Subsets

Login Time

Tukey HSD[a]

Model	N	Subset for alpha = 0.05	
		1	2
11	40	25086.03	
4	40	32592.33	32592.33
12	40		37277.15
Sig.		.305	.627

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 40.000.

APPENDIX 7 -- COMPARISON OF MEANS FOR EXPERIMENT 7 (SELECTION STYLES - WORD BASED MODEL) 1 - Standard spelling, 2 - Ordinal spelling, 3 - Fixed lettering, 4 - Ordered lettering, 5 - Random selection *** Ordinal lettering (OL) was not assessed

```
ONEWAY auth_time BY select_type
  /STATISTICS DESCRIPTIVES
  /MISSING ANALYSIS
  /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

```
[DataSet0]
```

Descriptives

Login Time

					95% Confidence Interval for Mean			
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
1	15	36384.27	11156.123	2880.499	30206.21	42562.32	19849	59970
2	15	35826.73	10581.778	2732.203	29966.74	41686.73	8563	53252
3	15	36558.53	7949.817	2052.634	32156.07	40961.00	23967	48234
4	15	38570.93	7949.661	2052.594	34168.56	42973.31	26672	53474
5	15	43188.40	8318.197	2147.749	38581.94	47794.86	27737	55940
Total	75	38105.77	9442.090	1090.279	35933.35	40278.20	8563	59970

ANOVA

Login Time

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	549015417.0	4	137253854.3	1.589	.187
Within Groups	6048310996	70	86404442.80		
Total	6597326413	74			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: Login Time

Tukey HSD

					95% Confidence Interval	
(I) Selection Type	(J) Selection Type	Mean Difference (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
1	2	557.533	3394.200	1.000	-8946.75	10061.81
	3	-174.267	3394.200	1.000	-9678.55	9330.01
	4	-2186.667	3394.200	.967	-11690.95	7317.61
	5	-6804.133	3394.200	.275	-16308.41	2700.15
2	1	-557.533	3394.200	1.000	-10061.81	8946.75
	3	-731.800	3394.200	1.000	-10236.08	8772.48
	4	-2744.200	3394.200	.927	-12248.48	6760.08
	5	-7361.667	3394.200	.204	-16865.95	2142.61
3	1	174.267	3394.200	1.000	-9330.01	9678.55
	2	731.800	3394.200	1.000	-8772.48	10236.08
	4	-2012.400	3394.200	.976	-11516.68	7491.88
	5	-6629.867	3394.200	.300	-16134.15	2874.41
4	1	2186.667	3394.200	.967	-7317.61	11690.95
	2	2744.200	3394.200	.927	-6760.08	12248.48

Multiple Comparisons

Dependent Variable: Login Time

Tukey HSD

(I) Selection Type	(J) Selection Type	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
	3	2012.400	3394.200	.976	-7491.88	11516.68
	5	-4617.467	3394.200	.655	-14121.75	4886.81
5	1	6804.133	3394.200	.275	-2700.15	16308.41
	2	7361.667	3394.200	.204	-2142.61	16865.95
	3	6629.867	3394.200	.300	-2874.41	16134.15
	4	4617.467	3394.200	.655	-4886.81	14121.75

Homogeneous Subsets

Login Time

Tukey HSD[a]

Selection Type	N	Subset for alpha = 0.05
		1
2	15	35826.73
1	15	36384.27
3	15	36558.53
4	15	38570.93
5	15	43188.40
Sig.		.204

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15.000.

APPENDIX 8 -- COMPARISON OF MEANS FOR EXPERIMENT 8 (SELECTION STYLES FOR COLOUR BASED MODEL)

1 - Inward Colouring, 2 - Outward colouring, 3 - Fixed colouring, 4 - Random colouring

```
GET
  FILE='C:\Users\Mal Hassan Suru\Desktop\Publications\Chapters\SPSS ANOVA Files\83\Exp 8.sav'.
DATASET NAME DataSet1 WINDOW=FRONT.
ONEWAY Total_time BY pw_type
  /STATISTICS DESCRIPTIVES
  /MISSING ANALYSIS
  /POSTHOC=TUKEY ALPHA(0.05).
```

Oneway

```
[DataSet1] C:\Users\Mal Hassan Suru\Desktop\Publications\Chapters\SPSS ANOVA Files\83\Exp 8.sav
```

Descriptives

Login Time

					95% Confidence Interval for Mean			
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
1	15	21252.20	10114.490	2611.550	15650.98	26853.42	4939	38239
2	15	15270.53	5450.910	1407.419	12251.92	18289.15	8286	28487
3	15	15363.13	8314.870	2146.890	10758.51	19967.75	6300	42486
4	15	25634.47	6598.242	1703.659	21980.48	29288.45	10969	36629
Total	60	19380.08	8791.700	1135.004	17108.95	21651.22	4939	42486

ANOVA

Login Time

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1134696303	3	378232101.0	6.183	.001
Within Groups	3425648576	56	61172295.99		
Total	4560344879	59			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: Login Time

Tukey HSD

					95% Confidence Interval	
(I) Selection style	(J) Selection style	Mean Difference (I-J)	Std. Error	Sig.	Lower Bound	Upper Bound
1	2	5981.667	2855.925	.167	-1580.50	13543.83
	3	5889.067	2855.925	.178	-1673.10	13451.23
	4	-4382.267	2855.925	.424	-11944.43	3179.90
2	1	-5981.667	2855.925	.167	-13543.83	1580.50
	3	-92.600	2855.925	1.000	-7654.77	7469.57
	4	-10363.933*	2855.925	.003	-17926.10	-2801.77
3	1	-5889.067	2855.925	.178	-13451.23	1673.10
	2	92.600	2855.925	1.000	-7469.57	7654.77
	4	-10271.333*	2855.925	.004	-17833.50	-2709.17
4	1	4382.267	2855.925	.424	-3179.90	11944.43
	2	10363.933*	2855.925	.003	2801.77	17926.10
	3	10271.333*	2855.925	.004	2709.17	17833.50

*. The mean difference is significant at the 0.05 level.

Homogeneous Subsets

Login Time

Tukey HSD[a]

Selection style	N	Subset for alpha = 0.05	
		1	2
2	15	15270.53	
3	15	15363.13	
1	15	21252.20	21252.20
4	15		25634.47
Sig.		.167	.424

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 15.000.

APPENDIX 9(A) - CHI SQAURE TEST FOR STEP 1

```
1 - COLOUR, 2 - PATTERN, 3 - MIXED, 4 MAGNITUDE AND 5 BUTTERFLY CROSSTABS
  /TABLES=auth_type BY failure_rate
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Model * Login failure	75	100.0%	0	0.0%	75	100.0%

Model * Login failure Crosstabulation

			Login failure		
			no	yes	Total
Model	1	Count	4	11	15
		% within Model	26.7%	73.3%	100.0%
		% within Login failure	36.4%	17.2%	20.0%
		% of Total	5.3%	14.7%	20.0%
	2	Count	3	12	15
		% within Model	20.0%	80.0%	100.0%
		% within Login failure	27.3%	18.8%	20.0%
		% of Total	4.0%	16.0%	20.0%
	3	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	23.4%	20.0%
		% of Total	0.0%	20.0%	20.0%
	4	Count	1	14	15
		% within Model	6.7%	93.3%	100.0%
		% within Login failure	9.1%	21.9%	20.0%
		% of Total	1.3%	18.7%	20.0%
	5	Count	3	12	15
		% within Model	20.0%	80.0%	100.0%
		% within Login failure	27.3%	18.8%	20.0%
		% of Total	4.0%	16.0%	20.0%

Model * Login failure Crosstabulation

		Login failure		Total
		no	yes	
Total	Count	11	64	75
	% within Model	14.7%	85.3%	100.0%
	% within Login failure	100.0%	100.0%	100.0%
	% of Total	14.7%	85.3%	100.0%

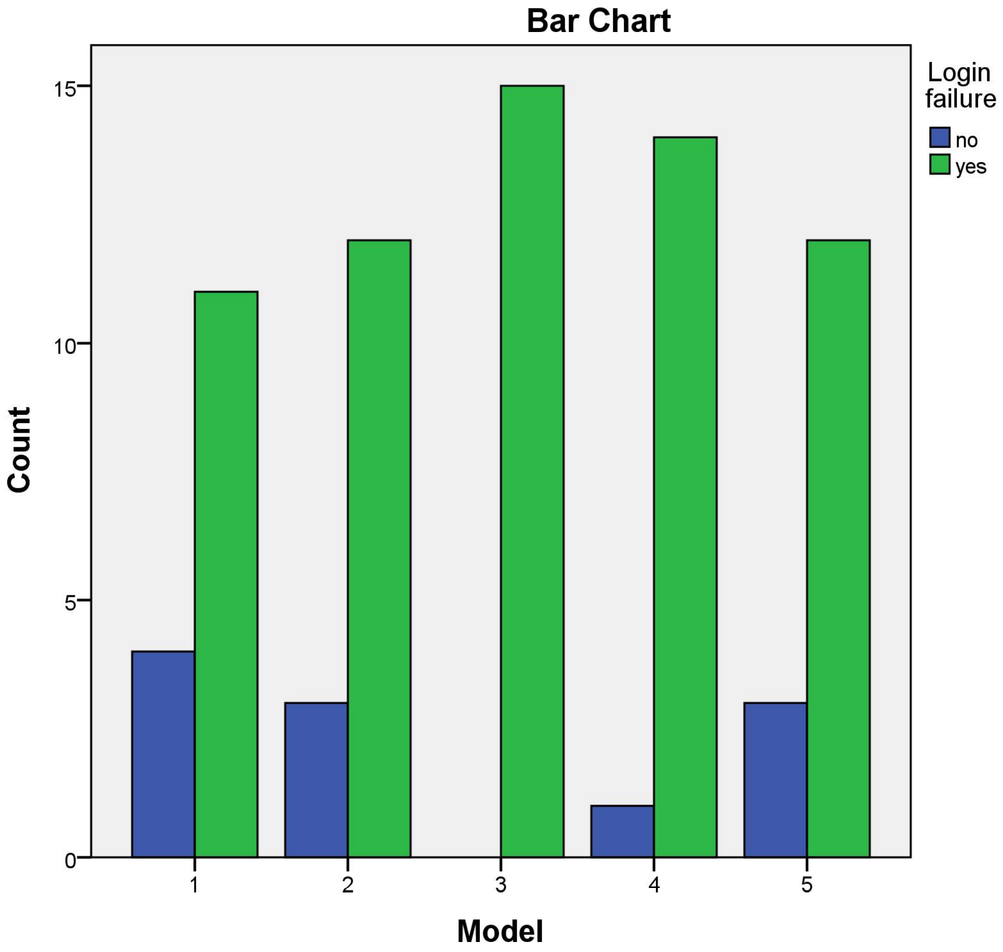
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.753[a]	4	.218
Likelihood Ratio	7.763	4	.101
Linear-by-Linear Association	.841	1	.359
N of Valid Cases	75		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is 2.20.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.277	.218
	Cramer's V	.277	.218
N of Valid Cases		75	


Bar Chart
Login failure
no
yes
Count
15
10
5
0
1
2
3
4
5
Model

APPENDIX 9(B) - CHI SQAURE TEST FOR 2 STEPS AUTHENTICATION

```
1 - COLOUR, 2 - PATTERN, 3 - MIXED, 4 - MAGNITUDE AND 5 - BUTTERFLY CROSSTABS
  /TABLES=auth_type BY failure_rate
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Model * Login failure	75	100.0%	0	0.0%	75	100.0%

Model * Login failure Crosstabulation

			Login failure		Total
			no	yes	
Model	1	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	20.3%	20.0%
		% of Total	0.0%	20.0%	20.0%
	2	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	20.3%	20.0%
		% of Total	0.0%	20.0%	20.0%
	3	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	20.3%	20.0%
		% of Total	0.0%	20.0%	20.0%
	4	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	20.3%	20.0%
		% of Total	0.0%	20.0%	20.0%
	5	Count	1	14	15
		% within Model	6.7%	93.3%	100.0%
		% within Login failure	100.0%	18.9%	20.0%
		% of Total	1.3%	18.7%	20.0%

Model * Login failure Crosstabulation

		Login failure		Total
		no	yes	
Total	Count	1	74	75
	% within Model	1.3%	98.7%	100.0%
	% within Login failure	100.0%	100.0%	100.0%
	% of Total	1.3%	98.7%	100.0%

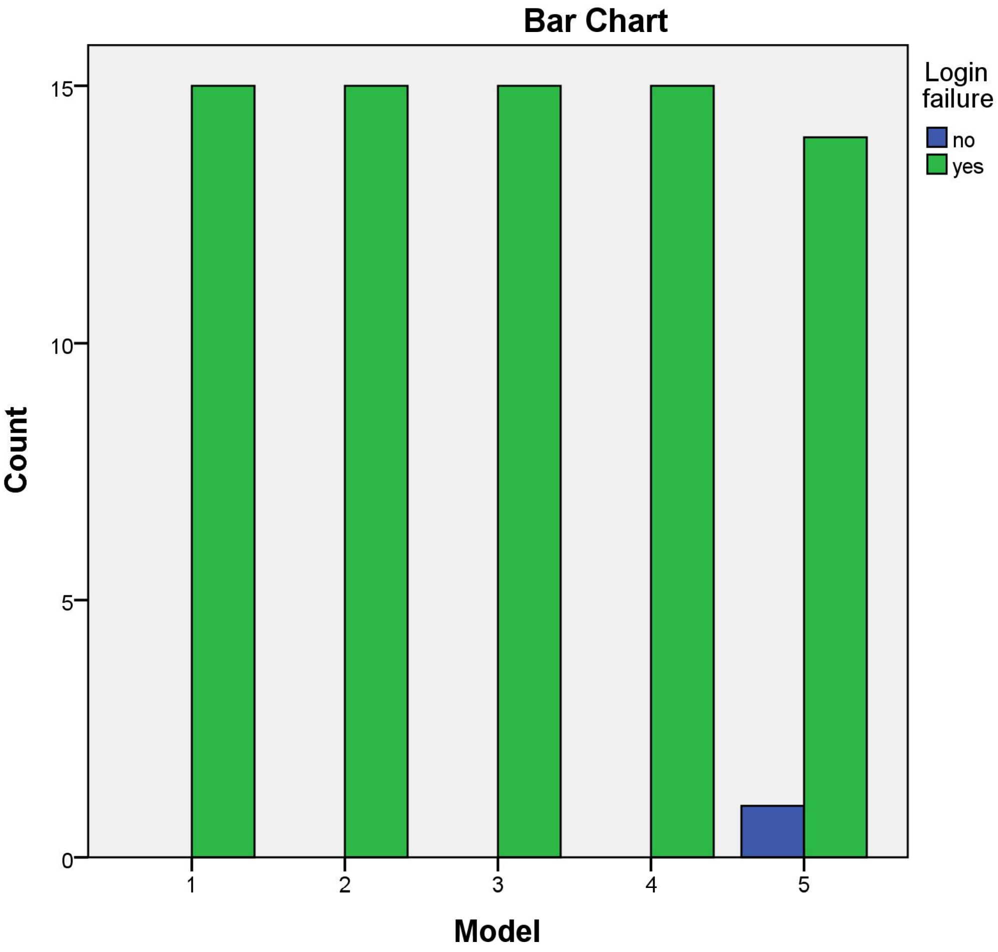
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.054[a]	4	.399
Likelihood Ratio	3.274	4	.513
Linear-by-Linear Association	2.000	1	.157
N of Valid Cases	75		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is .20.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.232	.399
	Cramer's V	.232	.399
N of Valid Cases		75	


Bar Chart
Login failure
no
yes
Count
15
10
5
0
1
2
3
4
5
Model

APPENDIX 9(C) - CHI SQUARE TEST FOR 2 ROUNDS AUTHENTICATION

```
1 - COLOUR, 2 = PATTERN, 3 - MIXED, 4 MAGNITUDE AND 5 BUYTTERFLY CROSSTABS
  /TABLES=auth_type BY failure_rate
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Model * Login failure	75	100.0%	0	0.0%	75	100.0%

Model * Login failure Crosstabulation

			Login failure		Total
			no	yes	
Model	1	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	21.1%	20.0%
		% of Total	0.0%	20.0%	20.0%
	2	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	21.1%	20.0%
		% of Total	0.0%	20.0%	20.0%
	3	Count	0	15	15
		% within Model	0.0%	100.0%	100.0%
		% within Login failure	0.0%	21.1%	20.0%
		% of Total	0.0%	20.0%	20.0%
	4	Count	2	13	15
		% within Model	13.3%	86.7%	100.0%
		% within Login failure	50.0%	18.3%	20.0%
		% of Total	2.7%	17.3%	20.0%
	5	Count	2	13	15
		% within Model	13.3%	86.7%	100.0%
		% within Login failure	50.0%	18.3%	20.0%
		% of Total	2.7%	17.3%	20.0%

Model * Login failure Crosstabulation

		Login failure		Total
		no	yes	
Total	Count	4	71	75
	% within Model	5.3%	94.7%	100.0%
	% within Login failure	100.0%	100.0%	100.0%
	% of Total	5.3%	94.7%	100.0%

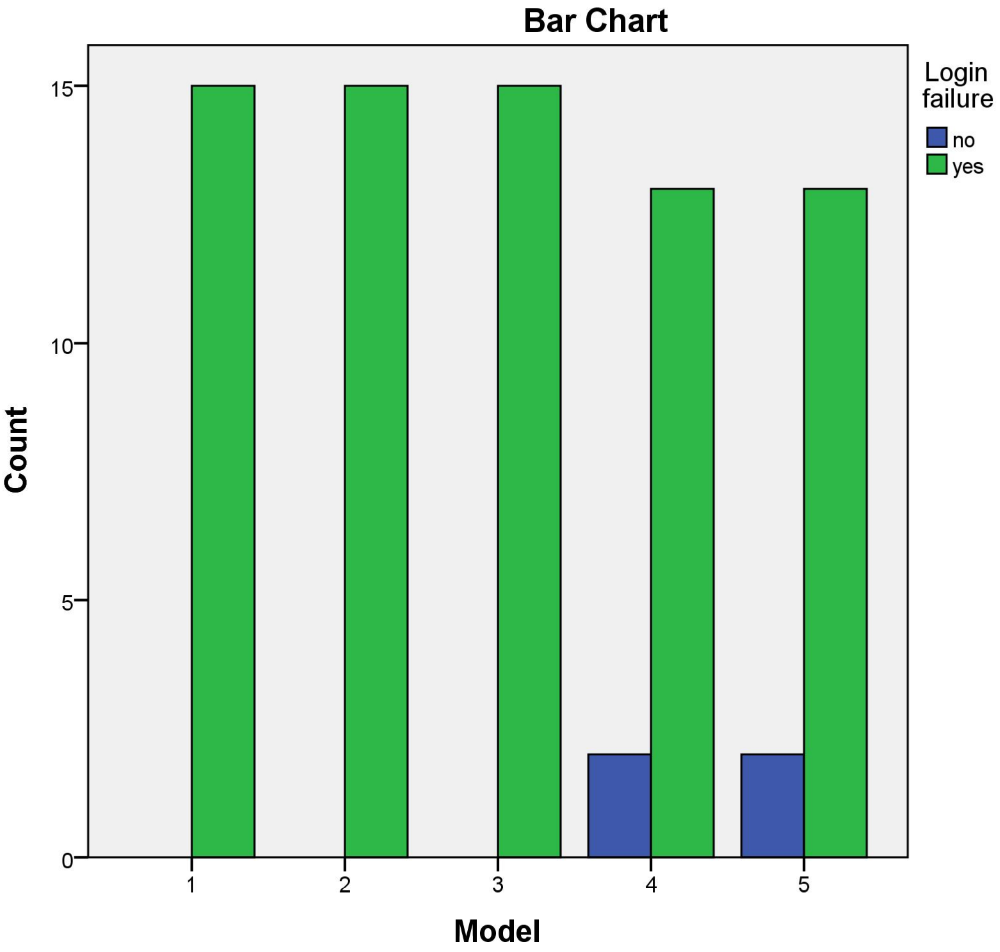
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.338[a]	4	.175
Likelihood Ratio	7.672	4	.104
Linear-by-Linear Association	4.690	1	.030
N of Valid Cases	75		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is .80.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.291	.175
	Cramer's V	.291	.175
N of Valid Cases		75	


Bar Chart
Count
Model
Login failure
no
yes
15
10
5
0
1
2
3
4
5

APPENDX 10 -- CHI SQUARE TEST FOR GUESSABILITY TEST

1 - COLOUR, 2 - MAGNITUDE, 3 - MIXED, 4 - DIGIT AND 5 - NUM. REP.

```
CROSSTABS
  /TABLES=f  ailure_rate BY auth_type
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT
  /COUNT ROUND CELL.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
failure_rate * auth_type	100	100.0%	0	0.0%	100	100.0%

failure_rate * auth_type Crosstabulation

Count

		auth_type					Total
		1	2	3	4	5	
failure_rate	no	3	0	3	2	1	9
	yes	17	20	17	18	19	91
Total		20	20	20	20	20	100

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.151[a]	4	.386
Likelihood Ratio	5.747	4	.219
Linear-by-Linear Association	.242	1	.623
N of Valid Cases	100		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is 1.80.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.204	.386
	Cramer's V	.204	.386
N of Valid Cases		100	

APPENDIX 11(A) OBSERVATIONAL TEST FOR AUTHENTICATION PROTOTYPES (SET 2)

1 - DIGIT, 2 - NUM. REP., 3 - FORM, 4 - CHARACTER AND 5 - WORDCROSSTABS

```
  /TABLES=failure_rate BY auth_type
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ CC
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Failure Rate * Model	100	100.0%	0	0.0%	100	100.0%

Failure Rate * Model Crosstabulation

			Model				
			1	2	3	4	5
Failure Rate	0	Count	1	0	0	0	0
		% within Failure Rate	100.0%	0.0%	0.0%	0.0%	0.0%
		% within Model	5.0%	0.0%	0.0%	0.0%	0.0%
		% of Total	1.0%	0.0%	0.0%	0.0%	0.0%
	1	Count	19	20	20	20	20
		% within Failure Rate	19.2%	20.2%	20.2%	20.2%	20.2%
		% within Model	95.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	19.0%	20.0%	20.0%	20.0%	20.0%
Total		Count	20	20	20	20	20
		% within Failure Rate	20.0%	20.0%	20.0%	20.0%	20.0%
		% within Model	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	20.0%	20.0%	20.0%	20.0%	20.0%

Failure Rate * Model Crosstabulation

			Total
Failure Rate	0	Count	1
		% within Failure Rate	100.0%
		% within Model	1.0%
		% of Total	1.0%
	1	Count	99
		% within Failure Rate	100.0%
		% within Model	99.0%
		% of Total	99.0%
Total		Count	100
		% within Failure Rate	100.0%
		% within Model	100.0%
		% of Total	100.0%

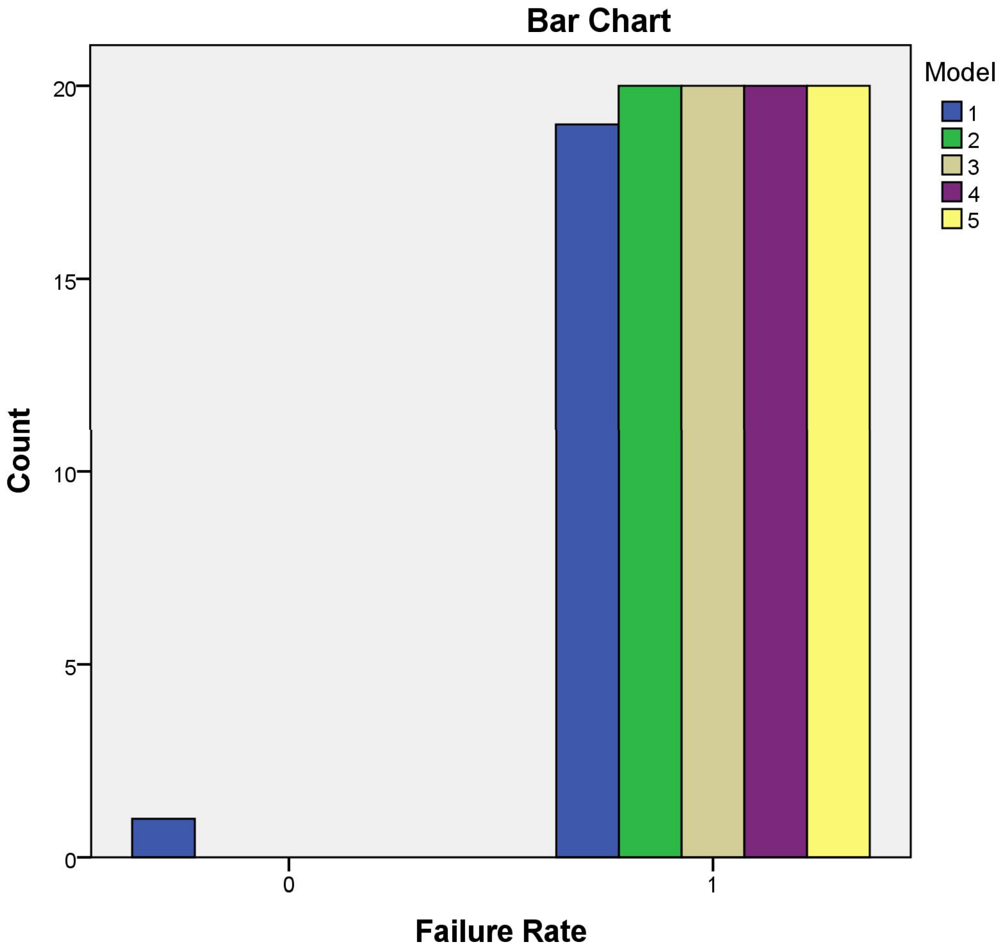
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.040[a]	4	.401
Likelihood Ratio	3.260	4	.515
Linear-by-Linear Association	2.000	1	.157
N of Valid Cases	100		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is .20.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Contingency Coefficient	.197	.401
N of Valid Cases		100	


Bar Chart
Count
20
15
10
5
0
0
1
Failure Rate
Model
1
2
3
4
5

APPENDIX 11(B) CHI SQUARE TEST FOR DUAL LOGIN FAILURE RATE

1 - DIGIT, 2 - NUM. REP, 3 - FORM, 4 - CHAR, 5 - WORD

```
CROSSTABS
  /TABLES=failure_rate BY auth_type
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Failure Rate * Model	100	100.0%	0	0.0%	100	100.0%

Failure Rate * Model Crosstabulation

			Model				
			1	2	3	4	5
Failure Rate	no	Count	2	1	1	1	0
		% within Failure Rate	40.0%	20.0%	20.0%	20.0%	0.0%
		% within Model	10.0%	5.0%	5.0%	5.0%	0.0%
		% of Total	2.0%	1.0%	1.0%	1.0%	0.0%
	yes	Count	18	19	19	19	20
		% within Failure Rate	18.9%	20.0%	20.0%	20.0%	21.1%
		% within Model	90.0%	95.0%	95.0%	95.0%	100.0%
		% of Total	18.0%	19.0%	19.0%	19.0%	20.0%
Total		Count	20	20	20	20	20
		% within Failure Rate	20.0%	20.0%	20.0%	20.0%	20.0%
		% within Model	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	20.0%	20.0%	20.0%	20.0%	20.0%

Failure Rate * Model Crosstabulation

			Total
Failure Rate	no	Count	5
		% within Failure Rate	100.0%
		% within Model	5.0%
		% of Total	5.0%
	yes	Count	95
		% within Failure Rate	100.0%
		% within Model	95.0%
		% of Total	95.0%
Total		Count	100
		% within Failure Rate	100.0%
		% within Model	100.0%
		% of Total	100.0%

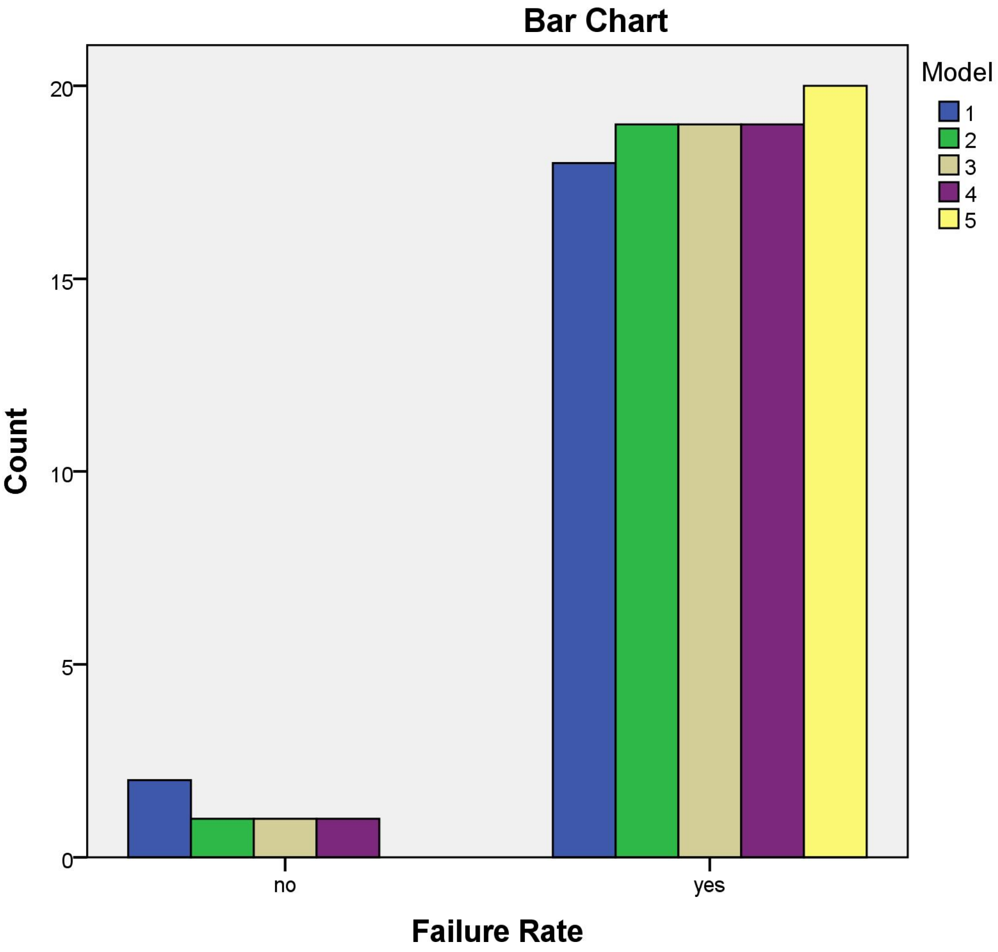
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.105[a]	4	.716
Likelihood Ratio	2.878	4	.578
Linear-by-Linear Association	1.667	1	.197
N of Valid Cases	100		

a. 5 cells (50.0%) have expected count less than 5. The minimum expected count is 1.00.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.145	.716
	Cramer's V	.145	.716
N of Valid Cases		100	


Bar Chart
Model
1
2
3
4
5
Count
20
15
10
5
0
no
yes
Failure Rate

APPENDIX 12(A) - CHI SQUARE ANALYSIS OF EXPERIMENT ON VULNERABILITY DUE TO VERBAL DESCRIPTIONS

1 - COLOUR, 2 - PATTERN, 3 - MAGNITUDE, 4 - MIXED, 5 - DIGIT, 6 - NUMBER REP.

```
CROSSTABS
  /TABLES=guess_success BY auth_type
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
guess_success * auth_type	120	100.0%	0	0.0%	120	100.0%

guess_success * auth_type Crosstabulation

			auth_type						Total
			1	2	3	4	5	6	
guess_success	guess fail	Count	8	8	10	12	5	7	50
		% within guess_success	16.0%	16.0%	20.0%	24.0%	10.0%	14.0%	100.0%
		% within auth_type	40.0%	40.0%	50.0%	60.0%	25.0%	35.0%	41.7%
		% of Total	6.7%	6.7%	8.3%	10.0%	4.2%	5.8%	41.7%
	guess pass	Count	12	12	10	8	15	13	70
		% within guess_success	17.1%	17.1%	14.3%	11.4%	21.4%	18.6%	100.0%
		% within auth_type	60.0%	60.0%	50.0%	40.0%	75.0%	65.0%	58.3%
		% of Total	10.0%	10.0%	8.3%	6.7%	12.5%	10.8%	58.3%
Total		Count	20	20	20	20	20	20	120
		% within guess_success	16.7%	16.7%	16.7%	16.7%	16.7%	16.7%	100.0%
		% within auth_type	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	16.7%	16.7%	16.7%	16.7%	16.7%	16.7%	100.0%

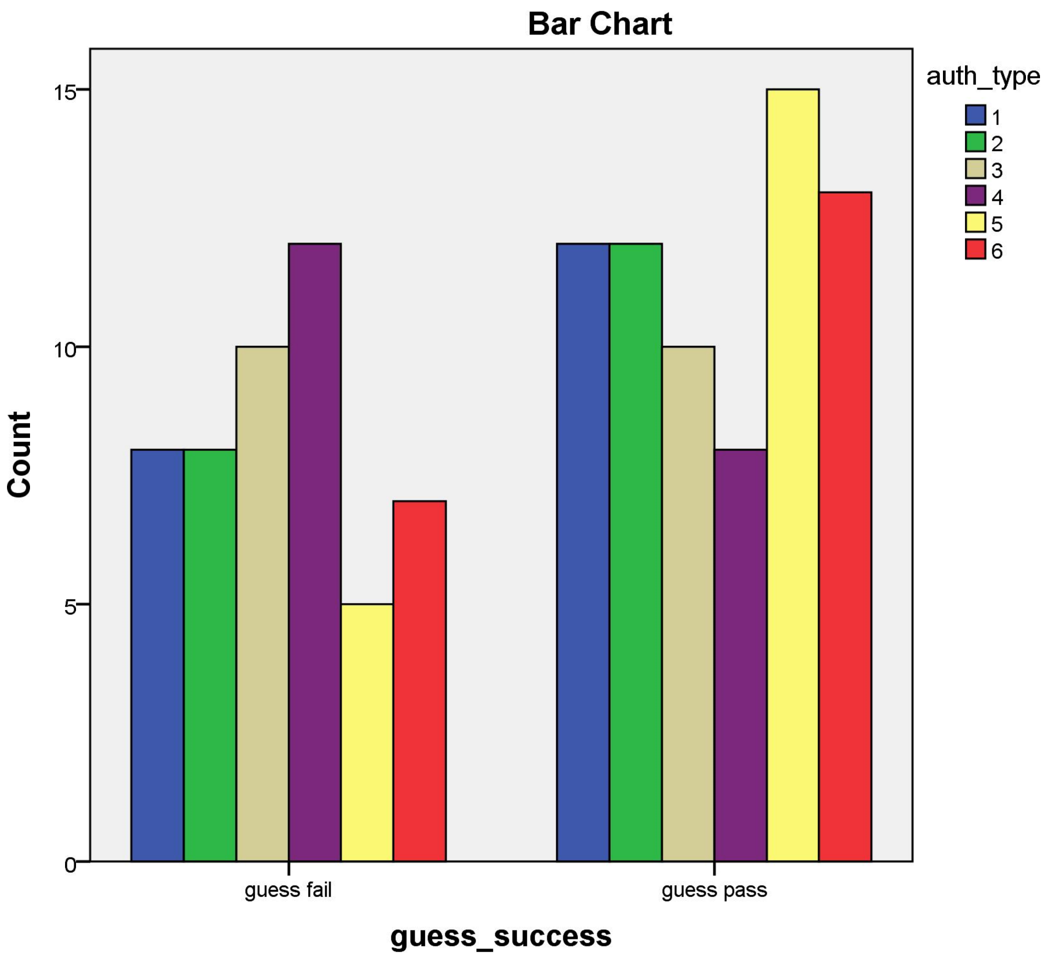
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.034[a]	5	.303
Likelihood Ratio	6.128	5	.294
Linear-by-Linear Association	.420	1	.517
N of Valid Cases	120		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 8.33.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.224	.303
	Cramer's V	.224	.303
N of Valid Cases		120	


Bar Chart
Count
15
10
5
0
guess fail
guess pass
guess_success
auth_type
🟦 1
🟩 2
3
4
🟨 5
🟥 6

APPENDIX 12(B) - RESULTS OF EXPERIMENT ON GUESSING ATTACKS DUE TO WRITTEN DESCRIPTIONS

1 - COLOUR, 2 - PATTERN, 3 - MAGNITUDE, 4 - MIXED, 5 DIGIT AND 6 - NUMBER REP.

```
CROSSTABS
  /TABLES=success_rate BY auth_type
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ PHI
  /CELLS=COUNT ROW COLUMN TOTAL
  /COUNT ROUND CELL
  /BARCHART.
```

Crosstabs

```
[DataSet0]
```

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Guess success * Model	120	100.0%	0	0.0%	120	100.0%

Guess success * Model Crosstabulation

			Model						Total
			1	2	3	4	5	6	
Guess success	guess fail	Count	7	10	11	13	7	9	57
		% within Guess success	12.3%	17.5%	19.3%	22.8%	12.3%	15.8%	100.0%
		% within Model	35.0%	50.0%	55.0%	65.0%	35.0%	45.0%	47.5%
		% of Total	5.8%	8.3%	9.2%	10.8%	5.8%	7.5%	47.5%
	guess pass	Count	13	10	9	7	13	11	63
		% within Guess success	20.6%	15.9%	14.3%	11.1%	20.6%	17.5%	100.0%
		% within Model	65.0%	50.0%	45.0%	35.0%	65.0%	55.0%	52.5%
		% of Total	10.8%	8.3%	7.5%	5.8%	10.8%	9.2%	52.5%
Total		Count	20	20	20	20	20	20	120
		% within Guess success	16.7%	16.7%	16.7%	16.7%	16.7%	16.7%	100.0%
		% within Model	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	16.7%	16.7%	16.7%	16.7%	16.7%	16.7%	100.0%

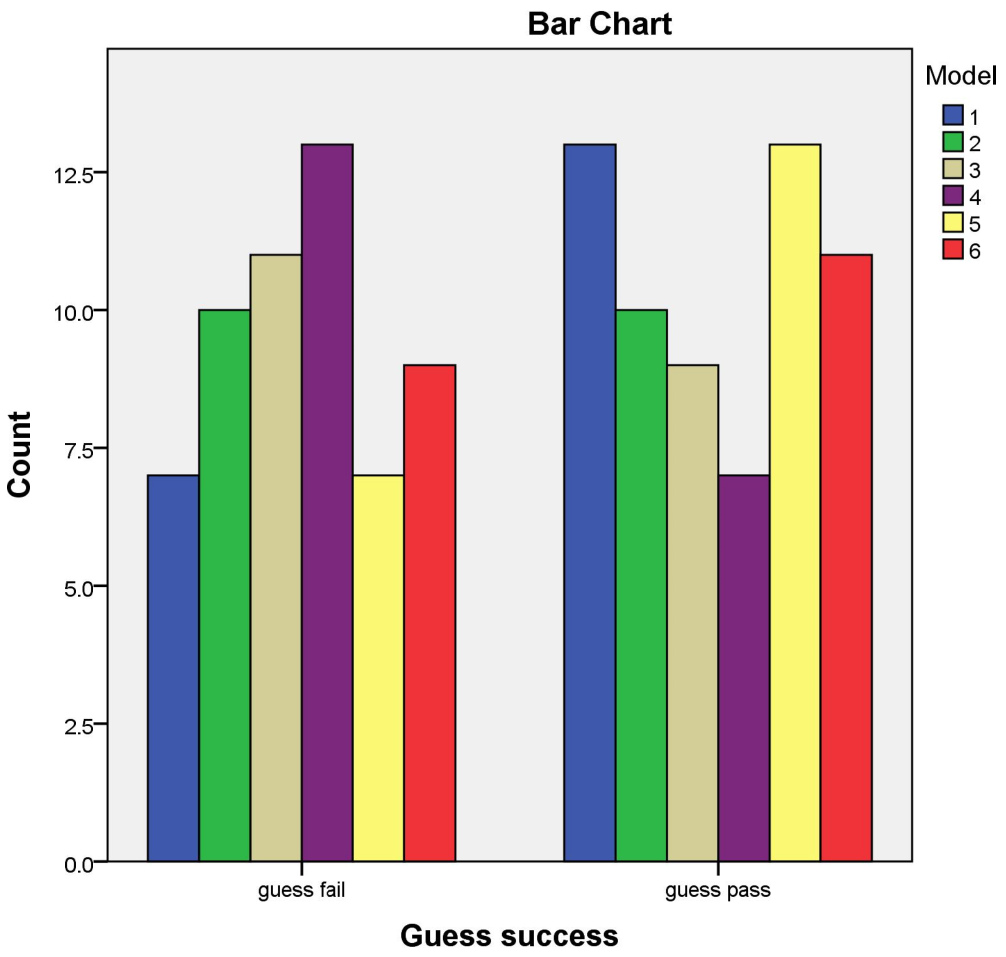
Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.514[a]	5	.356
Likelihood Ratio	5.585	5	.349
Linear-by-Linear Association	.026	1	.873
N of Valid Cases	120		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.50.

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	.214	.356
	Cramer's V	.214	.356
N of Valid Cases		120	


Bar Chart
Count
12.5
10.0
7.5
5.0
2.5
0.0
guess fail
guess pass
Guess success
Model
1
2
3
4
5
6