

**A Reversible and Imperceptible Watermarking
Approach for Ensuring the Integrity and Authenticity of
Brain MR Images**

Asaad Flayyih Qasim



University of
Salford
MANCHESTER

School of Computing, Science and Engineering

University of Salford, Greater Manchester, UK

Thesis Submitted in Partial Fulfilment of the Requirements for the
Degree of Doctor of Philosophy

2019

TABLE OF CONTENTS

TABLE OF CONTENTS	i
LIST OF FIGURES	vi
LIST OF TABLES	ix
ACKNOWLEDGEMENT	xi
DECLARATION	xii
LIST OF ABBREVIATIONS	xiii
LIST OF PUBLICATIONS	xv
ABSTRACT	xvi
CHAPTER ONE: Introduction	1
1.1 The Statement of the Problem	1
1.2 Research Motivation	3
1.3 Research Questions	5
1.4 Research Aim and Objectives	6
1.5 Research Contributions	7
1.6 Research Methodology	9
1.7 Thesis Organisation	14
CHAPTER TWO: Technical Background	16
2.1 Introduction.....	16
2.2 Medical Imaging System	17
2.2.1 Magnetic Resonance Imaging	17
2.2.2 Digital Imaging and Communications in Medicine	18
2.3 Conventional Security Measures	20
2.3.1 Data Encryption.....	20
2.3.2 Cryptographic Hash Functions.....	21
2.3.3 Perceptual Hash Functions	21
2.3.4 File Header	22
2.4 Digital watermarking	23
2.4.1 Digital Watermarking Classifications	24
2.4.2 Digital Watermarking Requirements	26
2.4.2.1 Fidelity	26
2.4.2.2 Robustness	26
2.4.2.3 Data Payload (Capacity)	26

2.4.2.4	Security	27
2.4.2.5	Computational Complexity	27
2.5	Evaluation of Watermarked Image Quality	28
2.5.1	Physical Assessment	28
2.5.1.1	Peak Signal to Noise Ratio	28
2.5.1.2	Structural Similarity Index.....	29
2.5.1.3	Root Mean Squared Error	30
2.5.1.4	Image Fidelity	30
2.5.2	Visual Assessment.....	30
2.5.2.1	Receiver Operating Characteristic	30
2.5.2.2	Visual Grading Analysis	32
2.5.2.2.1	Absolute VGA	33
2.5.2.2.2	Relative VGA	33
2.5.2.3	Variability in Visual Assessment of Image Quality	34
2.5.2.4	Image Quality Criteria	34
2.6	Evaluation of Extracted Watermark Validity	36
2.6.1	Correlation Coefficient.....	36
2.6.2	Similarity Measure (SIM)	36
2.6.3	Bit Error Rate	36
2.6.4	Accuracy Ratio.....	36
2.7	Chapter Summary	37
CHAPTER THREE: Literature Review		38
3.1	Introduction.....	38
3.2	Requirements of Medical Images Watermarking	40
3.2.1	Imperceptibility	40
3.2.2	Reversibility	40
3.2.3	Reliability	40
3.3	Medical Image Watermarking Techniques.....	41
3.3.1	Classical Methods while Minimising the Distortion.....	41
3.3.2	Region of Interest and Region of Non Interest Watermarking Methods	41
3.3.3	Reversible Watermarking Methods.....	42
3.3.3.1	Compression Based Technique.....	44
3.3.3.2	Histogram Modification Based Technique	45
3.3.3.3	Quantisation Based Technique	46

3.3.3.4	Difference Expansion Based Technique	46
3.4	Purposes of Medical Image Watermarking	48
3.4.1	Authentication Schemes	48
3.4.2	EPR Data Hiding Schemes.....	53
3.4.3	Authentication and EPR Data Hiding Schemes	54
3.5	Chapter Summary	55
CHAPTER FOUR: Assessment of Perceptual Distortion Boundary		57
4.1	Introduction.....	57
4.2	Study Design.....	58
4.3	Data Collection	60
4.4	Generation of Watermarked Images Samples.....	60
4.5	Reduction of Images Samples.....	69
4.6	Construction and Validation of Quality Criteria Items.....	70
4.7	Ethical Issues	72
4.8	Selection of Observer.....	72
4.9	Implementation of Visual Assessment	73
4.10	Experimental Results and Discussion.....	74
4.10.1	Approach Reliability	74
4.10.2	Data Analysis and Results	74
4.10.3	Comparison with Other Approaches	80
4.11	Chapter Summary	82
CHAPTER FIVE: Reversible Watermarking Approach Based on Difference Expansion Technique		83
5.1	Introduction.....	83
5.2	Proposed Scheme	85
5.2.1	Watermark Creation	85
5.2.1.1	Authentication Watermark.....	86
5.2.1.2	Integrity Watermark.....	86
5.2.1.3	Watermark Compression	86
5.2.2	Embedding Process	87
5.2.2.1	Image Segmentation	89
5.2.2.2	Smooth Regions Identification	90
5.2.2.3	Watermark Data Encoding.....	91
5.2.3	Extraction and Verification Process.....	92

5.3	Experimental Results and Discussion.....	95
5.3.1	Proposed System Performance Measurement.....	96
5.3.1.1	Imperceptibility.....	98
5.3.1.2	Reversibility.....	99
5.3.1.2.1	Image Reversibility.....	99
5.3.1.2.2	Watermark Reversibility.....	99
5.3.1.3	Capacity.....	102
5.3.1.4	Robustness.....	102
5.3.2	Comparison with Existing Approaches.....	106
5.4	Chapter Summary.....	109
CHAPTER SIX: Integration of the Proposed Watermarking Approach into Medical Imaging Systems.....		111
6.1	Introduction.....	111
6.2	Security Flaws in Medical Imaging Systems.....	113
6.3	Design and Evaluation Criteria for Medical Images Watermarking.....	114
6.3.1	Design Phase.....	115
6.3.2	Evaluation Phase.....	116
6.4	Integration of the Proposed Approach into Medical Imaging.....	117
6.5	Validation of the Proposed Medical Imaging Workflow.....	118
6.5.1	Security Threats in Medical Imaging Workflow.....	120
6.5.1.1	Scenario One (S1) – Acquisition Phase.....	120
6.5.1.2	Scenario Two (S2) – Transmission Phase.....	120
6.5.1.3	Scenario Three (S3) – Viewing Phase.....	120
6.5.1.4	Scenario Four (S4) – Archiving Phase.....	120
6.5.2	Validation of the Proposed Integration Process.....	122
6.5.2.1	Scenario One (S1) – Acquisition Phase.....	122
6.5.2.2	Scenario Two (S2) – Transmission Phase.....	122
6.5.2.3	Scenario Three (S3) – Viewing Phase.....	122
6.5.2.4	Scenario Four (S4) – Archiving Phase.....	122
6.6	Chapter Summary.....	124
CHAPTER SEVEN: Discussion.....		125
7.1	Critical Evaluation of Research.....	125
7.1.1	Imperceptibility.....	125
7.1.2	Reversibility.....	127

7.1.3 Integrity Control and Authentication	128
7.1.3.1 Imperceptibility.....	129
7.1.3.2 Reversibility.....	129
7.1.3.3 Capacity	129
7.1.3.4 Robustness	129
7.1.4 Relevance of Digital Watermarking in Medical Imaging Systems.....	130
7.2 Review of Aim and Objectives	131
7.3 Review of Methodology	133
7.4 Research Contributions and Implications	135
CHAPTER EIGHT: Conclusion and Future Research	137
8.1 Conclusion	137
8.1.1 Contributions of Research to Literature	140
8.1.2 Limitations of the Research.....	141
8.2 Future Research Direction	142
APPENDICES.....	144
I. Ethical Approval Provided by the University of Salford	144
II. Research Participant’s Consent Form	145
REFERENCES	146

LIST OF FIGURES

Fig. 1.1: An example of malicious manipulations applied to a medical image of a patient's liver.....	2
Fig. 1.2: The methodology steps adopted in this research to enhance trust within medical imaging domains.	10
Fig. 2.1: The structure of DICOM images.	19
Fig. 2.2: Main components of digital watermarking schemes: A) Watermark generation, B) Watermark embedding, and C) Watermark extraction.....	23
Fig. 2.3: Classification of digital watermarking based on four various criteria.....	25
Fig. 2.4: The trade-off triangle between the three essential watermarking properties.....	27
Fig. 3.1: Main components of reversible watermarking approaches.	43
Fig. 4.1: Key steps adopted in this research for visually assessing the imperceptibility of watermarked images.	59
Fig. 4.2: The eight brain MR images in DICOM format (16bpp, 512x512 pixels) used in the proposed approach to generate a set of images with various distortion levels.....	61
Fig. 4.3: An example of the modifications of the pixels for a part of an image (8x8 pixels) after encoding the watermark data.....	62
Fig. 4.4: Sections of the watermarked images after implementing the first reversible watermarking technique (1-bit per 2-pixels).	63
Fig. 4.5: Sections of the watermarked images after implementing the second reversible watermarking technique (3-bits per quad-pixels).....	64
Fig. 4.6: Sections of the watermarked images after implementing the third reversible watermarking technique (2-bits per 2-pixels).....	65
Fig. 4.7: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the first reversible watermarking technique (1-bit per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	66
Fig. 4.8: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the second reversible watermarking technique (3-bits per quad-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	67
Fig. 4.9: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the third reversible watermarking	

technique (2-bits per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	67
Fig. 4.10: The overall observers' scores for the eight criteria items against images PSNR values by using five-point Likert.....	76
Fig. 4.11: The overall observers' scores for the eight criteria items against images PSNR values by using three-point Likert.....	77
Fig. 4.12: The mean and SD error bars for the overall observers' scores for the eight criteria items against images PSNR values by using a five-point Likert scale.....	79
Fig. 4.13: The mean and SD error bars for the overall observers' scores for the eight criteria items against images PSNR values by using a three-point Likert scale.....	79
Fig. 5.1: Process diagram for the watermark embedding process.....	88
Fig. 5.2: An example of MR slice segmentation, A) Original image, B) Segmented, C) Eroded, D) Dilated, and E) Filled holes.	89
Fig. 5.3: An example of a 3x3 block of pixels inside the ROI part.....	90
Fig. 5.4: Process diagram for the watermark extraction and verification process.	94
Fig. 5.5: The sixteen brain MR scans in DICOM format (16bpp, 512x512 pixels) provided by the MRI unit of Al-Kadhimiya Teaching Hospital (Iraq) and utilised to assess the performance of the proposed technique.....	97
Fig. 5.6: The nine brain MR scans in DICOM format (16bpp, 512x512 pixels) selected from a publicly available and standardised medical images dataset downloaded from TCIA website and utilised to assess the performance of the proposed technique	98
Fig. 5.7: Examples of the original DICOM images and their corresponding watermarked and extracted images after applying the proposed watermarking approach.	100
Fig. 5.8: Comparison between the proposed approach and other reversible watermarking schemes presented in the literature in terms of distortion level (PSNR) versus hiding capacity.....	108
Fig. 5.9: Evaluation of distortion level (PSNR) versus payload capacity for the proposed scheme against other DE-based reversible watermarking schemes using the DICOM15.	108
Fig. 5.10: Evaluation of distortion level (IF) versus payload capacity for the proposed scheme against other DE-based reversible watermarking schemes using the DICOM15.	109
Fig. 6.1: A generic PACS infrastructure which comprises three main components connected by a high-speed communication network including acquisition devices, archive server, and diagnosis workstations.....	112
Fig. 6.2: The design and evaluation phases for the proposed watermarking approach. ...	114

Fig. 6.3: Integration of the proposed watermarking approach into PACS infrastructures.
..... **119**

Fig. 6.4: Security threats that may face medical imaging during routine medical practices.
..... **121**

Fig. 6.5: Validation of the ability of the proposed approach to tackle the identified security threats (scenarios) that may face medical images during routine medical practices..... **123**

LIST OF TABLES

Table 3-1: A comparison of existing digital watermarking schools applied to medical images.....	42
Table 3-2: Summary of different medical images watermarking approaches stated in the literature.....	49
Table 4-1: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the first reversible watermarking technique (1-bit per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	68
Table 4-2: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the second reversible watermarking technique (3-bits per quad-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	68
Table 4-3: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the third reversible watermarking technique (2-bits per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%).....	69
Table 4-4: The selected watermarked images after applying the reduction strategy.	70
Table 4-5: Image quality criteria adopted within this research to assess the visualisation of the anatomical details of brain MR images.	71
Table 4-6: Cronbach's alpha values for the observers' scores on all experimental images.	75
Table 4-7: Aggregated (mean) PSNR values for all experimental images with the SD considered.....	78
Table 4-8: Performance comparison of the proposed approach against approaches identified in the literature based on various criteria.	81
Table 5-1: A section of metadata fields selected from a DICOM data dictionary.	87
Table 5-2: The parameters used to conduct the experiment and evaluate the proposed system performance.....	96
Table 5-3: Imperceptibility between the original, watermarked, and extracted images using PSNR, SSIM, RMSE and IF metrics after applying the proposed watermarking approach.	101

Table 5-4: PSNR values after applying the proposed approach for hiding various payload.	103
Table 5-5: Reversibility evaluation of both the original image and embedded watermark after applying various manipulations to the watermarked images.	104
Table 5-6: Performance comparison of the proposed scheme against approaches identified in the literature.....	106

ACKNOWLEDGEMENT

First and foremost, all praise and gratitude are to **Allah**, the lord of the world, the most beneficent, and the most merciful for helping me and giving me the health and power to complete this research work.

I would like to express my sincere gratitude to my supervisors, Professor **Farid Meziane** and Dr **Rob Aspin**, for their enormous contributions, encouragement and guidance throughout the course of this research. I am honoured and consider myself fortunate to have worked under their supervision. I am also grateful to Professor **Peter Hogg**, Research Dean in the School of Health Sciences at the University of Salford., whose guidance, advice and ideas have improved my research many-fold.

I would like to acknowledge the Iraqi government, represented by the ministry of higher education and scientific research, for giving me the opportunity to accomplish my PhD study in the United Kingdom. I would also like to recognise with much appreciation the role of all those employees involved in Iraqi Cultural Attaché in London throughout my PhD study.

I also wish to thank my parents, brothers and sisters for their endless support, encouragement and attention. I am also grateful to my beloved wife, **Sorur Al-Bayati**, and my children, **Mayar** and **Adam**, for their support, kindness and patience as they accompanied me along this journey.

Finally, I would like to thank all friends, colleagues and staffs at the University of Salford for their help and support.

DECLARATION

I hereby declare that the work in this thesis is my own and no portion of it has been submitted in support of an application for another award or qualification of this or any other university or institute of learning.

Asaad Flayyih Qasim

19 March 2019

LIST OF ABBREVIATIONS

ACR	American College of Radiology
AES	Advanced Encryption Standard
API	Application Programming Interface
AR	Accuracy Ratio
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
CALIC	Context-based Adaptive Lossless Image Codec
CDCS	Class Dependent Coding Scheme
CEC	Commission of European Communities
CRC	Correlation Coefficient
CRC-16	Cyclic Redundancy Check-16 bits
CS	Critical Situations
CT	Computerised Tomography
DC	Data Compression
DCT	Discrete Cosine Transform
DE	Difference Expansion
DES	Data Encryption Standard
DGT	Discrete Gould transform
DICOM	Digital Imaging and Communications in Medicine
DROC	Differential Receiver Operating Characteristic
DS	Digital Signature
DSA	Digital Signature Algorithm
DT-CWT	Dual Tree Complex Wavelet Transform
DWPT	Discrete Wavelet Packet Transform
DWT	Discrete Wavelet Transform
ECG	Electrocardiograph
EPR	Electronic Patient Record
FDCT	Fractional Discrete Cosine Transform
FROC	Free-response Receiver Operating Characteristic
GSDF	Grayscale Standard Display Function
HBS	Histogram Bin Shifting
HIS	Hospital Information Systems
HVS	Human Visual System
IDEA	International Data Encryption Algorithm
IF	Image Fidelity
IODs	Information Object Definitions
ISB	Intermediate Significant Bit
IWT	Integer Wavelet Transform
JPEG	Joint Photographic Experts Group

JPEG-LS	JPEG Lossless
JPEG-XR	JPEG eXtended Range
LCD	Liquid Crystal Display
LROC	Localisation Receiver Operating Characteristic
LSB	Least Significant Bit
MAC	Message Authentication Code
MD5	Message Digest 5
MPEG	Moving Picture Expert Group
MRI	Magnetic Resonance Imaging
MSE	Mean Squared Error
NEMA	National Electrical Manufacturers Association
PACS	Picture Archiving and Communication Systems
PE	Prediction Error
PSNR	Peak Signal to Noise Ratio
PTB	Pixel to Block
QIM	Quantisation Index Modulation
RC	Rivest Cipher
RIS	Radiology Information Systems
RLE	Run Length Encoding
RMSE	Root Mean Squared Error
RNS	Residue Number System
ROC	Receiver Operating Characteristic
ROI	Region of Interest
RONI	Region of Non Interest
RSA	Rivest-Shamir-Adleman
SC	Similarity Coefficient
SD	Standard Deviation
SDT	Signal Detection Theory
SHA-256	Secure Hash Algorithm-256 bits
SIM	Similarity Measure
SNR	Signal to Noise Ratio
SQS	Sequential Quantisation Strategy
SSIM	Structural Similarity
SVD	Singular Value Decomposition
TCIA	The Cancer Imaging Archive
VGA	Visual Grading Analysis
VGAS _{abs}	Absolute Visual Grading Analysis Score
VGAS _{rel}	Relative Visual Grading Analysis Score
WQM	Weighted Quantisation Method

LIST OF PUBLICATIONS

1. Qasim, A. F., Mezziane, F., & Aspin, R. (2017). *Digital watermarking for confirming trust in digital medical workflows*. Salford Postgraduate Annual Research Conference (SPARC). University of Salford, Greater Manchester, UK, Page 95.
2. Qasim, A. F., Aspin, R., & Mezziane, F. (2017). *An initial exploration of digital watermarking in medical image authentication*. Paper presented at the CSE 2017 Annual PGR Symposium, University of Salford, Greater Manchester, UK.
3. Qasim, A. F., Mezziane, F., & Aspin, R. (2017). *An investigation into the imperceptibility boundary of medical images watermarking*. Poster presented at Health, Wellbeing and Society Research. University of Salford, Greater Manchester, UK.
4. Qasim, A. F., Mezziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27, 45-60.
5. Qasim, A. F., Mezziane, F., & Aspin, R. (2018). *A reversible and imperceptible watermarking scheme for MR images authentication*. The 24th International Conference on Automation and Computing (ICAC'2018), Newcastle upon Tyne, UK.
6. Qasim, A. F., Aspin, R., Mezziane, F., & Hogg, P. (2019). Assessment of perceptual distortion boundary through applying reversible watermarking to brain MR images. *Signal Processing: Image Communication*, 70, 246-258.
7. Qasim, A. F., Aspin, R., Mezziane, F., & Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. *Multimedia tools and applications*, 78 (12), 16433-16463.
8. Qasim, A. F., Aspin, R. & Mezziane, F. (2019). *Integration of Digital Watermarking Technique into Medical Imaging Systems*. The 10th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2019), Leeds, UK. (Awarded as Best Paper).
9. Qasim, A. F., Mezziane, F., & Aspin, R. (2019). The Integration of Digital Watermarking Approach into Smart Healthcare for Verifying the Integrity and Authenticity of Medical Images. Submitted to *Springer Journal of Reliable Intelligent Environments Special Issue on 'Security, Usability and Sustainability of Smart Cities'*.

ABSTRACT

The digital medical workflow has many circumstances in which the image data can be manipulated both within the secured Hospital Information Systems (HIS) and outside, as images are viewed, extracted and exchanged. This potentially grows ethical and legal concerns regarding modifying images details that are crucial in medical examinations. Digital watermarking is recognised as a robust technique for enhancing trust within medical imaging by detecting alterations applied to medical images. Despite its efficiency, digital watermarking has not been widely used in medical imaging. Existing watermarking approaches often suffer from validation of their appropriateness to medical domains. Particularly, several research gaps have been identified: (i) essential requirements for the watermarking of medical images are not well defined; (ii) no standard approach can be found in the literature to evaluate the imperceptibility of watermarked images; and (iii) no study has been conducted before to test digital watermarking in a medical imaging workflow. This research aims to investigate digital watermarking to designing, analysing and applying it to medical images to confirm manipulations can be detected and tracked. In addressing these gaps, a number of original contributions have been presented. A new reversible and imperceptible watermarking approach is presented to detect manipulations of brain Magnetic Resonance (MR) images based on Difference Expansion (DE) technique. Experimental results show that the proposed method, whilst fully reversible, can also realise a watermarked image with low degradation for reasonable and controllable embedding capacity. This is fulfilled by encoding the data into smooth regions (blocks that have least differences between their pixels values) inside the Region of Interest (ROI) part of medical images and also through the elimination of the large location map (location of pixels used for encoding the data) required at extraction to retrieve the encoded data. This compares favourably to outcomes reported under current state-of-art techniques in terms of visual image quality of watermarked images. This was also evaluated through conducting a novel visual assessment based on relative Visual Grading Analysis (relative VGA) to define a perceptual threshold in which modifications become noticeable to radiographers. The proposed approach is then integrated into medical systems to verify its validity and applicability in a real application scenario of medical imaging where medical images are generated, exchanged and archived. This enhanced security measure, therefore, enables the detection of image manipulations, by an imperceptible and reversible watermarking approach, that may establish increased trust in the digital medical imaging workflow.

CHAPTER ONE

Introduction

Digital medical images can be manipulated both within the secure medical system environment and outside, as images are viewed, extracted and transmitted. This, potentially, leads to a breakdown in trust which impacts on the reliability of image reading and diagnosis. Digital watermarking has been recognised as a promising approach to confirm the authenticity and integrity of medical images through applying techniques that have the ability to detect manipulations that may occur on images during viewing, transmitting and archiving. This thesis presents a novel digital watermarking approach to enhance trust in the digital clinical workflow by applying robust integrity and authenticity constraints within medical imaging. This is achieved through both investigating the security threats that can face medical images during routine clinical practices and identifying the essential requirements of medical domains when applying digital watermarking to medical images. The approach intends to create a framework to select techniques and criteria for evaluating the proposed methods to verify their validity and applicability.

1.1 The Statement of the Problem

In most medical imaging domains, conventional file-based diagnosis has mostly migrated to technology enabled e-diagnosis within digital medical imaging systems. Hospital Information Systems (HIS) and medical imaging platforms produce and manage digital images across many modalities including X-ray, Ultrasound, Magnetic Resonance Imaging (MRI) Computerised Tomography (CT), etc. Images taken in a hospital are saved in the Picture Archiving and Communication Systems (PACS), which act as integrated systems for capturing, exchanging and archiving medical data. Typically, the digital images are managed within a digital workflow based on the Digital Imaging and Communications in Medicine (DICOM) standard (DICOM, 2006).

The exchange of these medical images through, and across, hospitals, locations and administrative organisations, has become a common practice for many purposes within the digital medical workflow. These include diagnosis, treatment, training, distance learning and medical consultations between clinicians and radiologists (Memon et al., 2011). In most cases, this is within the defined workflows of the PACS systems, but there are also many

cases, both valid and occasionally nefarious, in which images and data are withdrawn from one system to be transferred to other institutions or people. Malicious manipulations (Fig. 1.1) on the medical images are feasible for getting counterfeit health insurance demands by some insurance companies or for hiding medical situations for gaining personal advantages (Liew and Zain, 2011). Many cases of manipulations can be applied to medical images, but the issue is how they can be detected? By physically viewing the images, detecting such reasonable manipulations that include entirely forged abnormalities would be impossible. This potentially has serious implications on the diagnosis of patients with possible life affecting impact outcomes, mortality, etc (Rathi, 2012). Therefore, the ability to maintain the integrity and authenticity of these images has become significant, both within the internal systems and during their transfer to other systems (Qasim et al., 2018a). Integrity of images can be fulfilled by encrypting the images during sharing across the network. Authentication requires utilising measures to determine whether confidentiality and/or the integrity of the data has been breached (Pushpala and Nigudkar, 2005).

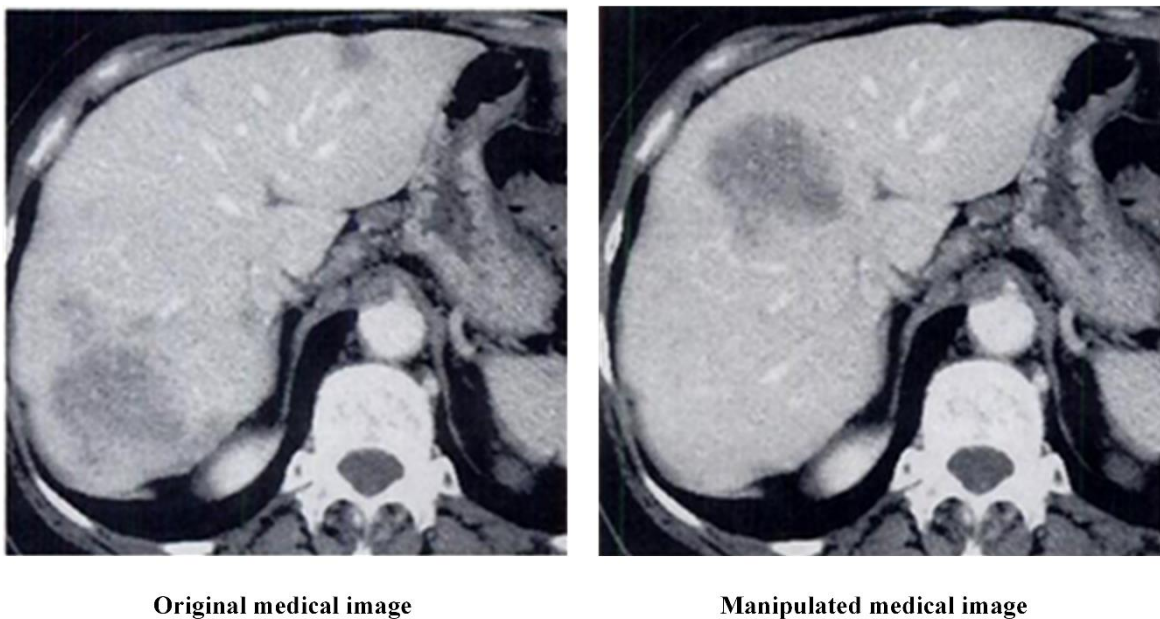


Fig. 1.1: An example of malicious manipulations applied to a medical image of a patient's liver. The position of the infected region (dark grey) was changed from the lower left corner to the upper left corner by using available software (e.g. Adobe Photoshop) (Richardson et al., 1995).

Two methods are typically utilised to ensure the integrity and authenticity of image data: metadata and digital watermarking. In medical imaging, metadata includes patient information connecting the image to the patient and medical report (Kobayashi et al., 2009). The most common metadata structure fulfils part 15 of the DICOM standard, where the data

is saved in the image header as a part of the image file and includes information to describe the patient, image, and acquisition properties (Pianykh, 2009). Existing metadata techniques not providing a secure relationship between the metadata and medical image. It is, therefore, easy to destroy, modify, or otherwise disconnect the metadata rendering the image unreliable. Digital watermarking is recognised as a robust approach to tackle these failings by using techniques to hide digital data (watermark) within digital objects, such that the embedded data can be revealed or extracted later to provide a confirmation of the validity of the object (Guru and Damecha, 2014).

1.2 Research Motivation

Security requirements of medical data are mostly derived from legislative rules and strong ethics of security policies that must be followed by professionals and concerned patients (Nyeem et al., 2013). Protection of medical images is not only required for confidentiality purposes but also to detect manipulations of images that may be applied during exchanging and storing. This probability has serious implications on the validity of medical diagnosis and treatment which may, therefore, impact the patients' life. In order to ensure confidentiality, the image data must not be understandable to unauthorised users and this matter can be achieved using encryption techniques. Integrity and authenticity of digital images require additional measures (e.g. digital watermarking) to verify that manipulations of images data can be detected and tracked (Guru and Damecha, 2014).

Despite its efficiency in ensuring the integrity and authenticity of digital data, digital watermarking technology has not been widely adopted in medical imaging. Existing watermarking techniques often suffer from technical and security shortcomings. Evaluation and Validation of the appropriateness of those techniques for medical domains become more challenging. One main reason for these issues is that no standard approach is undertaken for the watermarking application (Nyeem et al., 2013). Particularly:

1. Essential requirements of medical imaging are not well defined and considered when applying digital watermarking to medical images. Specifically: (i) type of embedding: how to modify pixels data, using reversible or irreversible techniques?; (ii) region of embedding: which part of images can be used to encode watermark data? Are all the images pixels can be used to carry the watermark?; and (iii) level of modification: how much data can be encoded to medical images without causing a noticeable distortion to the image? Therefore,

justifying the select of a watermarking technique for medical images applications remains a complicated task.

2. There is no existing digital watermarking approach appropriate for different medical images applications. Conventional irreversible watermarking techniques cause perceptual changes to original images and cannot recover the original images after extracting the encoded data. These techniques remain subjected to non-acceptance by clinicians while the original unmodified images are preferred for medical practices. On the other hand, reversible watermarking methods do not consider the visual quality of watermarked images since the original unmodified images can be retrieved at extraction. This potentially increases ethical and legal concerns about modifying images details, despite their reversible embedding property, because in some urgent cases there could be a need to work on the watermarked image before extracting the encoded data.

3. No standard approach can be found in the literature to assess the distortion level of watermarked images. Physical metrics, such as Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM), are often utilised in previous studies (Chauhan et al., 2019, Zear et al., 2018, Yang et al., 2018, Pan et al., 2018) to evaluate visual differences between original and watermarked images since they are quick and easy to implement. Imperceptibility is a factor of human cognition that needs to be assessed within the human context to determine where the distortion boundary exists. This requires defining a visual assessment approach by involving experts in reading medical images to evaluate the watermarked images to ensure that the property of imperceptibility has been met before releasing the watermarked images into the medical imaging workflow (Zear et al., 2018, Nasr and Martini, 2017).

4. Many approaches have been proposed for utilising digital watermarking technique within medical imaging (Chauhan et al., 2019, Atta-ur-Rahman et al., 2018, He et al., 2017, Roček et al., 2016). However, no study has been conducted to test digital watermarking in an operational PACS workflow. Therefore, proposing an approach for integrating digital watermarking into medical imaging is crucial to verify its applicability in a real application scenario of the medical imaging workflow to ensure that manipulations can be detected and tracked.

All these gaps in the literature can have many serious consequences. A watermarking approach without a robust methodology can have technical flaws in terms of its suitability and validity which may render it inappropriate for its intended use. For example, some studies select to use reversible watermarking techniques for medical imaging, since the original image can be reconstructed at extraction and thus there may not have any ethical or legal consequences (Yang et al., 2018, Qin et al., 2018, Pan et al., 2018). Others may argue that reversible techniques can cause a distortion higher than irreversible watermarking methods, thus encoding watermark into the insignificant region of the image (e.g. background) could perform better (Chauhan et al., 2019, Parah et al., 2017). Consequently, it is significant to investigate the systematic development and evaluation of digital watermarking techniques and their application to medical images to develop an approach to address the identified research gaps.

1.3 Research Questions

In order to ensure the integrity and authenticity of medical images, as well as fulfilling essential requirements of medical imaging workflow, the following research questions require to be considered:

- **Q1:** What are the security risks that may face medical images during routine clinical practices?
- **Q2:** Have the images been manipulated whether intentionally or accidentally and how to detect these manipulations?
- **Q3:** What are security tools that can be used to ensure the integrity and authenticity of medical images?
- **Q4:** What are the fundamental requirements of medical imaging workflow when utilising digital watermarking within medical domains?
- **Q5:** Which digital watermarking techniques can satisfy the particular requirements of medical imaging workflow?
- **Q6:** What are the appropriate criteria for evaluating the suitability of the proposed watermarking technique for medical imaging?

- **Q7:** What is the watermarking modification level that can be applied to medical images so that these images remain acceptable for medical investigations?
- **Q8:** Which approach is appropriate for assessing the perceptual distortion of watermarked medical images?

1.4 Research Aim and Objectives

This research aims to ensure trust in digital medical workflows by enabling robust authenticity and integrity controls within medical images. This work will identify and study the requirements of medical imaging and investigate security threats that may face medical images during regular clinical practices. This contributes to developing approaches and techniques required to verify the reliability of medical images as well as fulfilling the substantial requirements of medical imaging workflow. Specifically, the aim of this research will be accomplished by realising the following research objectives:

- **O1:** Define and investigate essential requirements of medical imaging workflow that are required to be considered when utilising digital watermarking within medical domains.
- **O2:** Develop a visual assessment approach to evaluate the noticeable differences of different watermarked medical images to define the level of modification that can be applied to the images without causing a perceptual distortion.
- **O3:** Develop a new watermarking approach that can confirm integrity and authenticity of medical images, through detecting manipulations, besides achieving the essential requirements of medical imaging.
- **O4:** Propose a framework to integrate the developed watermarking approach into medical imaging to ensure its ability to operate in a real application scenario (e.g. PACS) where medical images are captured, exchanged and archived.
- **O5:** Evaluation of proposed approaches to verify that the aim of this research has been achieved before releasing the watermarked images in medical pipelines.

These interrelated objectives and their relationship to the aim of this study contribute to the answering of the research questions by developing approaches that iteratively refines the understanding of each objective and validates the approaches taken. This will aid in selecting

the appropriate tools and techniques for enhancing trust in medical imaging workflow by ensuring that modifications of medical images can be detected and tracked.

1.5 Research Contributions

In the context of addressing the research questions and objectives, this research offers some innovative contributions and achievements in the area of medical image watermarking. The research contributions and outcomes, which will be elucidated in this thesis, have been presented and published in several respectable conferences and journals. The main contributions of this research are summarised below:

1. A comprehensive literature review (Chapters 3) has been conducted on recent digital watermarking techniques applied to medical images for the purpose of integrity and authentication. This includes an in-depth look at (i) the essential requirements of digital medical imaging workflow when applying digital watermarking to medical images, (ii) the strengths and weaknesses of various watermarking methods, (iii) the purposes and objectives of encoding digital watermarking into medical images, and (iv) the current approaches utilised to evaluate the distortion level of watermarked medical images. The outcomes of this survey have come up with some suggestions and recommendations for the design and evaluation criteria for medical image watermarking. This work was published in Computer Science Review journal (Qasim et al., 2018a).
2. A novel visual assessment approach (Chapter 4) based on relative Visual Grading Analysis (VGA) has been developed to investigate the imperceptibility of digital watermark that was encoded into different brain MR images. This trial sought to define a perceptual boundary, below which change is noticeable, to identify heuristic guidelines for selecting the techniques of watermarking and determining the level of modification that can be applied to encode a known magnitude of payload data in an invisible manner. Three main reasons have prompted to conduct a visual assessment approach: (i) the existed physical measures not accurately estimating the level of imperceptibility between tested images, (ii) no visual measure exists to evaluate the imperceptibility of the digital watermark which is encoded within medical images, and (iii) no reliable approach exists to assess the visual quality of medical images due to the notable variability in using the quality criteria to evaluate the visibility of anatomical structures of medical images (Mraity et al., 2014). Therefore, a visual trial has been conducted, based on standard

criteria derived from European guidelines, for assessing the quality of brain radiographs (Menzel et al., 2000), to investigate the imperceptibility issue which represents the greatest requirement of invisible digital watermarking schemes. No similar study has been conducted before to visually evaluate watermarked images by involving clinicians to evaluate the clarity of anatomical details of the brain MR images based on standard quality criteria. This work was published in *Signal Processing: Image Communication* journal (Qasim et al., 2019b).

3. A new imperceptible and reversible watermarking approach (Chapter 5) based on Difference Expansion (DE) technique has been developed to ensure the integrity and authenticity of medical images by revealing manipulations applied to images during routine medical practices. In conventional reversible watermarking based on DE, location map (location of pixels used for encoding the data) needs to be encoded into the image alongside the watermark to retrieve the encoded data at extraction. This huge additional information minimises the embedding capacity and raises the distortion level of watermarked images. In this research, the watermark data is encoded into ‘smooth’ regions, which are defined as blocks that have the least differences between their pixels’ values, inside the ROI part of medical images to make the deformation less visually noticeable. At extraction, the encoded data can be retrieved without the need for any auxiliary information (e.g. location map) to maximise hiding capacity whilst reducing image distortion. The distortion level of the watermarked images has been evaluated through the conducted visual assessment to ensure the imperceptibility of the proposed technique. This work was presented at ICAC’18 (Qasim et al., 2018b) and also published in *Multimedia Tools and Applications* journal (Qasim et al., 2019c).
4. A theoretical framework (Chapter 6) has been proposed to test the ability of the developed watermarking approach to operating in a real application scenario of medical imaging (e.g. PACS). No similar investigation has been conducted before to test digital watermarking in an operational PACS to address security threats that may face medical images during the routine medical imaging workflow. This work was presented at DESSERT’2019 (Qasim et al., 2019a).
5. A new research methodology has been proposed to develop a watermarking approach to enhance trust in medical domains by applying strong integrity and authenticity controls within medical imaging workflow. The methodology applied has been designed,

implemented, evaluated and validated to present a robust and repeatable methodology for investigating, defining, and validating digital watermarking approaches across the wide range of medical imaging modalities for utilising in future studies.

1.6 Research Methodology

This study concentrates on enhancing trust in digital medical domains by providing strong integrity and authenticity controls within medical imaging workflow to ensure that manipulations of images can be detected and tracked. Adopting an appropriate and successful research methodology helps in the formulation of research questions and objectives in order to achieve them effectively and present a contribution to the research domain. The methodology adopted for this research comprises three main phases; define the requirements, design and implementation, and evaluation and validation of the proposed approaches (Fig. 1.2). These research phases were devised to accomplish the identified objectives of this research.

A. Define the Requirements

The first phase of this study is to identify the medical images, and workflow, requirements to manage techniques and approaches for this study. To achieve this, current digital watermarking techniques, applied to medical images, have been reviewed and investigated to define the particular requirements of the medical imaging workflow. This also sought to identify the strengths and shortcomings of previous studies to identify the research gap and develop appropriate techniques and approaches for this research. Mousavi et al. (2014) presented a comprehensive review of digital watermarking techniques applied to medical images to provide a clear prospect for interested researchers by analysing the strengths and weaknesses of various existing approaches. This article, which has been published in a respectable journal and it is often cited in related research, has stated three essential requirements that must be taken into account when using digital watermarking in medical domains including imperceptibility, reversibility, and reliability. Therefore, this article, with the identified requirements, have been determined as the principal key to this research to propose and develop tools and approaches for this research.

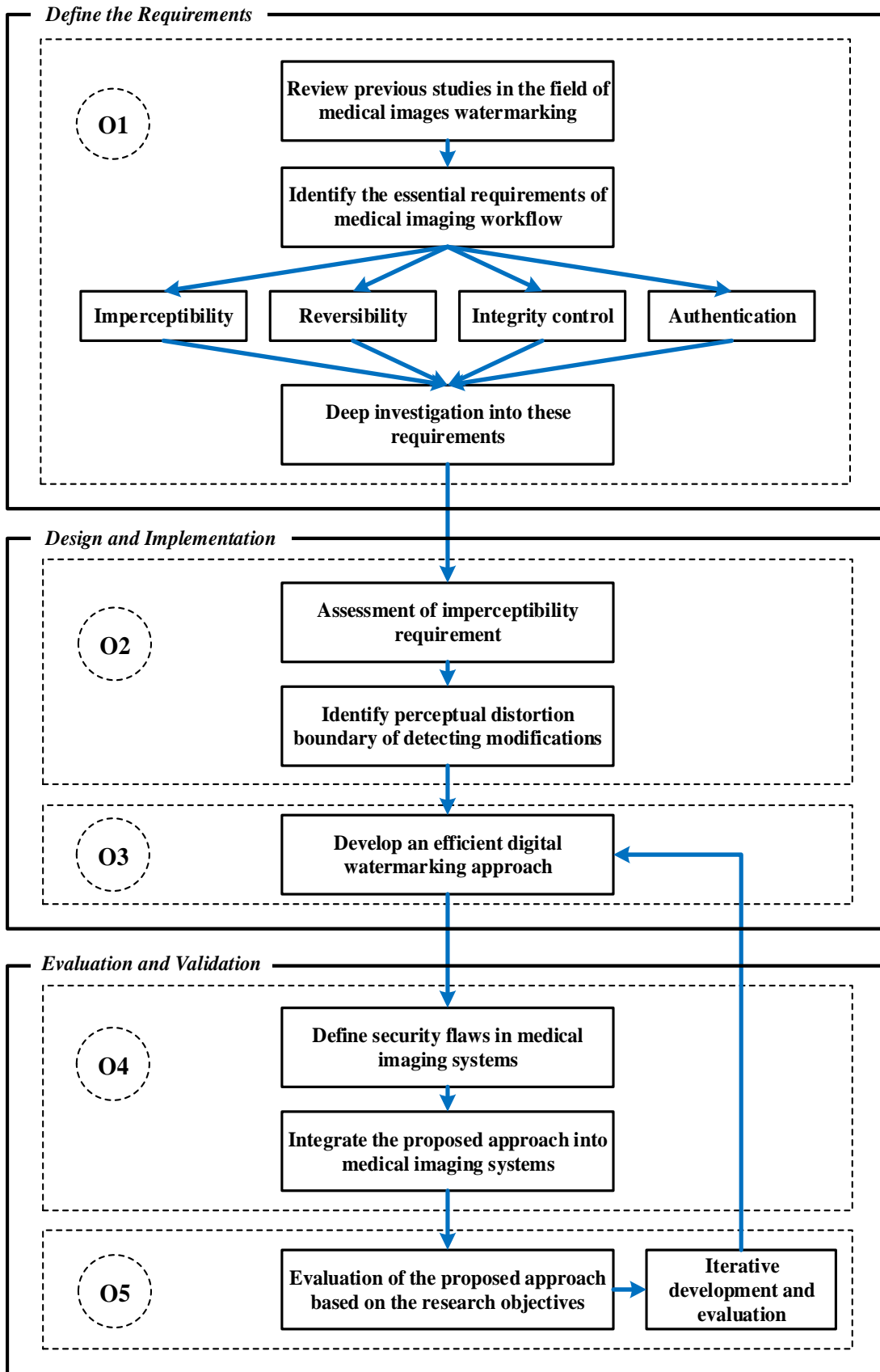


Fig. 1.2: The methodology steps adopted in this research to enhance trust within medical imaging domains. Essential requirements are identified first before developing techniques and approaches to ensure integrity and authenticity of medical images. Iterative evaluation is applied to confirm the achievement of the research objectives.

- **Imperceptibility**

Usually defined as invisibility or fidelity, it represents the highest requirement of invisible watermarking. A digital watermark is called imperceptible if the reference and modified images are perceptually indistinguishable and can be realised by sacrificing either robustness, capacity or both. Therefore, a suitable balance between these three properties might be found depending on the desired application (Ali et al., 2018).

Imperceptibility of digital watermark can be assessed either directly (using physical measures) or indirectly (using visual evaluation approaches). The majority of previous studies utilise physical metrics to evaluate distortion of watermarked images due to their simplicity and ease of implementation (Báth, 2010). Visual evaluation approaches are more relevant in the medical domain than physical measures since visual methods concentrate on how clearly each anatomical structure can be visualised by an observer. However, they reflect observer view and therefore it is highly susceptible to inter-observer variability. Further shortness of visual approaches is that the anatomical structures under assessment need to be pre-identified. No formal guidelines on this exist; it is also likely that these will be highly variable between studies (Mraity et al., 2014). In this research, it became apparent that utilising the visual assessment approaches to evaluate the imperceptibility of the watermarked image would make the outcomes more appropriate to medical domains.

- **Reversibility**

Modification of image data due to encoding a digital watermark may cause a visual degradation to original images, no matter how slight the modification is. In healthcare domains, if an image is manipulated during the medical workflow a collapse in trust regarding the validity and integrity of the images is formed. Any slight change to original images could lead to misdiagnosis with possible life-threatening consequences, or legal, implications which therefore make retrieving the original unmodified images from the watermarked images is necessary after extracting the encoded data successfully (Qin et al., 2018). Reversible watermarking techniques can fulfil this requirement by employing methods that can ensure the extraction of the watermark along with precisely retrieving the complete reference image. Many reversible watermarking approaches stated in the literature to serve various applications in medical domains. A deep investigation into various reversible watermarking techniques was carried out in this work to select appropriate

methods and approaches for encoding the watermark data into medical images to achieve the objectives of this research.

- **Reliability**

It may be decomposed into two aspects; *integrity control* and *authentication*. Integrity control indicates the ability to ensure that the information has not been altered without authorisation and authentication refers to verify that the data belongs to the right patient and was received from the correct source. Images integrity can typically be verified by encoding Digital Signature (DS) or Message Authentication Code (MAC) of the images. Images authenticity can be achieved by hiding the Electronic Patient Record (EPR) or the complete metadata of DICOM images or some of its fields to confirm that the images belong to the right patient. Selecting the appropriate watermark for accomplishing the aim of the application depends on the amount of data that can be concealed in an undetectable manner. At extraction, the integrity and authenticity of medical images can be verified by extracting the concealed data exactly. Manipulations of watermarked images must distort the encoded data resulting in a mismatch between the original and extracted watermarks. Therefore, fragile watermarking techniques are preferred to reveal the slight modifications that may occur in medical images.

B. Design and Implementation

To identify the imperceptibility of distortion boundary, both assessment methods (physical and visual) were adopted to measure the distortion level of watermarked images. Three different reversible watermarking techniques, based on DE method, were used to encode various amount of data into eight different medical images, provided by the MRI unit of Al-Kadhimiya Teaching Hospital/Iraq (Hasan and Meziane, 2016, Hasan et al., 2016a), to produce a set of watermarked images with various degradation levels. Standard PSNR and SSIM metrics were utilised to physically measure the distortion level between the original and watermarked images. A visual assessment, based on relative VGA, was implemented to visually evaluate the watermarked images. This assessment method was adopted due to its ability to discover and evaluate the slight changes between images being tested. Five qualified radiographers, who are experienced in diagnostic radiography, were invited to estimate the differences in the anatomical structures of the tested images based on eight standard criteria dedicated for assessing the visual anatomical details of brain radiographs

(Menzel et al., 2000) using a five-point Likert scale, ranging from strongly agree to strongly disagree, to grade the criteria items. Relating the scores of the observers to objective measures for image fidelity was then undertaken to identify the imperceptibility boundary in which the observers cannot realise any differences between the original and watermarked images. This contributed to defining quantitative criteria to guide the selection of a watermarking technique and enabled an objective post modification evaluation of the watermarked image to verify that the requirement of imperceptibility was met.

A fragile and reversible watermarking approach, based on DE technique, was then developed to encode both the DS of the whole images and the essential metadata fields of DICOM images into the medical images to ensure the integrity and authenticity of images raw data as well as the header data. The proposed watermarking approach was applied to twenty-five brain MR images in DICOM format (16bpp, 512×512 pixels). Sixteen images were provided by the MRI unit of Al-Kadhimiya Teaching Hospital/Iraq (Hasan and Meziane, 2016, Hasan et al., 2016a) and nine images were selected from a publicly available and standardised medical images dataset downloaded from The Cancer Imaging Archive (TCIA) (Clark et al., 2013).

C. Evaluation and Validation

The performance of the approach was evaluated based on the four identified essential requirements of medical image watermarking; imperceptibility, reversibility, capacity, and robustness (Qasim et al., 2018a, Mousavi et al., 2014) to verify its efficiency and applicability. Imperceptibility between the original and watermarked images was evaluated using common objective measurements and this was also assessed through conducting a visual trial to identify a perceptual boundary, below which change is detectable. Reversibility of the approach was evaluated at extraction to verify the ability to recover the concealed data as well as the original unmodified images. Capacity of the approach was also evaluated to verify that the proposed technique can carry the watermark data which is required for ensuring the integrity and authenticity of images. To evaluate the fragility of the proposed approach, various image processing operations were applied to the watermarked images simulating image data manipulations. Iterative development and evaluation were then undertaken to the proposed approach to verify that the objectives of this research were realised before releasing the watermarked images in medical imaging workflow.

After the proposed approach has been developed and evaluated, it is necessary to validate the ability of the approach to operate in medical imaging systems or PACS workflow. Validation of digital watermarking is a challenging issue and has not been widely investigated in the literature. To accomplish this, security threats that may face medical images during acquisition, exchanging, and archiving were defined and investigated first to verify the ability of the approach to tackle these security threats and provide a secure system for medical environments.

1.7 Thesis Organisation

The remainder of this thesis is organised into the following chapters which establish the context for the research (Chapters 2 and 3), present the main contributions (Chapters 4-6), review and evaluate the findings of the research against the aim, objectives and research questions (Chapter 7), and conclude the thesis with a summary of the original contributions and some suggestions for future research (Chapter 8).

- **Chapter 2** presents a technical background for the proposed research in this thesis to clarify the basic concepts, requirements and evaluation methods of digital watermarking. This would aid in the selection of techniques and approaches through which the identified research questions can be answered to realise the objectives of this study.
- **Chapter 3** undertakes a literature review of the state of the art in the related work in the field of digital watermarking utilised in medical domains for the purpose of ensuring the integrity and authenticity of medical images. This seeks to identify the particular requirements of medical imaging workflow when applying digital watermarking to medical images and define the shortcomings of the existing techniques to direct the research route and provide a basis for the assessment of the proposed approaches.
- **Chapter 4** demonstrates the work undertaken to conduct the visual evaluation to assess the brain MR images which were watermarked by varying methods and magnitude of image/pixel modification. This work contributes to defining the range of modifications within which changes to the image pixels are unnoticeable to the viewers to identify the level of modification that can be applied to hide a known volume of data in an imperceptible manner.

- **Chapter 5** presents a new reversible and imperceptible watermarking scheme developed to enhance trust in medical imaging workflow by revealing manipulations within brain MR images. Performance of the proposed approach is evaluated, validated and compared with existing watermarking techniques to ensure its suitability and capacity to operate within medical domains.
- **Chapter 6** deeply analyses the security flaws in medical imaging systems to identify threats that may face images during routine medical practices. This work aids in designing a theoretical framework to integrate the proposed watermarking approach into medical imaging workflow to address the identified security threats and to verify the ability of the approach to work in a real application scenario (e.g. PACS) where medical images are captured, exchanged, viewed and archived.
- **Chapter 7** discusses the techniques and approaches developed to achieve the aim of this study and presents an objective evaluation of the research undertaken to evaluate and validate the proposed approaches based on the determined research objectives.
- **Chapter 8** concludes the thesis with a summary of the main contributions and shortcomings of the research with some recommendations for future studies.

CHAPTER TWO

Technical Background

Digital watermarking has already shown its preference over a range of techniques due to having a number of attractive properties such as the ability to hiding the information in an imperceptible manner and keeping visual semantics of digital images. This chapter presents a background on the role of watermarking in protecting digital objects, specifically medical images, and relate this to the research objectives. The chapter is divided into four main parts; the basic principles of medical imaging modalities and formats, the concept of digital watermarking and its requirements and classifications, the existed methods for evaluating the distortion level of watermarked images, and the physical metrics used to measure the validity of the extracted watermark. This is significant to identify the appropriate evaluation criteria for the selection of tools and techniques through which the objectives of this research can be achieved.

2.1 Introduction

Medical imaging platforms generate and manage digital images across many modalities including X-ray, Ultrasound, CT, MRI, etc. Typically, the images are managed and exchanged within the medical pipeline based on the DICOM format. These medical images usually comprise critical clinical data which makes any manipulation on images during using is unbearable. Therefore, developing a highly reliable management system for medical images is substantial (Fontani et al., 2010).

The security of medical data, constructed from strict ethics and legislative precepts, gives rights to the patient and responsibilities to the health specialists. This requires three essential properties: confidentiality, reliability and availability (Nyeem et al., 2013).

- **Confidentiality** indicates that only the authorised users, under identified conditions, have access to the data.
- **Reliability** is based on two aspects; integrity and authentication. Integrity ensures that the information has not been manipulated in an unauthorised manner. Authentication confirms that the information refers to the right patient and was released from the correct source.

- **Availability** points out the ability of an information system to be accessed, as required by authorised users, in regular situations.

Security hazards of medical images can vary from accidental operations to malicious manipulations that might occur on images during exchanging within a hospital or when transferred to another healthcare provider. Matching the header of the image with the raw image data needs to be always assured. In addition, detecting the intentional alterations, which aim to replace or modify parts of the image, is necessary (Al-Haj, 2015). Digital watermarking has the ability to enhance the security of medical imaging workflow by ensuring the integrity and authenticity of digital medical images data. The general requirements of digital watermarking are the invisibility of the encoded watermark, the embedding capacity of the watermarking approach, the secrecy to unauthorised persons, and the ability of the technique to survive against different image processing operations. Further requirements need to be considered and investigated when implementing digital watermarking in medical domains in addition to the general requirements of digital watermarking (Mousavi et al., 2014).

2.2 Medical Imaging System

Medical imaging denotes the techniques employed to generate images of the interior of a body for clinical analysis and medical intervention. Acquisition devices capture X-ray, Ultrasound, nuclear or magnetic field signals, and then convert those data into images by using reconstruction algorithms to produce different medical image modalities (Toennies, 2012). Typically, these modalities are managed within a digital medical workflow based on the DICOM standard (Pianyk, 2009). Medical imaging modalities comprise various scanning methods to visualise the human body for diagnostic and treatment targets. These modalities are very beneficial for the follow-up of patients regarding the progress of the disease situation, which has already been diagnosed, and/or is subjecting to a treatment program. Several medical image modalities can be found in most healthcare provider units to help in providing the proper diagnoses (Stocksley and Phillips, 2005).

2.2.1 Magnetic Resonance Imaging

MRI is a major innovation in medical imaging technology and has been used since the beginning of the 1980s. In comparison with other medical imaging technologies like X-ray and CT, MRI is harmless to the human body due to using a strong magnetic field and radio

waves instead of radiation to build cross-sectional soft tissue visualisation for all interior organs of the human body and blood vessels. The majority of studies on medical imaging utilise MRI because it offers images with high-resolution, excellent contrast for the soft tissue and high Signal to Noise Ratio (SNR) (Hasan and Meziane, 2016). The MRI technique is based on the interaction between an external magnetic field and the protons of hydrogen possessed by the body. Therefore, the MRI is especially appropriate for the imaging of biological tissue like the brain and eyes rather than bones which do not contain many hydrogen atoms (Petrou, 2010).

2.2.2 Digital Imaging and Communications in Medicine

In 1983, a joint committee was created by American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA) to develop a standard for encoding, transmitting and managing medical images generated from various medical equipment and manufacturers (Larobina and Murino, 2014). The first version, which is called ‘ACR/NEMA Standard Version 1.0’, was released in 1985. In 1988, revision for the first version was undertaken to create the second version ‘version 2.0’ by including new material to the first form. Both versions ‘1.0 and 2.0’ support point-to-point connection which represents a problem in modern communication networks that do not use completely dedicated channels. Consequently, a new version named ‘DICOM Version 3.0’ was released in 1993 which uses the networked environment as an alternative to point-to-point connections for imaging system transmission. Since its release in 1993, the DICOM standard has been developed by workgroups, mostly every year, to satisfy practically any medical department (Mustra et al., 2008). Nowadays, DICOM is the backbone of all medical imaging branches and represents the industry standard for the creation of medical images, though there are variations of it (Larobina and Murino, 2014). DICOM standard provides many benefits, such as medical images can be captured and exchanged more quickly, and clinicians can give decisions and produce patients’ reports faster (Stanescu et al., 2006).

In addition to image data, DICOM contains an important structure located in the header of the image for describing it called ‘metadata’. The metadata includes information about the image matrix, object’s description and the procedure performed to create the image (Larobina and Murino, 2014). The header also contains the Information Object Definitions (IODs) which represents the most important components of metadata. IODs are tables of attributes that consist of the time of taking the image, diagnosis result and basic patient details such as

the name, ID number, age, gender, weight and height. For these characteristics, the DICOM header differs in size, modality-dependent and it lets the image to be self-descriptive (Mustra et al., 2008).

Although DICOM supports different data types, including floats, to store metadata, it can only save pixel values as signed and unsigned integers and cannot recently store data in floating point. DICOM allows another document with a different format to be encapsulated in a DICOM file through the compression mechanism. Compression techniques supported by DICOM involves Run Length Encoding (RLE), Joint Photographic Experts Group (JPEG), JPEG-2000, JPEG Lossless (JPEG-LS), Moving Picture Experts Group (MPEG2/MPEG4) and Deflated. The JPEG eXtended Range (JPEG-XR) compression scheme has been recently suggested to be accepted by DICOM format (Larobina and Murino, 2014). DICOM file consists of the following structure (Fig. 2.1) (Varma, 2012):

- A preface of 128 bytes.
- A prefix of 4 bytes for storing 'D', 'I', 'C', 'M' letters to identify the file format.
- The data set to save the metadata fields.
- Pixels data to shape the image contained within the DICOM file.

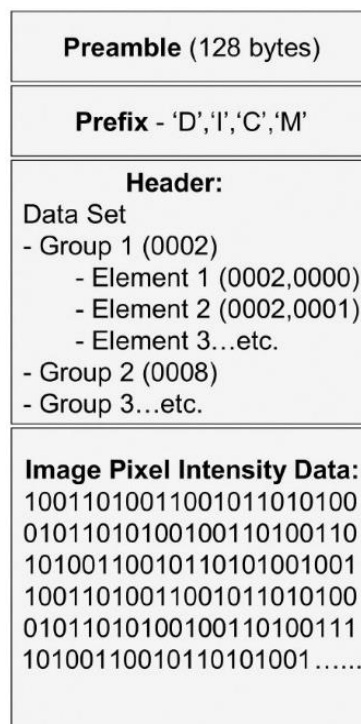


Fig. 2.1: The structure of DICOM images. Consists of four parts: a preface of 128 bytes, (D, I, C, M) letters to define the file format, a header to store the metadata fields and pixels data to shape the image (Varma, 2012).

2.3 Conventional Security Measures

In this section, conventional security measures are studied and investigated to ensure the appropriateness of digital watermarking as a complementary tool for protecting digital medical images. Various security tools are being utilised to protect the medical images and data. However, these security measures are considered to have limitations in protecting medical images and required to be properly addressed for enhanced security (Mousavi et al., 2014, Nyeem et al., 2013, Coatrieux et al., 2001).

2.3.1 Data Encryption

To protect the confidentiality and privacy of health information and medical records of patients, encryption has been a commonly accepted technology in medical domains. Encryption is the process of transmitting data (plain-text) in an unreadable form (cipher-text) using a particular algorithm to make it un-understandable to unauthorised parties (Haouzia and Noumeir, 2008). There are two types of encryption: symmetric encryption (private or secret key) such as Data Encryption Standard (DES), Rivest Cipher (RC), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), etc., and asymmetric encryption (public-key) such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), Diffie-Hellman, etc. (Kanso and Ghebleh, 2015, Yassein et al., 2017).

The robustness of the symmetric encryption technique largely depends on the size of the key and on keeping it secret. In general, the larger the key, the more secure the encryption technique. Symmetric encryption is relatively quick and easy to understand. However, the main shortcoming of this type of encryption is that the key or algorithm used at encryption need to be shared making it not well suitable for open and unsecured communications. In addition, the symmetric key does not provide a process for non-repudiation, which defined as the ability to prevent individuals or entities from denying that a message was transmitted or received or that file was accessed or manipulated, when indeed it was. On the other hand, asymmetric encryption employs two keys: a private key (use at encryption) and a public key (used at decryption). Unlike symmetric scheme, the public key provides a protected communication over an open network since no secret key need to be shared and a means of authentication and non-repudiation are provided with the help of digital certificate. Asymmetric encryption is relatively slower and more complicated and requires a trusted

certificate authority which issues a digital certificate to certify the ownership of the public key by the named subject of the certificate (Yassein et al., 2017).

2.3.2 Cryptographic Hash Functions

A cryptographic hash function is a deterministic operation which returns a fixed-size of bits (hash value) for an arbitrary block of data, such that any manipulation to this data will change the hash value (Paar and Pelzl, 2009). The data to be hashed is often called the message, and the hashes are occasionally defined as the message digest or simply digest. These techniques offer three main features: (i) it is simple to calculate the hash value for any given message; (ii) it is impossible to find two different messages having the same hash value; and (iii) it is impossible to alter a message without modifying the hash value. These properties make them suitable for integrity verification applications and other purposes such as indexing, fingerprinting, detecting duplicate data, and data corruption, etc. (Katz et al., 2018). The majority of existing cryptographic hash function methods are vulnerable to accidental operations, such that a 1-bit modification to the data will change the hash value dramatically. This makes them appropriate for critical applications such as medical and legal applications. However, this severely limits their practical utility in some applications like robust content authentication of digital images in which authorised modifications are allowed (Paar and Pelzl, 2009).

2.3.3 Perceptual Hash Functions

Perceptual hash functions, also defined as robust perceptual hash functions, or simply, perceptual hashing, are designated hash functions for multimedia contents which returns a fixed-size binary vector (perceptual hash or robust hash) for a given digital image besides generating a content descriptor for the image. This hash is required to be invariant under changes to the image that are perceptually insignificant whereas, on perceptually distinct inputs, the hash needs to be approximately independent and hence different with high probability (Nyeem et al., 2013). An efficient perceptual hash function should have several features: (i) robust: modifications that do not alter the perceptual information should not modify the hash value; (ii) unique: perceptually different inputs should have fully different hash values; and (iii) secure: it should be very difficult to find perceptually different inputs with same hash values (Nyeem et al., 2013). Unlike getting a completely different hash value when changing a single bit in the input of the cryptographic hash function, perceptual hashes are expected to be different only with the modifications in the perceptual content of the input.

For example, for a perceptual hash function, the hash value of an image and its JPEG compressed version (with acceptable image quality) should be the same, since they have no noticeable variation, although their bit-string representation is totally different. Generally, perceptual hashing comprises feature extraction, randomisation that introduces irreversibility, and compression followed by quantisation and binary encoding to generate a binary hash output. Most randomisation techniques are linear, which allows using the input/hash pairs to restore a secret key. Moreover, the quantisation and encoding phases need the defining and storing of proper quantisation thresholds, which introduces further security limitations (Voloshynovskiy et al., 2009).

2.3.4 File Header

Appending metadata as a header with the data block to medical images (e.g. DICOM images) is an additional security measure. Since metadata includes a patient's ID, image size, last modified time, etc., the size of the header varies based on how much information is stored in the header. Existing metadata techniques not providing a secure relationship between the metadata and medical image. For example, for the images with a plain-text header, the main threat is the breach of the access rights and the manipulation of images by the unauthorised users. Hence, breaking confidentiality means that the integrity and authenticity of the images cannot be ensured anymore. Furthermore, for an encrypted header, the bit error sensitivity may increase complexity in managing medical images and loss or disclosure of header data. It is, therefore, easy to destroy, modify, or otherwise disconnect the metadata rendering the image unreliable (Coatrieux et al., 2000).

To summarise the above discussion, conventional security measures can be beneficial and suitable for transmission and distribution of digital images over networks. However, they are limited in ensuring the integrity of digital images and detection and localisation of any possible manipulation. Therefore, new measures are needed to be utilised for the improved security of medical images. Digital watermarking can be considered as a complementary tool to facilitate medical information security protection (Thilagavathi et al., 2015, Mousavi et al., 2014), which still requires an appropriate justification of watermarking applicability for medical images.

2.4 Digital watermarking

Digital watermarking is the hiding of information within the digital object. The embedded data can then be detected/extracted to confirm the validity of the object. It can be used along with some existing security tools, such as encryption, cryptographic hash function, digital signature, perceptual hashing, etc., for developing security properties (Loan et al., 2018, Liu et al., 2018, Brar and Kaur, 2015). The basic model of the digital watermarking scheme consists of three components (Fig. 2.2); watermark generation, watermark embedding, and watermark extraction (Nyeem et al., 2013).

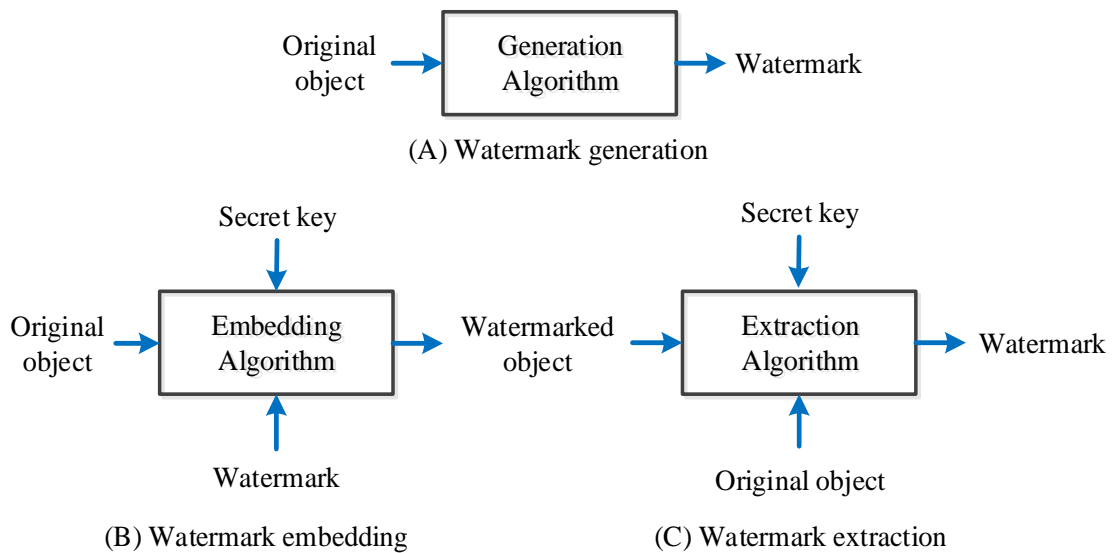


Fig. 2.2: Main components of digital watermarking schemes: **A)** Watermark generation, **B)** Watermark embedding, and **C)** Watermark extraction. The generated watermark is encoded into the original object using an embedding algorithm and a secret key. At extraction, the encoded data is retrieved by reversing the hiding algorithm and using the secret key and/or the original object.

- **Watermark Generation**

In this phase, a suitable watermark is created according to the purpose of the watermarking approach. In simple applications, such as ownership verification, the watermark data can be a text or an image. In developed applications, the watermark may have special characteristics based on the required purpose. For example, in medical applications, the watermark may need information about patients or features of medical images to verify the authenticity and integrity of the images.

- **Watermark Embedding**

The watermarked data is generated by encoding the watermark into the original object using a certain algorithm and a secret key. Various techniques can be utilised to encode the watermark into digital data. Selecting a suitable watermarking technique depends on the purpose of the application.

- **Watermark Extraction**

In this stage, the encoded data is detected/extracted from the watermarked object by reversing the hiding algorithm that was used to encode the watermark. The secret key and/or the original object are required for retrieving the embedded data successfully.

2.4.1 Digital Watermarking Classifications

Digital watermarking schemes can be classified into many groups in various ways (Fig. 2.3), including object type, embedding domain, perceptibility and reversibility (Mousavi et al., 2014). Based on the embedding techniques, watermarking systems can be categorised into spatial and transform domain (Zain and Clarke, 2007).

Watermarking methods can be divided according to human perception into visible, invisible, and dual watermarking techniques. Popular examples of visible watermarks are the sealing and logos, which are placed on the images, videos and the corners of TV channels for content protection and ownership verification. Invisible watermarks are hidden in such a way that they cannot be seen, but they can be extracted/detected by utilising the correct algorithm to serve various applications like authentication, integrity control and ownership verification of digital files. In some application, visible and invisible watermarks can be applied together. This technique is called dual watermarking, and in this situation, the invisible watermark is considered as a backup for the visible one (Qasim et al., 2018a).

Invisible watermarking approaches can be further divided, based on their robustness, into four categories: robust, fragile, semi-fragile and hybrid techniques (Mousavi et al., 2014). Robust watermarking, which is typically used for copyright protection, copy control, fingerprinting, and broadcast monitoring, should be able to survive against a wide range of operations, while the fragile watermarking methods are intolerable to the smallest modifications. Fragile techniques are designed with the goal of verifying the authentication and integrity of multimedia contents. The semi-fragile method is intermediate in robustness,

in such that it is robust against authorised operations and fragile with unauthorised operations. This watermarking method is also used for authentication and integrity purposes (Jain and Rajawat, 2012). Finally, the hybrid approach is a combination of fragile and robust methods to achieve the authenticity, integrity and ownership protection simultaneously (Mousavi et al., 2014).

In addition to the previous classifications, reversible watermarking, also defined as invertible or lossless watermarking, is another significant feature of digital watermarking. Compared to the conventional watermarking techniques, reversible methods can restore both the embedded watermark and the original unmodified object exactly. This feature is a crucial requirement for many fields such as medical, military and law-enforcement applications (Thilagavathi et al., 2015).

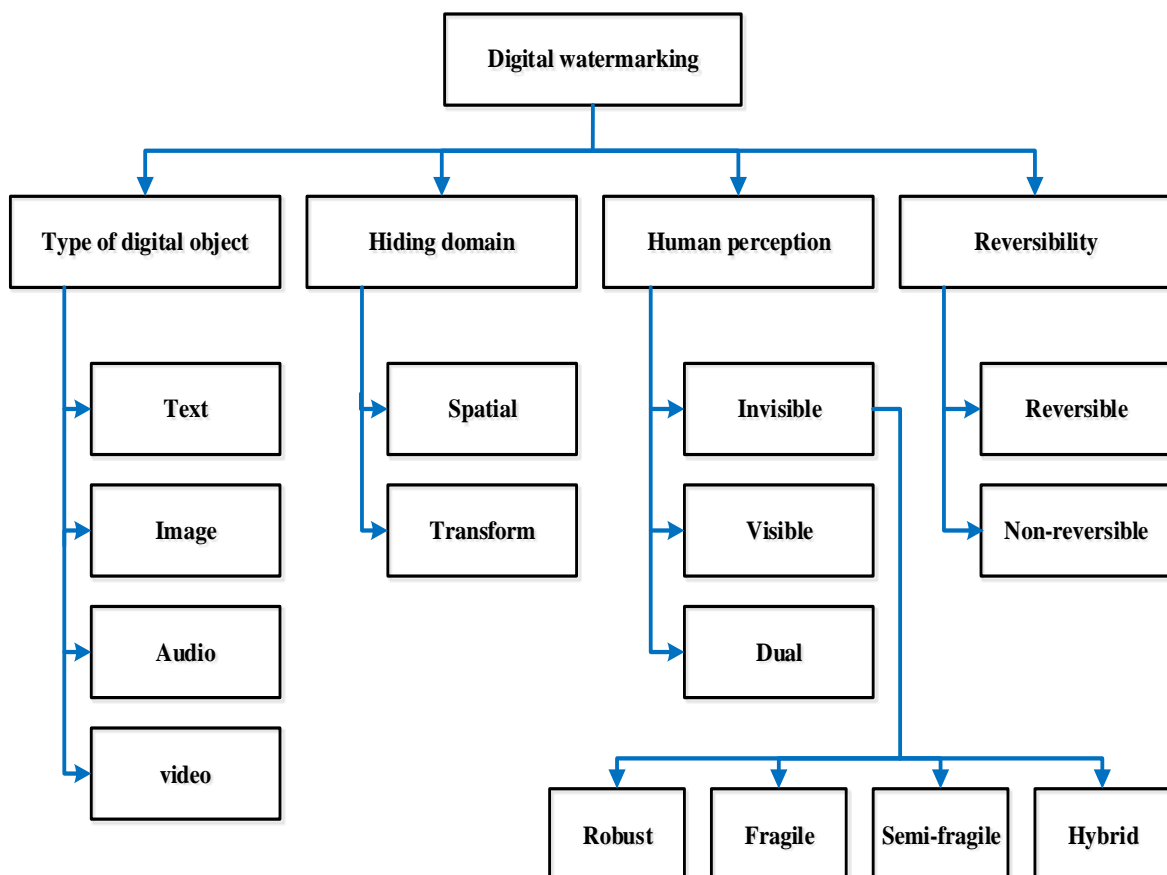


Fig. 2.3: Classification of digital watermarking based on four various criteria. Including object type, domains and techniques of hiding the watermark, visibility of the watermark to human perception and the possibility of retrieving the original object after extracting the encoded watermark. Invisible watermarks are further divided based on their robustness against a range of operations.

2.4.2 Digital Watermarking Requirements

Essential requirements for designing a digital watermarking can be considered as properties or attributes. Requirements of digital watermarking vary and result in various design issues depending on the desired application and purpose. These requirements need to be taken into account while designing a digital watermarking system (Mousavi et al., 2014).

2.4.2.1 Fidelity

It represents the most important requirement of watermarking systems and can be defined as the similarity amount between original and modified images. In invisible watermarking applications, embedded data must be visually imperceptible, as much as possible, to human perception even the incidence of slight distortions in original cover images (Fung et al., 2011).

2.4.2.2 Robustness

This requirement signifies the ability of the implemented watermarking technique to resistant to different image processing operations/attacks which aim to frustrate the encoded watermark from fulfilling its intended purpose. The wide class of existing operations can be categorised into four groups; removal, geometric, protocol and cryptographic attacks (Ridzoň et al., 2004, Voloshynovskiy et al., 2001). Implemented watermarking algorithms cannot survive with all types of operations. Some of the algorithms are strong against many attacks, however, they fail to survive with other stronger operations. Moreover, not all applications require a robust watermarking technique. In some applications, it is needed to be fragile to detect manipulations that may be applied to digital images (Durvey and Satyarthi, 2014).

2.4.2.3 Data Payload (Capacity)

This property refers to the number of bits that can be concealed as a watermark into the cover image without impacting the visual image quality. The required embedding capacity depends on the purpose of the watermarking approach and different watermarking applications require various capacity requirements (Arya et al., 2015). This requirement is determined by two other properties; imperceptibility and robustness (Fig. 2.4). A high payload capacity can be achieved by sacrificing either robustness, imperceptibility or both. Therefore, a suitable trade-off might be found depending on the desired application (Durvey and Satyarthi, 2014).

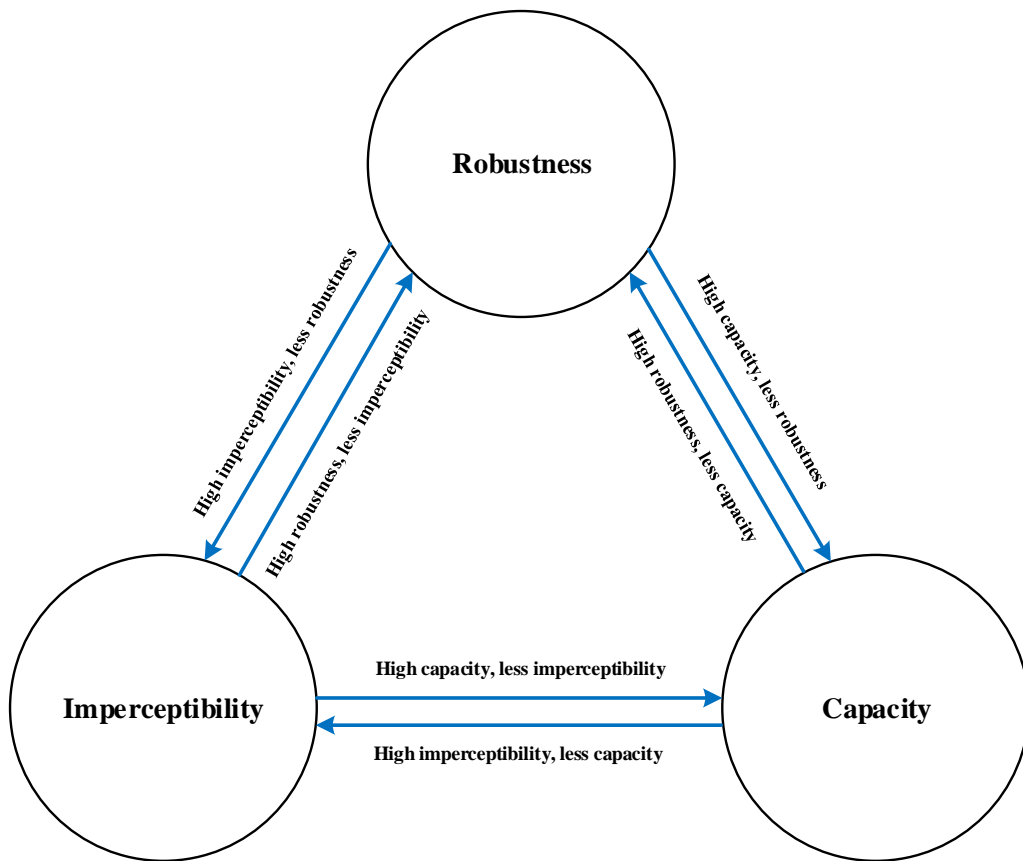


Fig. 2.4: The trade-off triangle between the three essential watermarking properties. A high capacity can be realised by reducing either imperceptibility, robustness or both. The required watermarking application determines an appropriate balance between these properties (Durvey and Satyarthi, 2014).

2.4.2.4 Security

Security is a significant factor in digital watermarking systems. A watermarking approach is considered as secure if and only if unauthorised users cannot detect or extract the encoded data without having full information about the algorithm that has been used to embed the watermark. A secret key need to be utilised for the encoding and extraction processes in case the issue of security is crucial (Abdullatif et al., 2013).

2.4.2.5 Computational Complexity

This feature is defined as the amount of time taken by the watermarking algorithm for embedding and extracting the data. More computational complexity is required for integrity and authenticity applications to deliver high-security. On the other hand, real-time applications require both fast and efficient algorithms (Patel and Bhatt, 2015).

2.5 Evaluation of Watermarked Image Quality

In this research, the term ‘image quality’ refers to the rate of imperceptibility/fidelity between an original image and its watermarked version. The measurement of image quality is vital for various image processing purposes. In general, image quality scales fulfil three kinds of applications (Wang et al., 2002):

- To examine and monitor the image quality in quality control systems.
- To improve algorithms and parameter setting of image processing systems.
- As an indicator for selecting the applicable image processing algorithms.

Image quality can be evaluated either directly (e.g. physical measurements) or indirectly (e.g. visual approaches). Physical metrics are easy and commonly used in assessing image quality. However, their efficacy in achieving a measurement which is relevant to the observer judgment is not yet confirmed as they not considering all the clinical characteristics that are related to medical investigations (Båth, 2010). Therefore, they should be accompanied by observers' attitudes to ensure their efficiency and validity (McCollough et al., 2006). Visual assessments are complicated, expensive, time-consuming, and require specific equipment and conditions, which make them ineffective for real-time applications (Mohammadi et al., 2014).

2.5.1 Physical Assessment

The goal of this approach is to design mathematical models that are able to autonomously evaluate the quality of a modified image against its unmodified version. The similarity between the reference and modified images can be measured using the following most commonly adopted metrics (Nasr and Martini, 2017). In all of the used equations, $N \times M$ is the dimension of the image, and I_{ref} and I_{test} represent the reference and test images respectively.

2.5.1.1 Peak Signal to Noise Ratio

It is a basic measure used to estimate the distortion amount between original and watermarked images (Eq. 2.1). The PSNR approaches infinity as the MSE approaches 0; this shows that a higher PSNR value indicates lower distortion and higher image quality. At the other end of the scale, a small value of the PSNR implies high numerical differences between the tested images (Hore and Ziou, 2010).

$$PSNR(I_{ref}, I_{tst}) = 10 \times \log_{10} \frac{MAX_I^2}{MSE} \quad (2.1)$$

Where MAX_I represents the highest possible pixel value of the input images and MSE is the Mean Squared Error between the original and watermarked images (Eq. 2.2) (Qasim et al., 2018a).

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_{ref}(i, j) - I_{tst}(i, j))^2 \quad (2.2)$$

2.5.1.2 Structural Similarity Index

It is a Human Visual System (HVS) based measures to quantify the degradation in the structural information between two images (Eq. 2.3). The SSIM approach compares the similarity between three factors: luminance, contrast, and structure (Hore and Ziou, 2010).

$$SSIM(I_{ref}, I_{tst}) = L(I_{ref}, I_{tst}) C(I_{ref}, I_{tst}) S(I_{ref}, I_{tst}) \quad (2.3)$$

Where:

$$\begin{aligned} L(I_{ref}, I_{tst}) &= \frac{2\mu_{I_{ref}}\mu_{I_{tst}} + C1}{\mu_{I_{ref}}^2 + \mu_{I_{tst}}^2 + C1} \\ C(I_{ref}, I_{tst}) &= \frac{2\sigma_{I_{ref}}\sigma_{I_{tst}} + C2}{\sigma_{I_{ref}}^2 + \sigma_{I_{tst}}^2 + C2} \\ S(I_{ref}, I_{tst}) &= \frac{\sigma_{I_{ref} I_{tst}} + C3}{\sigma_{I_{ref}}\sigma_{I_{tst}} + C3} \end{aligned} \quad (2.4)$$

The first term in (Eq. 2.4) is the luminance comparison function which measures the closeness of the luminance of the two images' mean luminance ($\mu_{I_{ref}}$ and $\mu_{I_{tst}}$). This factor is maximal and equal to 1 only if $\mu_{I_{ref}} = \mu_{I_{tst}}$. The second term is the contrast comparison function which measures the closeness of the contrast of the two images. Here the contrast is measured by the standard deviation $\sigma_{I_{ref}}$ and $\sigma_{I_{tst}}$. This term is maximal and equal to 1 only if $\sigma_{I_{ref}} = \sigma_{I_{tst}}$. The third term is the structure comparison function which measures the correlation coefficient between the two images I_{ref} and I_{tst} . The $\sigma_{I_{ref} I_{tst}}$ is the covariance between I_{ref} and I_{tst} . The positive values of the SSIM index are in [0,1]. A value of 0 means

no correlation between the tested images, and 1 means that the images are equal. The positive constants $C1$, $C2$ and $C3$ are used to avoid a null denominator (Hore and Ziou, 2010).

2.5.1.3 Root Mean Squared Error

Root Mean Squared Error (RMSE) is the rooted value of the MSE and is mainly utilised to measure the reversibility of the watermarking technique (Eq. 2.5). RMSE value close to 0 indicates lower image distortion (Selvam et al., 2017).

$$RMSE = \sqrt[2]{MSE} \quad (2.5)$$

2.5.1.4 Image Fidelity

Image Fidelity (IF) metric measures the similarity between the original and watermarked images (Eq. 2.6). The value of IF equal to 1 indicates that the two images are identical (Selvam et al., 2017).

$$IF = 1 - \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_{ref}(i,j) - I_{tst}(i,j))^2}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I_{ref}(i,j))^2} \quad (2.6)$$

2.5.2 Visual Assessment

Visual testing methods represent the most clinically recognised approach for evaluating the visual quality of images since human observers are the definitive users in most multimedia applications. In this measurement, a group of experts are required to give their subjective response about the quality of each image (Mohammadi et al., 2014). When adopting this approach, the variation and average of the outcomes from various observers are considered to determine high reliability in the evaluation results (Månsson, 2000). Two main visual techniques are employed to evaluate the quality of the images and the observer's performance; Receiver Operating Characteristic (ROC) and Visual Grading Analysis (VGA).

2.5.2.1 Receiver Operating Characteristic

The main task of an observer in medical imaging is to identify whether a displayed patient's image presents proof of pathology, or not. Therefore, developing a system to measure the observers' performance about the diagnosis quality is necessary (Båth, 2010). ROC approach is often employed in radiology to evaluate the observers' performance against known diagnostic images. This method, which is constructed from the Signal Detection Theory

(SDT), assesses whether an observer can identify a low contrast signal (artefact) in a noisy environment (digital image). The clinical equivalent to this is the distinguishing of the irregular case, from a series of regular cases (Månsson, 2000). Accordingly, an observer is required to identify features within the image and the performance of the observer's group can then be measured by counting the number of right responses (Båth, 2010).

Two main approaches can be used for performing ROC analysis. In the first approach, an observer is shown one image at a time and is asked to reply 'yes' if the signal is present or 'no' if the signal is absent. In this method, the observer is required to apply one decision criterion for a large number of cases; true and false positive response fractions are collected to create one data point on the ROC curve. This process is then repeated for other decision criteria, against the same image set. The ROC is defined by a plot of the variation of the true positive and false positive responses fractions. The second approach employs a rating scale to assess each image. The rating scale contains several levels of confidence regarding the presence or absence of the signal in the displayed image to enable the observer to use a number of decision criteria concurrently. To analyse the outcomes, the ratios of true and false positive responses for each decision criterion are defined, and the boundary between each of these ratings is evaluated to determine whether it matches a particular decision criterion (Burgess, 1995).

ROC analysis has a serious limitation in that it is strongly reliant on the ubiquity of the disease. Moreover, the images must be classified into two categories (normal and abnormal), indicating that a significant number of images with subtle pathology are needed. The ROC approach does not serve adequately for many lesions within the same image, and the localisation of lesions is not considered, therefore an image may be diagnosed as abnormal for the incorrect reason (Zarb et al., 2010, Båth, 2010). To overcome these weaknesses in the ROC methodology, several measures have been developed to enhance its efficiency. These measures involved the development of ROC related approaches to improving its statistical strength while utilising a low number of images (Månsson, 2000).

Adaptions to the basic ROC approach have sought to overcome these limitations. The Localisation ROC (LROC) approach requires the observer to define both the artefact and its location. This is further developed as the Free-response ROC (FROC), in which the observer is asked to identify multiple lesions concurrently with their position, within this an estimation of the observer's confidence regarding the artefact, typically a lesion, and its

location is also recorded. This scheme provides greater statistical power with extended sets of cases and viewers. Differential ROC (DROC) was developed to compare between two different modalities. DROC has higher statistical power than that of ROC (Zarb et al., 2010). These approaches have been confirmed to be approximately correlated to the clinical environments and tackled the earlier shortcomings (Båth, 2010).

2.5.2.2 Visual Grading Analysis

Visual grading of the visibility and reproduction of the anatomical structures is a popular, simple and valid scheme to visually assessing the quality of the clinical images (Seeram et al., 2014). Its implementation is based on the visualisation of the anatomical structures by asking a viewer to estimate the clarity of some details in medical images. This assessment method, based on the human decision, offers a clinically favoured method for evaluating the image quality (Smedby and Fredrikson, 2010). The significance of the VGA approach in the detection of diseases has been studied and confirmed as defining a robust relationship between the anatomical clarity of normal anatomy and the ability to detect the pathological structures (Månsson, 2000, Sund et al., 2004). The reasons for using visual grading as a preferred technique are reported as (Båth, 2010):

- The validity of VGA investigations can be considered high when the anatomical structures are chosen based on their clinical relevance and the observers are experts in radiography.
- In special cases, VGA methods have been proved to coincide with both detection investigations using human observers (Tingberg et al., 2000, Herrmann et al., 2000) and utilising physical assessment for image quality (Sandborg et al., 2001, Sandborg et al., 2000).
- In comparison to ROC methods, VGA studies are comparatively easy to implement, especially when optimising equipment at the local level. This is because, with the VGA method, a lesser number of images are needed, and fewer evaluators may be sufficient than that of ROC approach.
- The time required to perform VGA assessment is comparatively short, at least for the observers, which means that it can be conducted in any dispensary or hospital.

- Special preparations are needed to conduct ROC analysis, for example, half of the images should contain pathologies and particular software is needed to conduct the test; these issues are not required for VGA investigations.

Two common ways can be employed to conduct VGA trial to assess the image quality (Zarb et al., 2010):

2.5.2.2.1 Absolute VGA

In this method, each image is viewed individually, and the observer is asked to give his/her opinion about the visibility of the anatomical structures in the image. The absolute VGA score ($VGAS_{abs}$) can be calculated from the collected ratings (Eq. 2.7) (Sund et al., 2004).

$$VGAS_{abs} = \frac{\sum_{i=1}^I \sum_{c=1}^C \sum_{o=1}^O G_{(abs)i,c,o}}{I \times C \times O} \quad (2.7)$$

Where $G_{(abs)i,c,o}$ is the absolute rating for a given image (i), criterion (c), and observer (o). I , C and O represent the total number of images, criteria and observers, respectively.

2.5.2.2.2 Relative VGA

In relative VGA, the observer compares and rates the visibility of anatomical structures of a test image against the same structures of a reference image. A range of scores is used to define the observers' judgment. The relative VGA score ($VGAS_{rel}$) can be computed from the collected ratings (Eq. 2.8) (Seeram et al., 2014). It is recommended that when implementing this method, the reference image should always be displayed side by side on a screen similar to the screen used to display the test image to guarantee that these images are presented with the identical monitor brightness and contrast (Seeram et al., 2014, Zarb et al., 2010, Månsson, 2000).

$$VGAS_{rel} = \frac{\sum_{i=1}^I \sum_{c=1}^C \sum_{o=1}^O G_{(rel)i,c,o}}{I \times C \times O} \quad (2.8)$$

Where $G_{(rel)i,c,o}$ is the relative grading for a given image (i), criterion (c) and observer (o). I , C and O indicate to the total number of images, criteria and observers, respectively.

Utilising the visual approaches to evaluate digital image quality would make the outcomes more appropriate to clinical environments since these measures concentrate on how obviously an observer can visualise the anatomical structure of a given image (Ludewig et al., 2010, Månsson, 2000). Two key shortcomings are identified; VGA reveals the observer's

view and hence can be sensitive to inter-observer variability (Sund et al., 2004), and the anatomical details, required to be assessed, must be determined previously. No official and validated guidelines on this are available and there is a difference of opinion in the published literature; hence, performing comparisons is difficult (Shet et al., 2011, Li et al., 2010).

2.5.2.3 Variability in Visual Assessment of Image Quality

In diagnostic radiology, the variance in assessing image quality has been generally identified as a phenomenon and many studies have been suggested to address this aspect and improve the measurement of image quality (Seeram et al., 2014, Mraity et al., 2014, Shet et al., 2011, Freedman and Osicka, 2006). In the setting of image quality evaluation, system efficiency may not be the sole cause of decision discrepancy where observer variability can significantly affect the overall diagnostic reliability (Manning et al., 2005) which may, therefore, impact the accuracy of the outcomes gained from the implementation of the visual measurements. This variability may happen due to the lack of standard criteria to evaluate image quality visually. Inconstancy in the estimation of image quality has been studied since the 1940s (Kundel, 2006). In this context, Krupinski and Jiang (2008) have proposed two significant things which require being thought to tackle the variability issue; systems are needed to improve observers' performance and minimise the interpretation variability, and techniques are required to evaluate systems and their impact on the observer's performance. European guidelines on quality criteria for CT images can be considered as a standard for handling the variability in the visual assessment of image quality (Menzel et al., 2000).

2.5.2.4 Image Quality Criteria

At the end of the 1980s, it was felt that new criteria would be required to tackle the previously identified problems in assessing visual image quality (Mraity et al., 2014). In 1987, an approach for identifying quality criteria was launched within the framework of the radiation protection programme/Commission of European Communities (CEC). The main objective of this project was to improve the ability of medical imaging experts on evaluating image quality. These constructed criteria covered radiological, technical and physical factors (Maccia et al., 1995).

Having developed the quality standards, two clinical experiments were performed within twenty-four European countries to present a set of guidelines for implementing unified techniques for routine radiographic tests. The main objective was to gain an adequate image quality while minimising the radiation dose. At first, six regular X-ray scans were

investigated, involving skull, chest, breast, lumbar spine, urinary tract and pelvis. These radiographic examinations have been selected because of their common use and the large amount of radiation that was given to patients (Nahrstedt et al., 1990). A second trial was conducted in 1991 to validate the suggested criteria by concentrating on chest, breast and lumbar radiographs only. Three separated questionnaires created, for each of the three examinations, and then were given to the participated radiology departments. The quality criteria adopted by these departments to evaluate the images was one of the things that were requested in this investigation. The questionnaires were collected with the corresponding films and sent to fifteen specialists to analyse the data and assess the films using the same criteria and questionnaires (five experts for each examination). The criteria were then selected based on the conformity that occurred between the observers (Maccia et al., 1995).

Since that, many radiography departments started developing the quality criteria to evaluate the image quality, with the final version of the guidelines has been issued in 2000 (Menzel et al., 2000). This final release includes an updated set of criteria and essentially tackles three subjects: diagnostic image quality, absorbed radiation dose, and the election of radiographic methods. These guidelines concentrate on the visibility of anatomical structures within the clinical image and how this helps in getting a reliable diagnosis. Moreover, the level of clarity of anatomical structures was classified into three main definitions (Seeram et al., 2014):

- *Visualisation*, which means that the distinctive characteristics are discoverable, but details are not entirely reproduced; *only features are clear*.
- *Reproduction*, which indicates that the details of the anatomical structures are noticeable but not indeed obviously identified; *detail is appearing*.
- *Visually sharp reproduction*, which refers to the clear representation of the anatomical structure details; *details are clear*.

These standard criteria are deemed as a basis by which the radiological community can conduct additional investigations to develop image quality measures (Menzel et al., 2000). In general, the aim of developing these criteria was to standardise the practices and, significantly, in the assessment of image quality.

2.6 Evaluation of Extracted Watermark Validity

The following metrics can be applied to measure the similarity between encoded and extracted watermarks. In all of the used equations, W and W' denote the embedded and extracted watermarks, respectively.

2.6.1 Correlation Coefficient

Correlation Coefficient (CRC) uses to measure the equivalence between the embedded and extracted watermarks (Eq. 2.9). It takes values between 0 and 1 (Jabade and Gengaje, 2011).

$$CRC = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2 * \sum_i \sum_j W'(i,j)^2}} \quad (2.9)$$

2.6.2 Similarity Measure (SIM)

Similarity Measure (SIM), also defined as Similarity Coefficient (SC), can be utilised to calculate the similarity between the embedded and extracted watermarks (Eq. 2.10) (Jabade and Gengaje, 2011).

$$SIM = \frac{\sum_i \sum_j W(i,j)W'(i,j)}{\sum_i \sum_j W'(i,j)^2} \quad (2.10)$$

2.6.3 Bit Error Rate

Bit Error Rate (BER) metric is defined as the ratio between binary patterns, that are decoded wrongly, and length of the binary sequence. It calculates the number of error bits between the original and extracted watermarks (Eq. 2.11). A BER value of 0 indicates that the embedded and extracted watermarks are identicals (Selvam et al., 2017).

$$BER = \frac{EB}{TB} \quad (2.11)$$

Where EB is the number of error bits, and TB is the total number of watermark bits.

2.6.4 Accuracy Ratio

Accuracy Ratio (AR) can also be used to evaluate the matching between the original and extracted watermarks. It calculates the number of correct bits between the original and extracted watermarks (Eq. 2.12). An AR value of 1 indicates that the embedded and extracted watermarks are equals (Selvam et al., 2017).

$$AR = \frac{CB}{TB} \quad (2.12)$$

Where CB is the number of correct bits, and TB is the total number of watermark bits.

2.7 Chapter Summary

This chapter presented a technical background on some popular medical image modalities which are commonly used in medical domains. It also provided basic information of digital watermarking including its classifications, techniques and requirements that must be taken into account when designing a watermarking system. This would aid in the selection of techniques and approaches for achieving the objectives of this research.

DICOM is a standard for using, managing and exchanging medical images captured from various medical. Metadata, which is located in the header of the DICOM images, comprises information to describe the images and patients which make the size of the header varies from one image to another and also varies according to the imaging modality. Medical images typically contain crucial information which makes any modification during viewing, transmitting and archiving is intolerable. This issue leads to the significant need for developing a robust and reliable approach to enhance security tools within the medical imaging workflow.

Digital watermarking is recognised as a robust approach to verify the integrity and authenticity of medical images. It has many attractive properties, which cannot be seen in other security techniques, such as preserving the visual semantics of images and considering the visual image quality when encoding the watermark data. Applying digital watermarking to digital images require considering several fundamental requirements including imperceptibility, robustness, capacity, security, and complexity. A high embedding capacity can be realised by sacrificing either imperceptibility, robustness or both. Therefore, a suitable balance might be found according to the desired application.

Distortion of watermarked images, watermark imperceptibility, can be measured either physically or visually or using both approaches. Physical measures are easy to implement which made them heavily used in evaluating visual image quality. However, they not taking into account the anatomical structures of the images which are significant in clinical practices. Therefore, physical metrics should be accompanied by a visual assessment to confirm the reliability and validity of the evaluation approach.

CHAPTER THREE

Literature Review

This chapter presents a review of significant published works in the field of digital watermarking, applied to ensure integrity and authenticity of medical images, to identify the strengths and limitations of various techniques developed to enhance the trust in medical diagnosis workflow. This contributes to establishing the context of the research and direct possible research paths to tackle the weaknesses of existing watermarking approaches and provide a foundation for the evaluation of the work to realise the objectives of this research. This literature review has been conducted based on particular criteria constructed from the defined research problem. These criteria aid in evaluating the previous studies to select materials related to the scope of this research.

3.1 Introduction

Hiding digital watermark in medical images is a significant issue and can be utilised for many applications including authentication, integrity verification, tamper detection and copyright protection. The medical images have to be carefully dealt with as the encoded data can affect the visual image quality and therefore might impact the medical diagnosis, which ultimately leads to severe consequences. While each has its advantages and limitations, almost all watermarking techniques revolve around several fundamental factors such as visibility, robustness, hiding capacity, retrieving method, etc. In this research, a comprehensive survey has been conducted on the existing techniques utilised to verify the authenticity and integrity of medical images to select a convenient approach for hiding the watermark to achieve the desired goals.

This literature survey carried out three key phases: planning, conducting, and reporting the results. In the first phase, the need for a literature review has been identified and then the research questions have been formulated based on particular criteria derived from both the identified research problem and the aim of this research. In the second phase, the related studies have been analysed and assessed in terms of relevance to the research scope. The results have been collected, investigated and reported in the final stage of this survey. Based on the identified research problem and the aim and objectives of this research, this literature review strives to answer several questions:

Q1: Is there a need to watermark medical images?

Q2: What are the proper techniques for encoding digital watermark into medical images?

Q3: Are there particular requirements for watermarking medical images?

Q4: What are the appropriate techniques for evaluating the visual quality of watermarked medical images?

Q5: What are the proper criteria for evaluating the performance of medical images watermarking approaches?

The first question is necessary to highlight the security threats in medical imaging workflow and how digital watermarking can tackle these threats to enhance trust in medical domains. The second and third questions are significant to investigate the existing watermarking techniques and define the particular requirements of digital imaging workflow to select suitable approaches for watermarking medical images. The fourth and fifth questions contribute to determining the proper tools and techniques to evaluate the visual quality of watermarked images as well as assessing the efficiency of the proposed approaches.

To obtain an integrated list of studies relevant to the research scope, an advanced search in most famous and related digital libraries has been undertaken using peer-reviewed journal articles, conference proceedings and book chapters. The selected databases comprise SCOPUS, SCIENCEDIRECT, SPRINGER, and IEEE explorer. The search words were formulated based on several factors:

- The main keywords derived from the research question.
- Synonyms of the main keywords.
- Keywords that were appeared in related studies.
- Boolean AND and OR were used to combine the main research keywords and synonyms.

Examples of key search words utilised in all chosen digital libraries include but are not limited to: *digital watermarking, medical imaging, Digital Imaging and Communications in Medicine, medical image watermarking, Digital Imaging and Communications in Medicine watermarking, reversible watermarking, medical image security, medical image authentication, medical image integrity, image quality, image quality criteria, medical image quality assessment, medical image quality evaluation, physical assessment, physical evaluation, visual assessment, visual evaluation, Receiver Operating Characteristic, Free-*

response Receiver Operating Characteristic, Visual Grading Analysis, relative Visual Grading Analysis. Furthermore, significant studies that have been cited in relevant researches were taken into account.

Based on the formulated research questions and objectives, inclusion and exclusion criteria were applied to select the studies that are related to the research scope. These studies were imported to EndNote X7 library to be used in this research and studies that did not satisfy the inclusion criteria were excluded.

3.2 Requirements of Medical Images Watermarking

In addition to the general requirements of digital watermarking (Section 2.4.2), some other fundamental requirements are essential and must be considered when applying digital watermarking to medical images. Developing a new watermarking approach that can satisfy these requirements remains a significant and relevant research area. These requirements include imperceptibility, reversibility, and reliability (Mousavi et al., 2014).

3.2.1 Imperceptibility

This feature indicates the amount of distortion that occurs on an image after encoding the watermark data. It considers the highest requirement of invisible watermarking schemes and might be achieved by reducing either robustness, capacity or both. A digital watermark is defined as imperceptible/invisible if the original and modified images are visually indistinguishable (Qasim et al., 2018a).

3.2.2 Reversibility

In medical domains, if an image is modified during the workflow process a collapse in trust regarding the validity of the images is formed. Any small change to the image could lead to misdiagnosis with possible life-threatening consequences or legal implications. Therefore, recovering the original unmodified image after extracting the encoded watermark is an essential issue that needs to be considered when applying digital watermarking to medical imaging (Qin et al., 2018).

3.2.3 Reliability

This may be decomposed into two aspects (Priya and Sadasivam, 2014):

- Integrity control: the ability to confirm that the data has not been changed without authorisation.
- Authentication: the ability to identify data source and verifying that the information relates to the right patient.

3.3 Medical Image Watermarking Techniques

Existing digital watermarking techniques applied to medical images can be classified into three groups; classical methods, a Region of Interest (ROI) and Region of Non Interest (RONI) methods, and reversible approaches (Table 3-1). Whatever technique is used, the computational complexity of the watermarking operation should not cause a delay in the clinicians' time (Coatrieux et al., 2006).

3.3.1 Classical Methods while Minimising the Distortion

In conventional watermarking methods, watermark data is embedded in whole cover images by replacing some details like LSBs or losing some details when using lossy image compression methods (Coatrieux et al., 2006). When implementing a digital watermarking scheme for a medical image, the image must not be perceptually changed because no radiologist will agree to use the degraded image for taking a decision, no matter how small the modification is. Hence, the watermarking algorithm must be reversible (Fontani et al., 2010). The irreversible watermarking approaches remain subject to an admission by clinicians while the original images stay usually preferred for medical investigations (Tan et al., 2011).

3.3.2 Region of Interest and Region of Non Interest Watermarking Methods

Coatrieux et al. (2001) assume that medical images can be divided into two regions ROI and RONI. ROI section includes the informative region of the image that is used for diagnostic purposes and must be preserved without any distortion. However, RONI usually represents the black background of the image, but occasionally it can contain grey level parts of slight interest (Shih and Wu, 2005). In the case of encoding watermark data into the ROI, spatial and transform domain techniques can be utilised for the embedding process. The encoding technique may be robust or fragile to manipulations based on the purpose of the desired application. These watermarking techniques are implemented in a particular way without impacting the visual quality of images (Memon et al., 2011, Coatrieux et al., 2007).

Table 3-1: A comparison of existing digital watermarking schools applied to medical images. Several features are used to evaluate these hiding schools including the technique of hiding, robustness, imperceptibility, capacity, reversibility and the objective of use. Reversible methods utilise particular embedding techniques differ to those used in the classical methods.

Hiding school	Hiding technique	Robustness	Imperceptibility	Capacity	Objective
Classical methods	Spatial domain	Fragile	High	High	Integrity, Authentication
	Transform domain	Robust	Low	Low	Ownership protection
ROI & RONI methods	Spatial domain	Fragile	High	Dependent	Integrity, Authentication
	Transform domain	Robust	Low	Dependent	Ownership protection
Reversible methods	Compression based	Fragile	High	High	Integrity, Authentication
	Histogram based	Robust, Semi-fragile	Low	Low	Ownership protection
	Quantisation based	Fragile	High	High	Integrity, Authentication
	Expansion based	Fragile	High	High	Integrity, Authentication

Using ROI sections for embedding the watermark may deform the pixels in those regions which may consequently cause a wrong medical diagnosis. On the other hand, RONI watermarking approaches embed watermark data in areas that unimportant in medical diagnosis, but they have several drawbacks such as they can be only implemented if the RONI exists, the amount of information to be embedded depends on the RONI size, and the ROI may not be protected against malicious operations.

3.3.3 Reversible Watermarking Methods

Embedding of a secret message as a watermark, no matter how trivial the modification is, can cause degradation to the visual image quality. In some applications, such as military, medical, legal and archival applications, where the authentication requirements are often essential, there are typically strict restraints on data reliability that prevent any deformation in the watermarking operation. Modifying a patient's medical image could affect the patient's life by causing errors in diagnosis and treatment. As a result, reversible watermarking techniques have been developed which can stop this shortcoming by applying

a technique that can recover the embedded watermark as well as the original unmodified image at extraction (Fig. 3.1). Reversible watermarking, utilised for image authentication applications, offer a comprehensive framework as it maintains the integrity of the image, while the advantage of reversibility protects the visual quality of images. Reversible watermarking can be considered as a special case of digital watermarking (Khan et al., 2014).

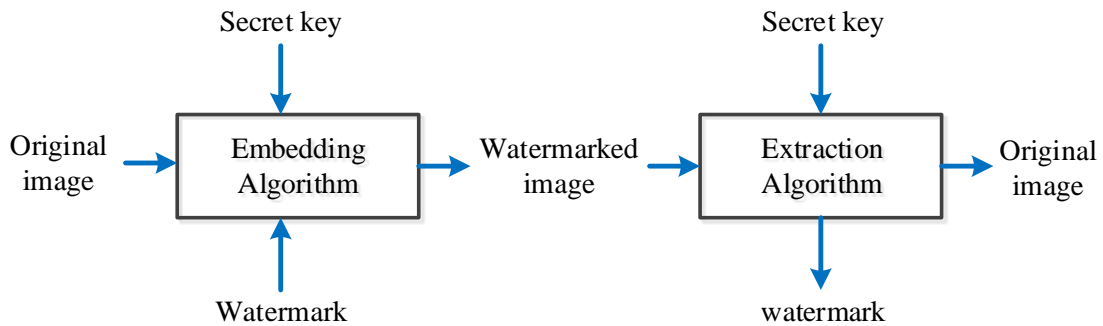


Fig. 3.1: Main components of reversible watermarking approaches. In the embedding process, the watermark is encoded into the original image by using a secret key while both the watermark and the original unmodified image can be retrieved at extraction.

Patented work on reversible watermarking was introduced by embedding digital signature of an image into the original image to verify its integrity by implementing a spatial additive watermark method (Honsinger et al., 2001). This approach suffers from salt and pepper noise and delay in retrieving the encoded watermark due to the use of modulo additions 256 that was combined with the implemented watermarking method. A different watermarking technique was proposed by utilising circular interpretation of bijective transformations of the histograms to reduce the salt and pepper noise found in the previous approach (De Vleeschouwer et al., 2003). Some metrics were used to evaluate the implemented method. However, comparison of payload capacity against image distortion was not presented.

Feng et al. (2006) have categorised reversible watermarking techniques into three groups; Data Compression (DC), Difference Expansion (DE) and Histogram Bin Shifting (HBS). Pan et al. (2009) have classified reversible watermarking methods into two groups based on the hiding technique; additive and substitution methods. A different survey has been conducted by categorising the reversible watermarking techniques based on the robustness of the watermarking algorithm into three groups; robust, fragile and semi-fragile methods, and also based on the hiding domain into spatial and transform techniques (Caldelli et al., 2010).

In this survey, reversible watermarking techniques have been categorised into four groups; compression based, histogram modification based, quantisation based and Difference Expansion (DE) based. Recently, reversible watermarking techniques based on DE concept have been proposed in many research, and they typically exceeded the other reversible methods in that they offer a higher embedding capacity and a lower computational complexity compared to the other techniques (Qasim et al., 2018a, Khan et al., 2014).

3.3.3.1 Compression Based Technique

Reversible watermarking requires encoding additional information into cover images along with the watermark data to recover original unmodified images at extraction. This makes the length of the watermark is much more than the conventional watermarking methods. A simple technique for maximising the hiding capacity is by compressing a part of the host image to provide more space for carrying the watermark (Feng et al., 2006, Khan et al., 2014).

Several watermarking approaches based on compression technique were stated in the literature. A high-capacity reversible technique was developed by utilising integer wavelet transform and compounding method (Xuan et al., 2004b). The proposed method encodes the watermark data into the high-frequency coefficients by shifting the histogram of images and applying pre-processing operations to avoid the overflow/underflow problems, which might occur when pixel values become higher or lower than the boundary of pixel values. A common compression-based method was offered (Celik et al., 2005). The image pixels were first subjected to L-level scalar quantisation and the remainders were compressed by applying the Context-based Adaptive Lossless Image Codec (CALIC) algorithm. Watermark data were integrated with the compressed remainders and encoded into the quantised image to generate the watermarked image. At extraction, the watermarked image is quantised, and the remainders are decompressed to extract the embedded watermark and recover the original image. To improve the embedding capacity, Arsalan et al. (2012) gathered the compounding technique, which presented by Xuan et al. (2004b), with a genetic algorithm. Original images were converted into transform domain by applying integer wavelet transform. The transformed images were then segmented into blocks, and a threshold value was calculated for each block. The genetic algorithm was used to select the optimal/near-optimal threshold, which organises the compounding operation and efficient payload. Compounding process was executed for each block has a value larger than a particular

threshold. The weakness of this scheme is the large time required for the training phase and applying the genetic algorithm to each cover image.

3.3.3.2 Histogram Modification Based Technique

Comparing to other reversible watermarking techniques, which are not strong against image processing operations, histogram modification based technique has been developed to achieve the robustness issue. The embedding target is replaced by the histogram of a block to improve the robustness of the watermarking algorithm (Feng et al., 2006). Most embedding methods in this type are typically block-based, and therefore they have the strength to resist some image operations. The hiding capacity of this approach is low, but the robustness is the main purpose of this technique (Fotopoulos et al., 2008).

In the scheme presented by De Vleeschouwer et al. (2001), original images were segmented into blocks of neighbouring pixels and each block was then divided into two regions, with consistent histograms are computed. Circular interpolation was utilised to shift the histogram bins to encode the watermark bits. A high distortion may occur when shifting the highest and lowest bits to the other side. Therefore, this approach was enhanced by using the bijective transformations to reduce the massive distortion and control the change of maximum and the minimum bits by permitting two only shifts at most (De Vleeschouwer et al., 2003). Another histogram based techniques were developed to encode watermark data into only the peak bin pixels of images (Ni et al., 2006, Xuan et al., 2004a). These techniques require additional overhead to retrieve the concealed data as well as the original unmodified images. However, they provided a reasonable visual quality of watermarked images.

In order to raise the hiding capacity, Lin et al. (2008) proposed a multilevel reversible method using the difference image histogram modification that used the peak point to encode the watermark data. The input image was partitioned into non-overlapping blocks of 4x4 pixels, and then a variance matrix of size (3x4) was created for each block. Histogram shifting was applied to each difference block to conceal the watermark data. Although this approach offers a high capacity due to implementing a multi-level embedding method, it suffers from the massive amount of side-information that is required for saving the peak value of all blocks. Tsai et al. (2009) proposed a high capacity hiding scheme by employing a residue image. The remainder image indicates the difference between an original pixel and every other pixel in the non-overlapping block rather than the difference between neighbouring pixels. The highest and zero points of each block were required to be encoded

within the message bits to realise the reversibility. This issue reduced the hiding capacity of the proposed scheme. A high capacity reversible watermarking approach was presented by exploiting the idea of downsampling to enhance the implementation (Khan and Malik, 2014). Downsampling provides two sub-sampled forms; reference and data hiding, to create a space for embedding the data by utilising the histogram shifting technique. Location map of pixels was compressed and encoded into the image to obtain a blind scheme at extraction and reduce the distortion level of watermarked images.

3.3.3.3 Quantisation Based Technique

In general, conventional watermarking based on quantisation technique are robust. However, quantisation based reversible watermarking methods are, typically, fragile in nature (Khan et al., 2014). A combination of Sequential Quantisation Strategy (SQS) and reversible watermarking technique was proposed to increase the opportunity of detecting unauthorised modifications (Cheung and Wu, 2007). The proposed SQS makes the variation of a pixel value dependent on the other pixels to, therefore, enhance security measures to verify the authenticity and integrity of images. Saberian et al. (2008) introduced a reversible watermarking approach based on Weighted Quantisation Method (WQM) to encode watermark data in both spatial and transform domains. The deformation of this approach, unlike the other approaches, is not payload capacity dependent and can be easily controlled by adjusting quantisation levels.

Typically, classical Quantisation Index Modulation (QIM) watermarking methods are irreversible and original unmodified images cannot be recovered because of the modifications that occur on original images as a result of using the quantisation algorithm. However, Ko et al. (2012a) developed a reversible watermarking method for medical imaging applications based on nested QIM technique. The suggested nest structure contributed to reconstructing the original image at extraction and increasing the hiding capacity of the scheme. The proposed nested approach was developed by combining the QIM technique with Fractional Discrete Cosine Transform (FDCT) to reduce images distortion level alongside reconstructing the original images (Ko et al., 2012b).

3.3.3.4 Difference Expansion Based Technique

The concept of DE was first introduced in 2003 to present a new approach for reversible watermarking techniques (Tian, 2003). It embeds 1-bit of watermark data into the LSB of

the difference value of two pixels. Selected pairs can either be any two adjacent pixels (horizontal or vertical) or any two pixels selected in a pre-defined form. To raise the embedding capacity, Alattar (2003) extended the previous DE technique by utilising spatial and spectral triplets of pixels to encode 2-bits of data. Spatial triplets denote any 3-pixels selected from the identical spectral or colour part of the image. Spectral triplets can also be any 3-pixels chosen from different spectral components. Further enhancement of hiding capacity was achieved by encoding 3-bits in the difference values of 4-pixels (Alattar, 2004a). The easiest way of determining the pixel quad is by selecting a consecutive 2x2 pixel, and this approach can be further generalised (Alattar, 2004b). This generalised method encodes several bits in the difference values vectors of connected pixels instead of pairs, triplets and quads.

A significant development for the DE technique was presented by using a new technique called Prediction Error (PE) expansion (Thodi and Rodriguez, 2004). The encoding process is based on expanding the error instead of the difference between two adjacent pixels to decrease images degradation. To prohibit overflow/underflow issues, which might happen when pixel values become higher or lower than the boundary of the limit of pixel values, only expandable pixels are selected in the embedding process. Location map of pixels is combined with the watermark data and encoded into the images to extract the concealed data and retrieve the original images precisely at extraction. A further enhancement to the previous approach was realised by eliminating the need for location map through combining PE with histogram shifting technique (Thodi and Rodríguez, 2007). Histogram shifting requires an overflow/underflow map, which requires comparatively less space than location map which aids therefore in reducing the deformation level and controlling the capacity issue. The main difference between using histogram shifting technique and location map is the degradation amount generated in the embedding process. In case of using location map, the deformation only occurs in the pixels used to encode the watermark data, while in histogram shifting, pixels that are not employed for carrying the watermark are also suffering from modification due to the using of shifting operation (Khan et al., 2014).

The weakness of the DE watermarking technique is the reduction of the hiding capacity due to the need for a location map denoting the pixels where data is embedded. This location map needs to be encoded alongside the watermark into the image because it is required at extraction to extract the encoded data. This huge additional information reduces the embedding capacity and increases the distortion level of watermarked images (Qasim et al.,

2018a). Furthermore, most watermarking approaches based on DE techniques are pixel-wise or block-based and damage of pixel/block of data does not impact the other pixels/blocks. However, modifying the encoded location map impacts the ability to retrieve the embedded data and the original image as well. Therefore, DE watermarking techniques are fragile against operations making them appropriate for authenticity and integrity applications (Feng et al., 2006).

3.4 Purposes of Medical Image Watermarking

Navas and Sasikumar (2007) have divided medical images watermarking methods into two groups; authentication and integrity watermarking techniques, and Electronic Patient Record (EPR) watermarking techniques. Medical images watermarking approaches can also be classified to three groups based on the desired application (Table 3-2); authentication watermarking techniques, EPR watermarking techniques, and approaches that combine both authentication and EPR watermarking techniques to verify information source as well as to detect images manipulations (Al-Qershi and Khoo, 2011a).

3.4.1 Authentication Schemes

A range of methods can be used to verify the authenticity of digital medical images (Qasim et al., 2018a):

- Hiding the EPR to confirm that the information belongs to the correct patient.
- Hiding the metadata, which is located in the header of DICOM images. Some metadata may be modified each time with the distributed image. Therefore, only information related to the patient and the image should be employed.
- Combining the header with the raw image data by concealing the Digital Signature (DS) of the header. Although this method decreases the message length, the header data is inextricably connected to the image during transmission.

Image integrity verification can typically be achieved by:

- Hiding the Digital Signature (DS) of the image.
- Hiding the Message Authentication Code (MAC) of the image.

At extraction, the integrity of the images can be validated by matching the recalculated DS/MAC and the previously hidden DS/MAC and identifying differences, if any, to determine applied modifications.

Table 3-2: Summary of different medical images watermarking approaches stated in the literature. The performance of these approaches is compared based on various criteria including type of watermark data, regions and techniques used to encode watermark data, ability to retrieve original images at extraction, and robustness of approaches against images processing operations. (N/A not available).

Authors	Purpose	Watermark	Embedding region	Embedding technique	Robustness
Mostafa et al. (2010)	Minimising storage space Ensuring safety	EPR data	Whole image	DWPT	Robust
Al-Qershi and Khoo (2011a)	High capacity	Random bitstream	Smooth region Non-smooth region	DE	Fragile
Al-Qershi and Khoo (2011b)	Authentication Data hiding	EPR data ROI hash message Compressed ROI ROI embedding map ROI blocks	ROI RONI	DE DWT	Robust Fragile
Memon et al. (2011)	Copyright protection Authentication Integrity	Patient's information Doctor's code LSB _s of ROI	ROI RONI	Hybrid	Robust Fragile
Tan et al. (2011)	Integrity Authentication Tamper detection	Metadata Authentication data Tamper detection Estimator position	Whole image	Random location signal Estimator	Robust Fragile
Agung and Permana (2012)	Tamper detection	Image's LSB _s Authentication data	ROI RONI	LSB	Fragile
Das and Kundu (2013)	Security Authentication Save archiving Captioning Controlled access	ROI hash code DICOM metadata Indexing keyword Doctor's code Tamper localisation	Whole image	LSB	Fragile

Table 3-2: Continued.

Authors	Purpose	Watermark	Embedding region	Embedding technique	Robustness
Eswaraiah and Reddy (2014b)	Integrity Tamper detection	Authentication data ROI hash code ROI recovery data	LSB _s of RONI LSB _s of border pixels	LSB	Fragile
Tareef et al. (2014)	Integrity Authentication	Sparse code of EPR Reshaped ROI	RONI	Sparse coding Singular Value Decomposition (SVD)	Robust
Brar and Kaur (2015)	Authentication High capacity	EPR data Hash code	Virtual borders	DE LSB CDCS	Fragile
Roček et al. (2016)	Security Authenticity	Public share Secure share	ROI RONI	DT-CWT LSB	Robust
Parah et al. (2017)	High capacity Content authentication	EPR data Checksum bits Logo bits	Scaled up of the original image	PTB conversion ISB bit	Fragile
Selvam et al. (2017)	Integrity Authentication	EPR data	Whole image	IWT DGT	Robust
Pan et al. (2018)	Integrity Authentication	N/A	ROI RONI	DWT HS	Fragile
Atta-ur-Rahman et al. (2018)	Integrity Tamper detection	Chaotically generated watermark	Whole image	Chaotic key RNS CRC	Fragile

In digital watermarking, there is an inverse relationship between the capacity, robustness, and imperceptibility. Therefore, an evaluated trade-off of properties may be applied depending on the desired application. The priority order of authentication and integrity applications is imperceptibility, robustness, and capacity (Qasim et al., 2018a).

In healthcare applications, a reversible, fragile and blind watermarking method is required for validating authenticity and integrity of medical images. A dual layer reversible watermarking approach was proposed to confirm the integrity and authenticity of DICOM medical images (Tan et al., 2011). Input images were decomposed first into non-overlapping blocks of 2x2 pixels. One pixel from each block is selected to act as an estimator, and the other pixels were used to encode 3- bits of watermark data. In the first layer, metadata, authentication information, and estimator position were concealed, while tamper detection information was embedded in the second layer. For tamper localisation, Cyclic Redundancy Check-16 bits (CRC-16) is calculated and hidden in the same block. The embedding capacity reached 0.75bpp. Although this scheme can reveal tampered regions, it cannot recover the altered regions. Agung and Permana (2012) extended Liew et al. (2010) and Zain and Fauzi (2006) approaches by presenting a reversible watermarking technique to detect tampers and retrieve the original medical images. The extension based on compressing the original LSBs by applying the RLE compression technique before encoding the data into the RONI part of images. Tamper detection information and recovery data were encoded into the ROI, while RONI section was used to encode the LSBs of the whole image instead of only LSBs of ROI part (Liew et al., 2010) to ensure the reversibility of the proposed approach.

Das and Kundu (2013) developed a blind and fragile reversible watermarking scheme by combining lossless compression technique with encryption to encode DICOM metadata, the hash code of images, and tamper localisation information into medical images. Secure Hash Algorithm-256 bits (SHA-256) was adopted to calculate the hash code of the ROI part of the image and the integrity of the image was confirmed by comparing the embedded and recalculated hash codes. A fragile watermarking method was presented for validating the integrity of the ROI section, identifying the manipulated blocks inside the ROI, and recovering the original ROI (Eswaraiah and Reddy, 2014a). Medical images were first partitioned into three parts; ROI, RONI, and the border region and the hash code of the ROI part was computed using SHA-256. This hash code was encoded into the border region, and authentication and ROI recovery information were encoded into the RONI part. Several limitations can be observed in these approaches (Eswaraiah and Reddy, 2014a, Das and

Kundu, 2013); the ROI part needs to be defined manually, only the ROI section can be retrieved at extraction, and a substantive location map is required for extracting the concealed data. Al-Haj (2015) proposed an algorithm based on symmetric and asymmetric encryption to ensure confidentiality, integrity, and authenticity of the header data, as well as pixels data of medical images. The pixel data was totally encrypted to realise the confidentiality while integrity and authenticity were verified by using a digital signature technique. A newer approach combined the features of reversible, zero and RONI watermarking methods (Roček et al., 2016). This technique merges the zero-watermarking principle in the ROI using Dual Tree Complex Wavelet Transform (DT-CWT), with high capacity of reversible watermarking in the RONI. This scheme needs a location map to retrieve the embedded data and the original unmodified image.

Selvam et al. (2017) presented a blind hybrid reversible watermarking approach, operating in the transform domain, for increasing hiding capacity and protecting the medical image. Integer Wavelet Transform (IWT) and Discrete Gould Transform (DGT) are used to encode the watermark within the medical image. In the extraction, the concealed watermark is retrieved, and the original unmodified image is restored without any auxiliary data. However, this approach exhibits high distortion with low payload capacity. Pan et al. (2018) presented a fragile reversible watermarking approach for digital radiographic images. This technique differentiates the background from anatomical details within the image. Histogram shifting modulation is used to encode the watermark into the background section while HS is applied to wavelet detail coefficients of the anatomical object. This scheme delivers reasonable visual image quality, but the hiding capacity is very low. Atta-ur-Rahman et al. (2018) proposed a blind reversible watermarking to realise a high level of secrecy and integrity for medical images. This scheme utilises a chaotic key to choose some pixels from the cover image to hide a chaotically created watermark. The remainders of the pixels are transformed into residues by employing the Residue Number System (RNS). A primitive polynomial, of degree four, is applied to divide the selected pixels and obtain the remainder which is appended to the watermark message. The validity of the watermark is ensured, at extraction, based on the calculated remainder. This approach exhibits high levels of imperceptibility. However, the embedding capacity of the scheme has not been measured. Moreover, the scheme does not rely on a region based watermarking strategy which makes the technique incapable of selecting the hiding regions.

3.4.2 EPR Data Hiding Schemes

In order to avoid the detachment between images and patients data as well as decreasing the required storage space, the EPR data, which includes patient's information such as name, ID, age, sex, demographic information and diagnosis result, can be embedded into the images (Priya and Sadasivam, 2014). Hence, the capacity represents a significant requirement making the priority order of EPR data hiding is imperceptibility, capacity, and robustness (Navas and Sasikumar, 2007).

Several watermarking approaches were reported for encoding the EPR data. A blind watermarking approach encoded the EPR data into medical images to minimise the required storage space, reduce distribution overhead, and ensure the safety of the exchanged data (Mostafa et al., 2010). The EPR was concealed, as a watermark, into the Discrete Wavelet Packet Transform (DWPT) of the cover image and applying Bose-Chaudhuri-Hocquenghem (BCH) to improve the robustness of the embedding technique. The main drawback of this approach is the low payload capacity, which can only embed 1-bit of data in each block of 4x4 pixels and this can be lower due to the used error correction code. Nambakhsh et al. (2011) utilised Electrocardiograph (ECG) signal and patients' ID as a dual watermark to protect the patients' data and avoid the mismatching of diagnosis information. Medical images were decomposed into seven sub-bands implementing dual level Discrete Wavelet Transform (DWT) and the watermark data was hidden in the two-dimensional wavelet sub-bands using a texture feature extraction process. This approach is robust against several operations and achieved a high visual quality of watermarked images for up to 85% of JPEG compression. However, the visual quality of the images tends to degeneration with the increasing of the size of the ECG signal and tamper detection, which is crucial for medical images authentication, was not considered in this proposed approach.

To increase the embedding capacity for medical images, Al-Qershi and Khoo (2011b) proposed two reversible watermarking approaches based on the DE technique. The first approach combines a technique, which embeds 2 bits of the payload in each pair of pixels (Tian, 2003), with a scheme, which encodes 12 bits of the watermark into each smooth blocks of 4x4 pixels (Chiang et al., 2008). The second method combines ab technique, which embeds 3 bits of the watermark in each quad of pixels (Alattar, 2004a), with the same scheme in the first approach (Chiang et al., 2008). One of the special features of medical images, in comparison to nonmedical images, is the large 'smooth' areas (blocks with equal pixel

values). These proposed approaches segment the image into smooth and non-smooth regions instead of ROI and RONI. High hiding capacity techniques are utilised in the smooth regions. However, DE is applied to the non-smooth regions. Although the scheme achieves high capacity, the major drawback is the lack of capacity control due to the need for embedding the compressed location map which is required for extraction.

3.4.3 Authentication and EPR Data Hiding Schemes

A mixture watermarking approach was developed to verify the authenticity of the ROI part of medical images, detect image tamper, and retrieving the tampered regions (Al-Qershi and Khoo, 2011a). Medical images were segmented into two parts; ROI and RONI, and patient information and the hash code of the ROI were hidden into the ROI part using reversible watermarking based on the DE technique. Information for tamper detection and retrieving the encoded data, which include the location map, the average of ROI blocks, and the compressed ROI, were encoded into the RONI section by applying a robust technique based on DWT. The main limitation of this approach is the manual identification of the ROI. A hybrid method concealed multiple watermarks into medical images to verify the confidentiality and integrity of the images. A robust watermark was applied to encode patient's data, doctor's authentication code, and LSB of the ROI into the RONI part to confirm copyright protection (Memon et al., 2011). The integrity of images was ensured by embedding the watermark into the ROI section by using a fragile watermark. Location map was generated and encoded into the images instead of histogram shifting to avoid overflow/underflow. Tareef et al. (2014) proposed a recovery technique that can be used for many purposes including EPR data hiding, ensure the integrity and authenticity of the ROI part, and retrieving the manipulated area. Sparse coding of the EPR data and the reshaped of ROI was hidden in the transform domain of the RONI. The patient's information was saved alongside the image to verify the image authenticity. At extraction, the encoded sparse code and ROI can be retrieved to reconstruct the altered image.

An efficient reversible watermarking system based on the DE technique was proposed to decrease the storage and communication cost (Brar and Kaur, 2015). Message Digest 5 (MD5) Algorithm was used to calculate the hash of images to verify the authentication. To maximise the embedding capacity, Class Dependent Coding Scheme (CDCS) was applied to encode EPR data by using pixel difference of virtual borders. Parah et al. (2017) proposed a high capacity reversible watermarking scheme for content authentication of medical

images. A Pixel to Block (PTB) conversion method was applied, to the cover image, to achieve high embedding capacity and confirm reversibility. The watermark, which consists of EPR, block checksum and logo bits, was encoded into the Intermediate Significant Bit (ISB) of the whole image to avoid LSB removal operations. Although this scheme achieves high embedding capacity, the distortion of watermarked images is high.

3.5 Chapter Summary

The necessity of protecting medical images and other patients' data is not only for confidentiality purposes but also to prevent manipulations that might happen by authorised and unauthorised users while using these images. Therefore, there is a need to use a technique for ensuring trust in digital medical workflows. Digital watermarking is recognised as a robust approach to ensure data integrity and authenticity in medical environments. In this chapter, a comprehensive review of medical image watermarking approaches and various issues related to each approach have been presented and discussed.

Many techniques have been proposed in the literature to utilise digital watermarking within medical imaging by using both spatial and transform domain techniques. These techniques hide the watermark in the whole image or in the part of images (ROI or RONI) by implementing reversible and irreversible methods. In comparison to the transform domain techniques, which are suitable for ownership verification applications, spatial domain techniques offer lower complexity, higher capacity, and better visual image quality. However, the spatial domain methods are fragile and cannot survive against many image processing operations making them appropriate for integrity and authentication applications.

RONI watermarking methods embed the watermark in regions that are insignificant in medical diagnosis, but they have several drawbacks such as they can be only applied if a RONI exists, the size of the watermark depends on the RONI size, and the ROI section would not be protected against malicious attacks. Therefore, applying these methods to medical images highly depends on the characteristics of the images.

Medical imaging requirements are extremely strict with the visual quality of images and do not permit non-clinical based modification in any way. Irreversible watermarking methods remain subject to non-acceptance by radiologists while original images are favoured for diagnosis purposes. Therefore, watermarking algorithms applied to medical images must be able to retrieve the original unmodified images. Reversible watermarking assures recovering

the complete original image precisely after extracting the embedded watermark successfully. Consequently, hiding capacity and the number of potential methods that can be applied to medical images is restricted significantly because of this feature.

Selecting an appropriate and reliable approach for employing digital watermarking within medical imaging workflow is essential. Imperceptibility of watermarked images, for all watermarking approaches that have been reviewed in this chapter, was evaluated by using physical measures. PSNR and SSIM metrics were often used to assess the visual quality of watermarked images, but they not taking into consideration the anatomical details of images that are significant in medical investigations (McCollough et al., 2006). Therefore, relating these measures to visual assessment approaches is essential to verify and confirm their validity.

CHAPTER FOUR

Assessment of Perceptual Distortion Boundary

Reversible and imperceptible watermarking approaches have the potential to enhance trust within medical imaging pipeline by ensuring the authenticity and integrity of the images to confirm that changes can be detected and tracked. This study concentrates on the imperceptibility issue. Unlike reversibility, for which an objective assessment can be easily made, imperceptibility is a factor of human cognition that needs to be evaluated within the human context. By defining a perceptual boundary of detecting the modification, this study enables the formation of objective guidelines for the method of data encoding and level of image/pixel modification that translates to a specific watermark magnitude. This research implements a visual evaluation based on relative Visual Grading Analysis (relative VGA) of brain MR images watermarked by varying techniques and magnitude of image/pixel modification to determine where this perceptual boundary exists and relate the point at which change becomes noticeable to the objective measures of the image fidelity evaluation. The outcomes of the visual trial were linked to the images PSNR values, thereby identifying the visual degradation threshold.

4.1 Introduction

Imperceptibility, usually defined as invisibility or fidelity, represents the highest requirement of watermarking systems. A digital watermark is defined as imperceptible if the original and watermarked images are perceptually indistinguishable and might be fulfilled by sacrificing either robustness, capacity or both. Robustness indicates the ability of the watermarking scheme to resist to different image processing operations. Capacity refers to the number of bits that can be concealed into the cover image without impacting the image quality (Ali et al., 2018).

Unfortunately, there is no standard approach for automatically assessing the amount of noticeable distortion within watermarked images. PSNR and SSIM indices are often cited in the literature. However, they do not reflect the characteristics of the human visual system and perceptual process (Dowling et al., 2007). In exploring the use of digital watermark within medical imaging, the question of how much data could be encoded within the image became an important one to explore and establish trust in the medical environments. This

research investigates this issue. Specifically, it seeks to answer two questions; (i) is there a reliable technique to measure the degradation of images that have been watermarked? (ii) is there a threshold of imperceptibility which can be employed to calibrate an automated image quality measure? The aim of this investigation is to determine a set of guidelines for embedding the watermark, in terms of technique and level of modification/data encoding that ensure that the watermarked image has no perceivable difference to the original. This seeks to define an assessment approach, based on clinicians' assessment, that can be used to validate the watermarked images, before they are inserted into the PACS system, to ensure their integrity and authenticity within the digital medical workflow. This can be achieved by asking experts in reading medical images to detect the noticeable differences in the anatomical structure of images modified by varying techniques and magnitudes.

Several subjective and clinical evaluations have been conducted to inspect the imperceptibility of watermarked images from a quality perspective, and also in terms of the applicability of using them in medical practices (Zear et al., 2018, Das and Kundu, 2013, Zain et al., 2009, Maeder et al., 2008, Dowling et al., 2007). These studies highlighted the ability to recognise the watermarked images and evaluate the acceptability of using them for diagnosis. However, they did not take into consideration the anatomical structures of the organs during the evaluation. In many cases, the embedded watermark may not affect the diagnosis, although it is visible to human eyes. This is a significant issue in watermarking techniques where the transparency of the hidden data is an essential requirement. Therefore, a visual evaluation has been conducted in this research to assess the visualisation of the anatomical details of brain MR images distorted by various payload and techniques to define the perceptual boundary of detecting the modifications. No similar study conducted before to visually assess the watermarked MR images by using standard quality criteria dealing with the visibility of the anatomical details of brain radiographs.

4.2 Study Design

The literature reviewed demonstrated that the wide majority of published studies used physical measures to reach their proposed objectives. In this research, both approaches were adopted, but special attention is given to the visual method since it is more suitable for image assessment within clinical environments (Mraity et al., 2014). However, physical metrics (e.g. PSNR and SSIM) were utilised to support the visual assessment and validate the evaluation scale. Several steps have been utilised for evaluating the visual quality of

watermarked images (Fig. 4.1) to aid in determining the amount of information that can be inserted into the images as a watermark and specify the acceptable level of distortion.

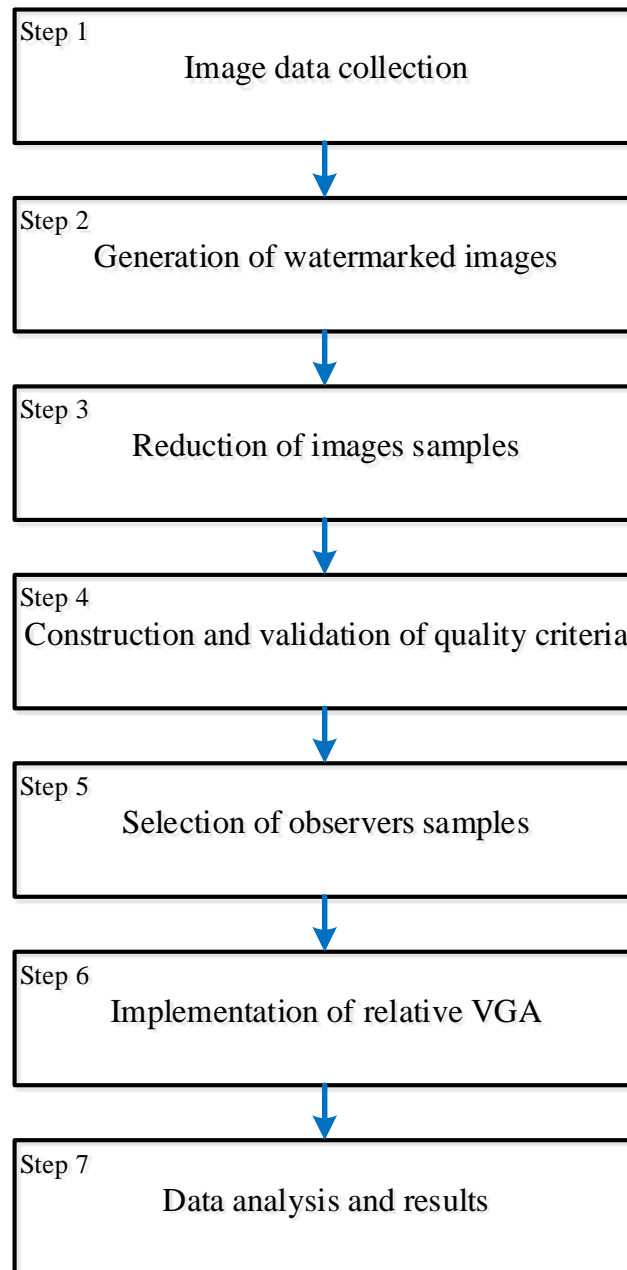


Fig. 4.1: Key steps adopted in this research for visually assessing the imperceptibility of watermarked images. This aids in identifying the noticeable distortion boundary between the watermarked images and therefore defining the amount of information that can be encoded into the images as a watermark and specify the acceptable level of distortion.

A visual assessment trial, based on relative VGA method, has been conducted to evaluate the watermarked images. This approach was selected because it is very sensitive to the slight changes between the images and also it can aid to decrease bias in decision-making (Pelli

and Farrell, 1995). In the relative VGA implementation, all images (watermarked) are compared to a reference image (the un-watermarked image). The reference and modified images are shown to the observers together at the same time on two separated and identical screens. Particular criteria items were utilised to visually rate the images and then determine the differences between the images. A Likert scale (scored from 1 to 5) was used to rate the observers' scores, where a score of 1 indicates "strongly disagree", 2 "disagree", 3 "neither agree nor disagree", 4 "agree", and 5 "strongly agree". A five-point Likert scale was adopted because it offers a more valid measure of the observer's attitude (Likert, 1932). A bespoke, Java-based application was utilised to show the criteria items and the images in random order on twin monitors (Hogg and Blindell, 2012). This software displays the original image on the same screen throughout the assessment process.

4.3 Data Collection

This research uses a dataset provided by MRI unit of Al-Kadhimiya Teaching Hospital (Iraq), from patients' records for use in this research conducted at the University of Salford (Hasan and Meziane, 2016, Hasan et al., 2016a). The dataset contains 165 brain MR images, in DICOM format, taken during the regular diagnostic process. These images have been independently diagnosed and categorised clinically into normal and abnormal pathologies by clinicians of this unit. These MRI slices were acquired using SIEMENS MAGNETOM Avanto 1.5 Tesla scanner and PHILIPS Achieva 1.5 Tesla scanner.

4.4 Generation of Watermarked Images Samples

To produce a set of watermarked images, three reversible watermarking approaches based on Difference Expansion (DE) technique have been applied. These approaches were chosen because they offer high capacity and low computational complexity compared to other reversible methods and are, therefore, suitable as potential techniques for the wider research project (Khan et al., 2014).

1. Tian (2003) (embeds 1-bit per 2-pixels) method, adapted to operate within a 16bpp (signed) colour space.
2. Alattar (2004a) (embeds 3-bits per quad-pixels) method, adapted to operate within a 16bpp (signed) colour space.
3. Extended (within this research) Tian (2003) method (by embedding 2-bits per 2-pixels) and adapted to operate within a 16bpp (signed) colour space.

The objective of these algorithms is to controllably hide information within a defined subset of the image pixels to generate a set of images with various distortion levels, defined by the quality of information encoded and the number of pixels modified. Each image was then assessed against the original, with specific assessment criteria relating to the clarity of features within the images to determine the level of modification at which the perceptual difference became noticeable. These algorithms allow to exactly recover the original image after extracting the watermark, thereby additionally meeting the requirement for a fully reversible process. All the encoding techniques have been applied to eight different brain MR images (16bpp, 512×512 pixels) in DICOM format using MATLAB (Fig. 4.2). These images contain various anatomical structures of the brain and different sizes of ROI and RONI. The ROI comprises the informative part of the image and the RONI includes the non-critical part of the image (Qasim et al., 2018a). This is significant to evaluate the clarity of details within the images after applying a different level of modifications to, therefore, identify the level of modification at which the difference becomes perceptible.

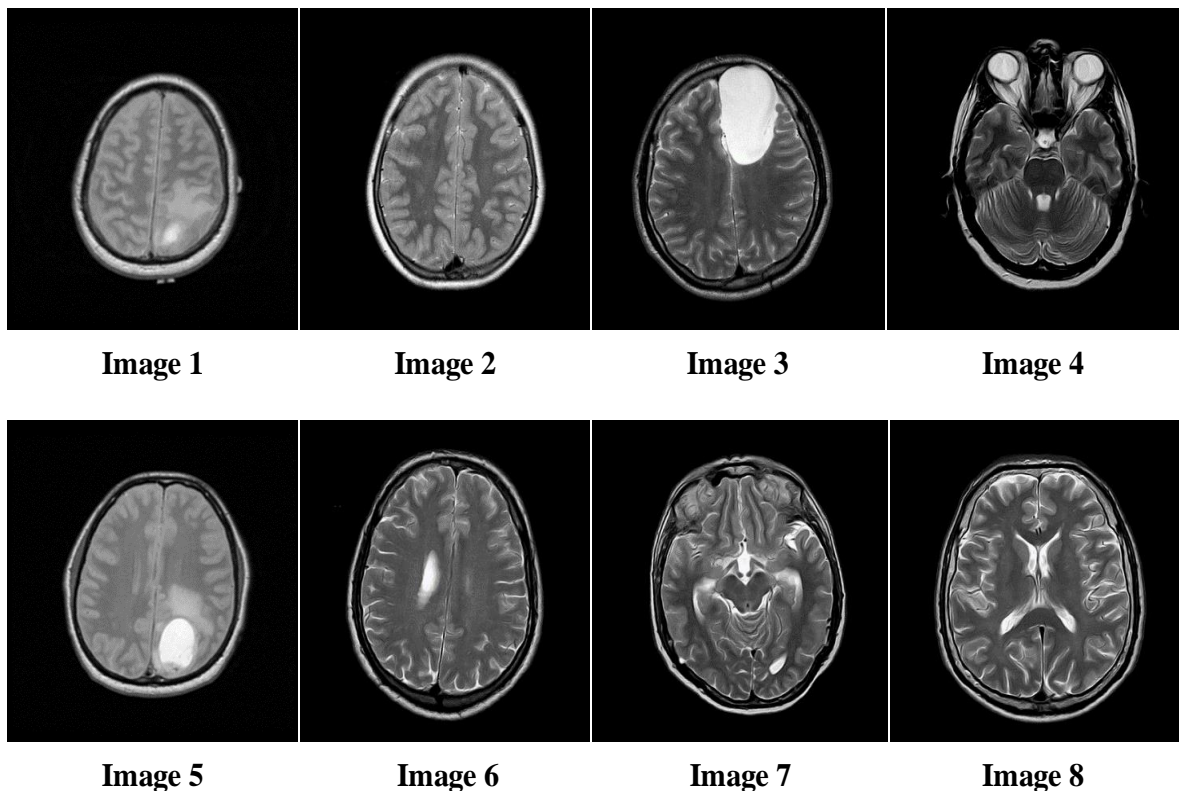


Fig. 4.2: The eight brain MR images in DICOM format (16bpp, 512x512 pixels) used in the proposed approach to generate a set of images with various distortion levels. These images contain various anatomical structures of the brain and different sizes of ROI and RONI.

The embedding process was performed in ten incremental steps. In each step, an additional 10% of the image matrix has been used to embed the watermark, with the entire matrix modified in the final step. Fig. 4.3 shows an example of the changes that occur in the pixels' values for a section of an image (8x8 pixels) after encoding the watermark data using the three watermarking techniques. Sections of the watermarked images after implementing the three watermarking algorithms are also shown in (Fig. 4.4, Fig. 4.5 and Fig. 4.6).

241	231	223	212	198	194	203	208
238	233	224	205	195	207	221	215
235	233	232	233	234	230	221	209
245	240	238	243	240	222	199	191
246	245	237	223	214	204	192	183
223	222	218	200	187	193	205	195
216	201	188	182	189	198	200	195
221	206	192	201	218	207	182	184

A

236	236	219	220	191	189	207	208
233	237	219	211	190	201	228	227
233	234	231	232	234	235	216	219
246	242	237	245	238	234	187	193
246	249	233	228	209	211	186	186
218	225	216	207	180	188	211	205
210	208	181	179	192	197	201	199
220	213	185	193	226	219	169	176

B

240	237	222	210	182	195	212	215
236	235	218	193	173	193	222	229
231	235	233	249	251	240	221	217
245	240	237	256	251	239	194	197
246	251	234	217	199	204	180	181
221	237	229	210	185	187	212	202
208	195	170	174	189	197	201	202
227	209	181	190	225	217	168	173

C

226	245	210	235	176	181	216	210
223	248	209	222	179	187	242	250
228	235	230	232	234	244	206	240
247	244	235	248	234	257	164	195
247	257	225	237	200	223	174	190
208	229	211	221	166	176	223	227
198	222	167	173	198	195	203	206
219	229	170	175	243	245	143	161

D

Fig. 4.3: An example of the modifications of the pixels for a part of an image (8x8 pixels) after encoding the watermark data. **A)** Original pixels, **B)** Modification of pixels using 1-bit per 2-pixels hiding technique, **C)** Modification of pixels using 3-bits per quad-pixels hiding technique, and **D)** Modification of pixels using 2-bits per 2-pixels hiding technique.

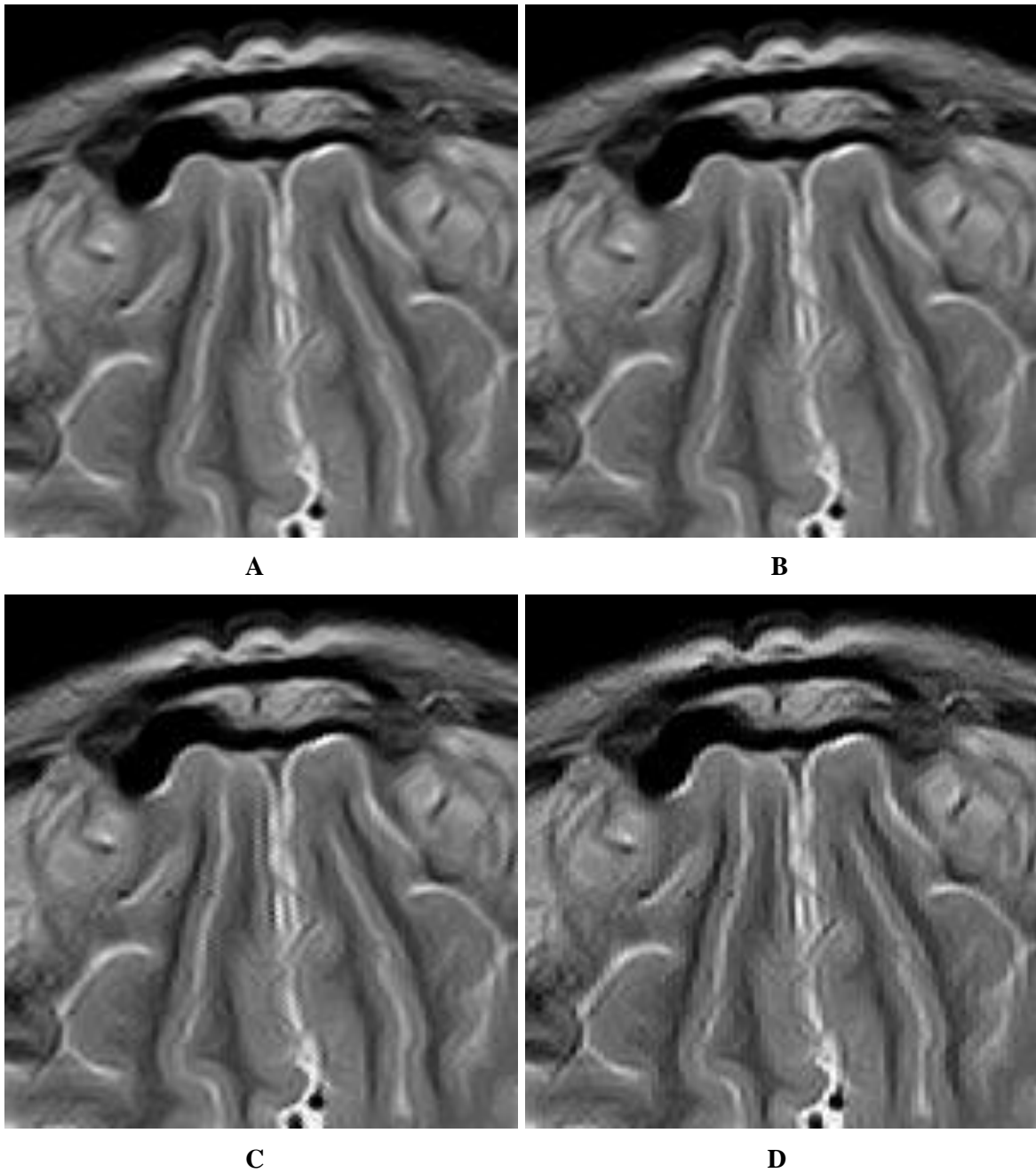


Fig. 4.4: Sections of the watermarked images after implementing the first reversible watermarking technique (1-bit per 2-pixels). **A)** Original image, **B)** Modification of 10% of image pixels (PSNR=83.07 dB), **C)** Modification of 50% of image pixels (PSNR=76.14 dB), and **D)** Modification of 100% of image pixels (PSNR=73.12 dB). The PSNR values reduce, which indicates higher distortion, with the increasing of the number of pixels utilised for carrying the watermark.

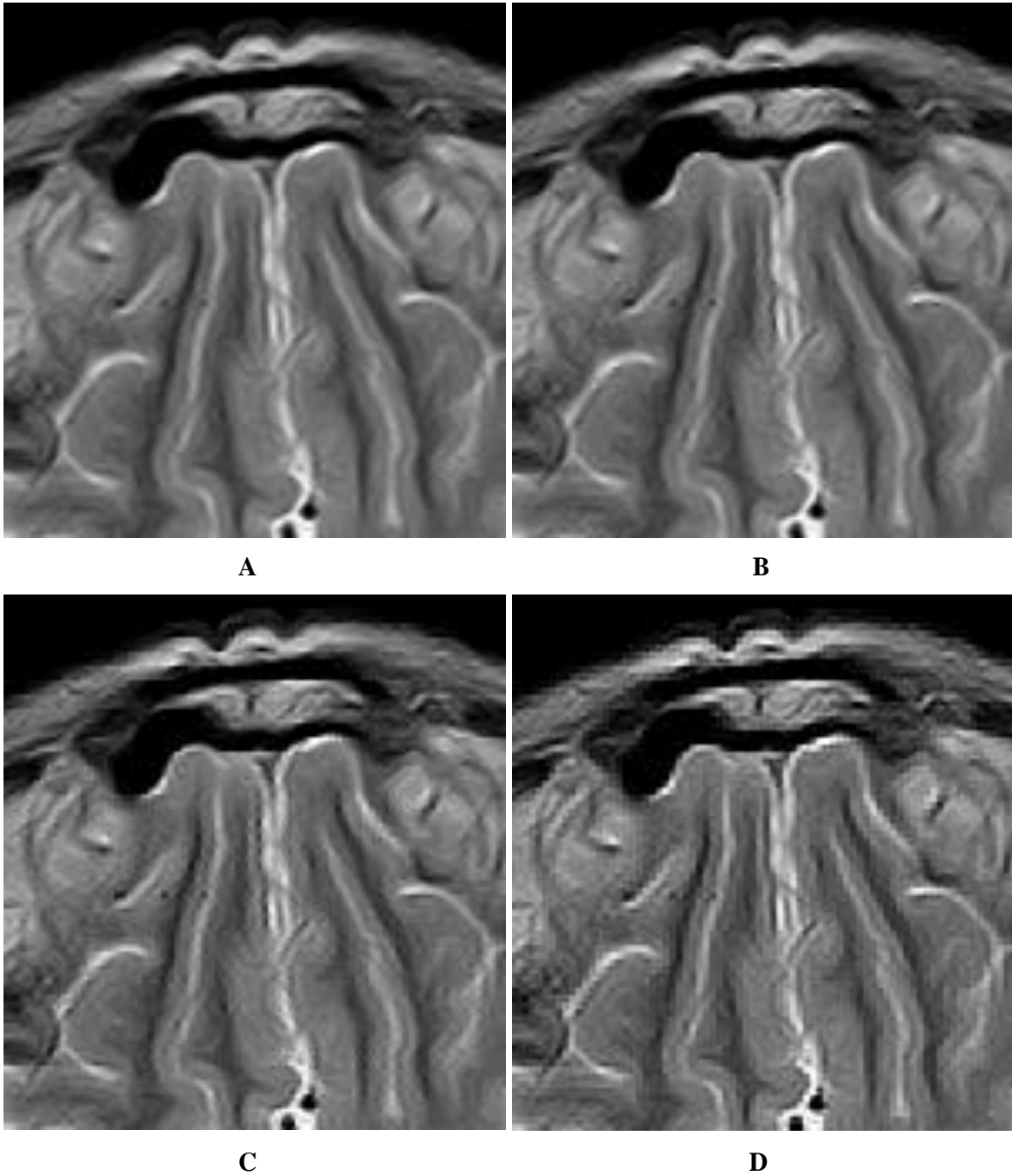


Fig. 4.5: Sections of the watermarked images after implementing the second reversible watermarking technique (3-bits per quad-pixels). **A)** Original image, **B)** Modification of 10% of image pixels (PSNR=80.62 dB), **C)** Modification of 50% of image pixels (PSNR=73.85 dB), and **D)** Modification of 100% of image pixels (PSNR=70.86 dB). The PSNR values reduce, which indicates higher distortion, with the increasing of the number of pixels utilised for carrying the watermark.

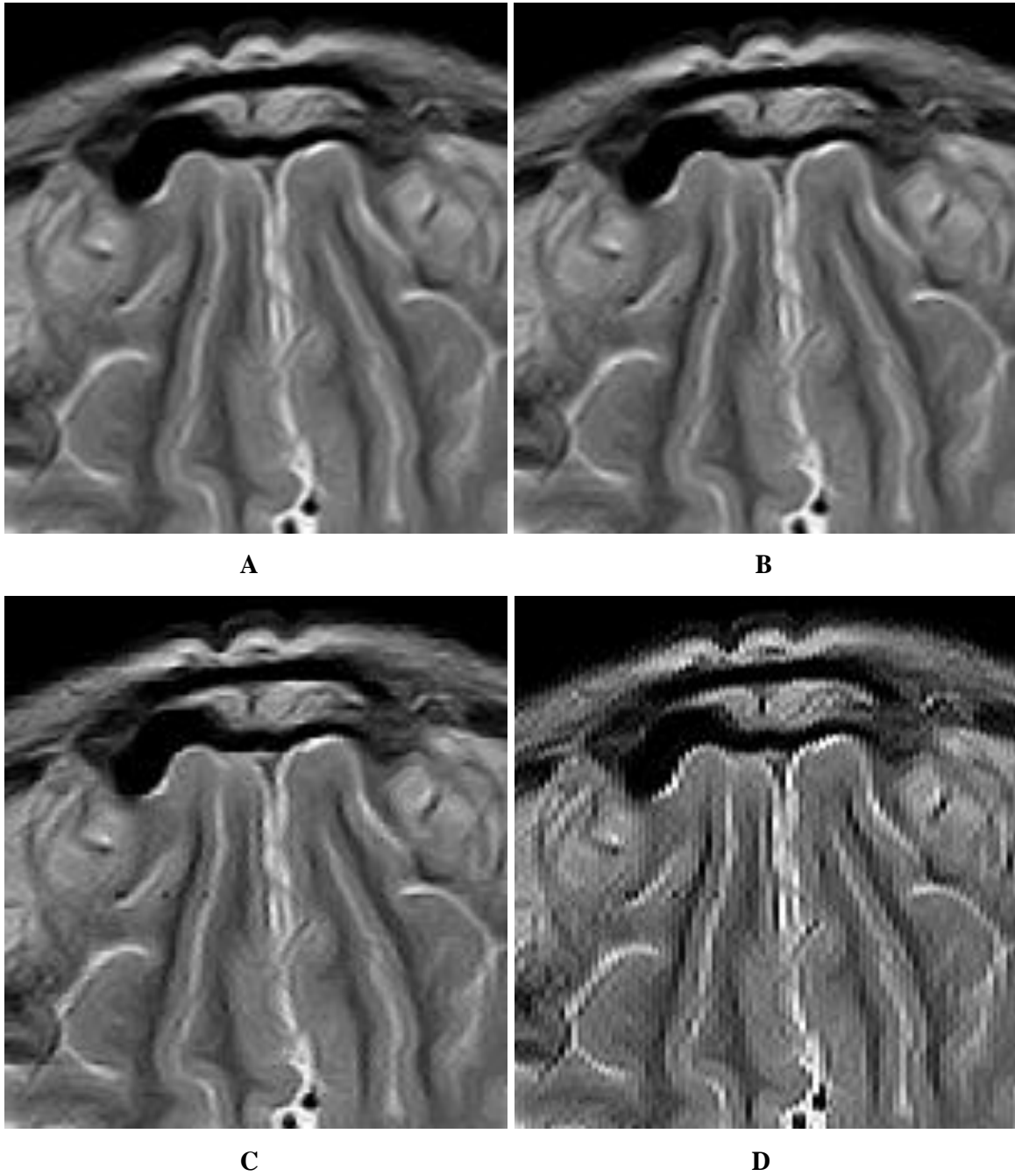


Fig. 4.6: Sections of the watermarked images after implementing the third reversible watermarking technique (2-bits per 2-pixels). **A)** Original image, **B)** Modification of 10% of image pixels (PSNR=73.46 dB), **C)** Modification of 50% of image pixels (PSNR=66.52 dB), and **D)** Modification of 100% of image pixels (PSNR=63.58 dB). The PSNR values reduce, which indicates higher distortion, with the increasing of the number of pixels utilised for carrying the watermark.

After modification, standard PSNR (Fig. 4.7, Fig. 4.8 and Fig. 4.9) and SSIM metrics (Table 4-1, Table 4-2 and Table 4-3) have been utilised to evaluate the distortion and the structural similarity between the original images and their corresponding watermarked versions. Higher PSNR indicates lower distortion, while the SSIM value of 1 denotes that both images are structurally similar. SSIM values for all the executed techniques are either 1 or very close to 1 which denotes that the change in structural information between the tested images is unworthy. In some of these figures, there is a slight discontinuity in the PSNR reduction in the 40-60% region of the image pixel modification. PSNR values depend on which part of the image has been selected to hide the watermark, and this region marks a threshold region in the proportion of pixels within the image ROI and RONI. This difference does not impact on the aim of these algorithms, which is to assess the clarity of anatomical structures of images after encoding a different amount of data to determine the level of modification at which the difference becomes visible in any part of the images.

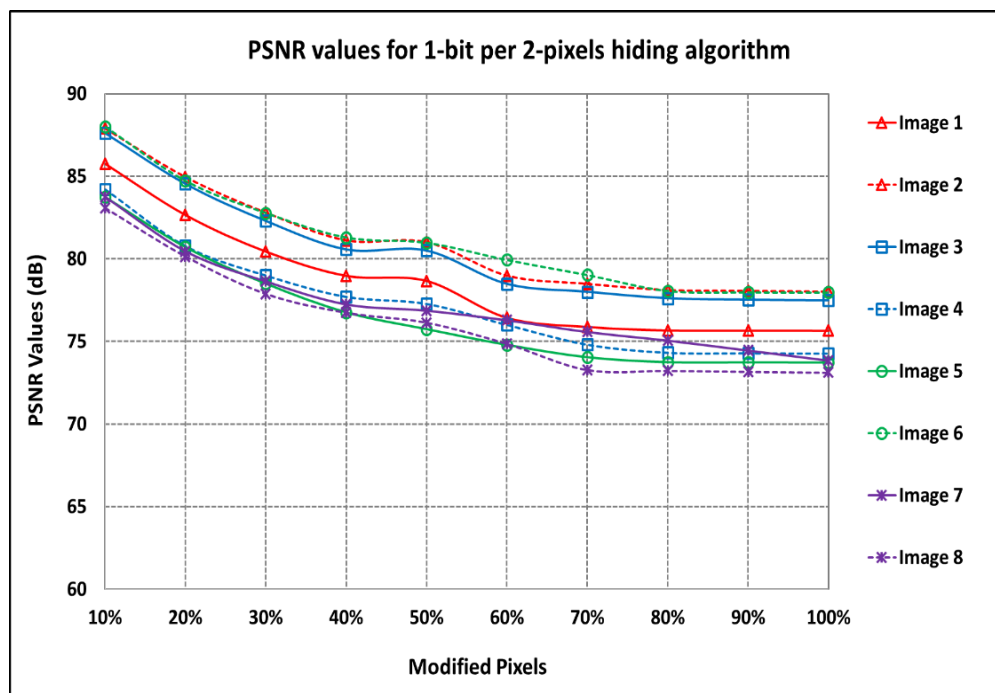


Fig. 4.7: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the first reversible watermarking technique (1-bit per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). PSNR values decrease, which means increased distortion level, with the increasing of the number of modified pixels. The region 40-60% of image pixels marks a threshold region in the proportion of pixels within the image ROI and RONI. Therefore, a slight discontinuity in the PSNR values in these regions can be observed in some images.

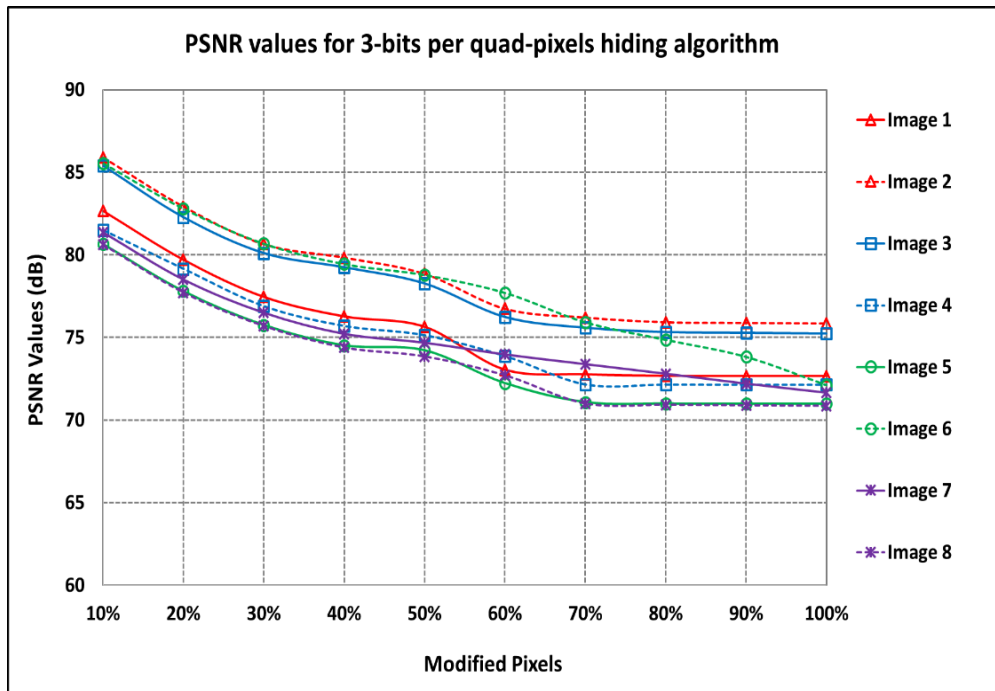


Fig. 4.8: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the second reversible watermarking technique (3-bits per quad-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). PSNR values decrease, which means increased distortion level, with the increasing of the number of modified pixels. The region 40-60% of image pixels marks a threshold region in the proportion of pixels within the image ROI and RONI. Therefore, a slight discontinuity in the PSNR values in these regions can be observed in some images.

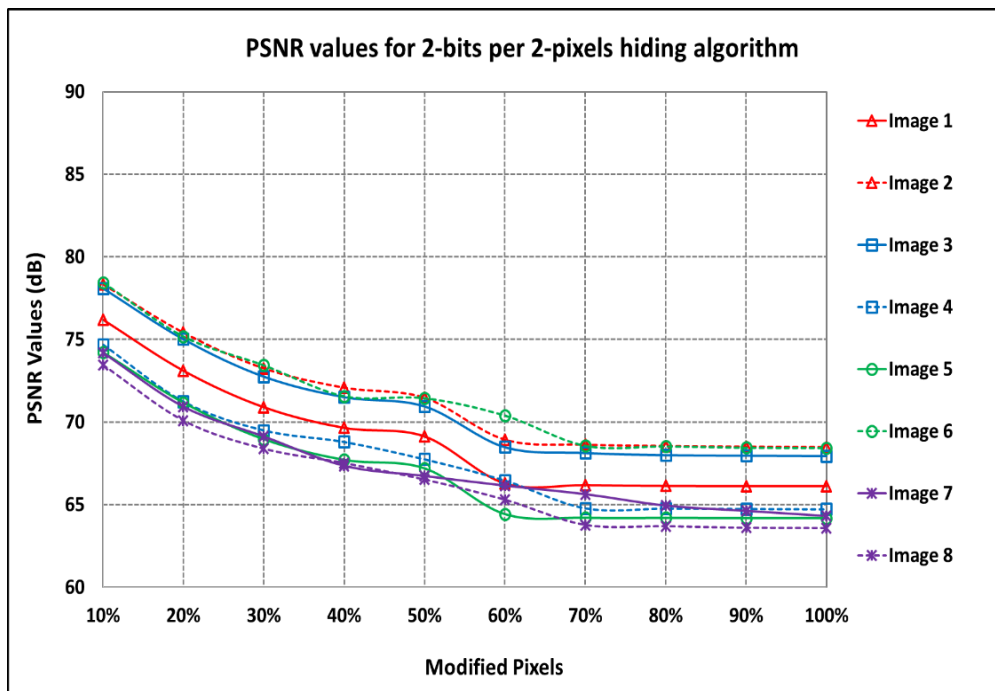


Fig. 4.9: Distortion level (PSNR) between the original eight DICOM images and their corresponding watermarked versions by implementing the third reversible watermarking technique (2-bits per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). The PSNR values decrease, which means increased distortion level, with the increasing of the number of modified pixels. The region 40-60% of image pixels marks a threshold region in the proportion of pixels within the image ROI and RONI. Therefore, a slight discontinuity in the PSNR values in these regions can be observed in some images.

Table 4-1: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the first reversible watermarking technique (1-bit per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). The resultant SSIM values are either 1 or very close to 1 which denotes that the change in structural information between the original and watermarked images is trivial.

Modified pixels	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8
10%	1	1	1	1	1	1	1	1
20%	1	1	1	1	1	1	1	1
30%	1	1	1	1	1	1	1	1
40%	1	1	1	1	1	1	1	1
50%	1	1	1	1	1	1	1	1
60%	1	1	1	1	1	1	1	1
70%	1	1	1	1	1	1	1	0.9999
80%	1	1	1	1	1	1	1	0.9999
90%	1	1	1	1	1	1	1	0.9999
100%	1	1	1	1	1	1	1	0.9999

Table 4-2: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the second reversible watermarking technique (3-bits per quad-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). The resultant SSIM values are either 1 or very close to 1 which denotes that the change in structural information between the original and watermarked images is trivial.

Modified pixels	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8
10%	1	1	1	1	1	1	1	1
20%	1	1	1	1	1	1	1	1
30%	1	1	1	1	1	1	1	1
40%	1	1	1	1	1	1	1	1
50%	1	1	1	1	1	1	1	1
60%	0.9999	1	1	1	0.9999	1	1	0.9999
70%	0.9999	1	1	0.9999	0.9999	1	0.9999	0.9999
80%	0.9999	1	1	0.9999	0.9999	1	0.9999	0.9999
90%	0.9999	1	1	0.9999	0.9999	1	0.9999	0.9999
100%	0.9999	1	1	0.9999	0.9999	0.9999	0.9999	0.9999

Table 4-3: Distortion level (SSIM) between the original eight DICOM images and their corresponding watermarked versions by implementing the third reversible watermarking technique (2-bits per 2-pixels hiding algorithm) to encode the watermark in ten incremental steps (10-100%). The resultant SSIM values are either 1 or very close to 1 which denotes that the change in structural information between the original and watermarked images is trivial.

Modified pixels	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7	Image 8
10%	1	1	1	1	1	1	1	1
20%	0.9999	1	1	0.9999	0.9999	1	0.9999	0.9999
30%	0.9999	0.9999	0.9999	0.9999	0.9999	1	0.9999	0.9998
40%	0.9999	0.9999	0.9999	0.9999	0.9998	0.9999	0.9998	0.9998
50%	0.9999	0.9999	0.9999	0.9998	0.9998	0.9999	0.9998	0.9998
60%	0.9997	0.9999	0.9998	0.9998	0.9996	0.9999	0.9996	0.9997
70%	0.9997	0.9999	0.9998	0.9996	0.9996	0.9998	0.9996	0.9995
80%	0.9997	0.9998	0.9998	0.9996	0.9996	0.9998	0.9996	0.9995
90%	0.9997	0.9998	0.9998	0.9996	0.9996	0.9998	0.9996	0.9995
100%	0.9997	0.9998	0.9998	0.9996	0.9996	0.9998	0.9996	0.9995

4.5 Reduction of Images Samples

The total number of the generated image set is 248 images (8 original and 240 modified images) where each original image has been modified ten times using each of the three algorithms. This presents a significant challenge for the observers, in terms of time and effect, which may also impact on the outcome of the evaluation as tiredness and constancy could become an issue. The images set size was, therefore, reduced to create a subset that covers both extreme cases and presented a wider range of images spanning the anticipated perceptual boundary as defined by the evaluated PSNR values for the image set. In the reduction process, the images were categorised into three groups according to their distortion level in terms of PSNR values; *Group 1* contains the images that have $PSNR \geq 80$ dB, *Group 2* contains the images that have $70 \text{ dB} \leq PSNR < 80$ dB and *Group 3* contains the images that have $PSNR < 70$ dB. For each group, a different number of images was selected by excluding the images that have convergent PSNR values taking into account the inclusion

of all ranges of PSNR (Table 4-4). The new sample size after applying the reduction steps includes 117 images (8 original and 109 modified images).

Table 4-4: The selected watermarked images after applying the reduction strategy. The images were categorised into three groups based on their PSNR values. For each group, a different number of images were chosen considering covering all ranges of PSNR values.

Image set	Total number of watermarked images			Selected images		
	Group 1 PSNR ≥ 80 dB	Group 2 PSNR [70-80) dB	Group 3 PSNR < 70 dB	Group 1 PSNR ≥ 80 dB	Group 2 PSNR [70-80) dB	Group 3 PSNR < 70 dB
Image 1	4	19	7	4	7	3
Image 2	8	17	5	4	7	2
Image 3	8	17	5	4	8	2
Image 4	3	19	8	3	7	4
Image 5	3	19	8	3	7	4
Image 6	8	18	4	4	6	2
Image 7	3	19	8	3	7	4
Image 8	3	19	8	3	6	5
Total	240			109		

4.6 Construction and Validation of Quality Criteria Items

Content validity indicates the adequacy of the selected criteria items to cover the subject and then to achieve the purposes of the investigation, items that are not relevant to the concept being evaluated could drive a wrong in the analysis, and therefore wrong conclusions may be drawn (McDowell, 2006). Two major recommendations have been suggested to ensure the investigation validity; utilising large numbers of items and employing items created from previous studies (Mraity et al., 2014). Unfortunately, no standard criteria for MR images can be found in the literature that can be adopted for this investigation. Therefore, the criteria items used in this research, which have been identified as fundamental to evaluate the quality of brain scans, were taken from various sources dealing with CT images. These criteria have been selected to fit the anatomical structure details of brain MR images. European guidelines on quality criteria for CT images (Menzel et al., 2000) have been recognised as one of the

essential sources for medical images (Section 2.5.2.4). These guidelines concentrate on the visibility of anatomical structures within the clinical image and how this helps in getting a correct diagnosis (Seeram et al., 2014).

Additional criteria were drawn from a published study that has utilised brain image as an area for the study was the second source for generating quality measures (Ledelius et al., 2014). In addition, several items have been created to examine some cases that may appear as a result of image processing operations (e.g. encoding the watermark data). Within this research, eight items have been constructed to assess the image quality and measure the distortion level between the experimental images, where items 1 to 7 refer to the reproduction of the structure, and item 8 estimates the overall image quality (Table 4-5). These scale items were revised by an expert (professor of radiography) alongside researchers to ensure their validity and applicability.

Table 4-5: Image quality criteria adopted within this research to assess the visualisation of the anatomical details of brain MR images. Criteria items from 1 to 7 refer to the reproduction of the anatomical structure of the brain while criterion 8 evaluates the overall visual image quality.

Criterion no.	Description
1	There is a visually sharp reproduction of the border between white and grey matter
2	There is a visually sharp reproduction of the mesencephalon (midbrain)
3	There is a visually sharp reproduction of the cerebrospinal fluid space over the brain
4	The superior sagittal sinus is clearly distinguishable
5	The presence or absence of the tumour is clearly identifiable
6	There are no noticeable regular/periodic intensity patterns in the image
7	There are no noticeable irregular/non-periodic intensity artefacts in the image
8	The image quality is adequate for diagnosis

4.7 Ethical Issues

When research needs human participation, special attention must be given to volunteers' rights (Polit and Beck, 2004). An ethical approval provided by the University of Salford was sought for this research (Appendix I). This is essential to enable the participants to evaluate the images. All volunteers in this study were asked to sign a consent form before conducting any related task (Appendix II).

4.8 Selection of Observer

The number of participants is a significant issue in scale validation as it is directly related to the number of random errors that may appear. Reliability scale and factor analysis utilised for content validation need a small number of participants (Mraity et al., 2014). According to the European guidelines on quality criteria, at least two observers should examine the assent of each image with the quality criteria individually (Menzel et al., 2000, EC., 1996). Rubin (1996) stated that five (or even three in some cases) of such observers are sufficient in many situations. Some recommended a rule of five members per item (Tabachnick and Fidell, 2013). Consequently, five qualified radiographers from the University of Salford were invited to assess the images. This is considered to be adequate due to this investigation being concerned with the differences in the anatomical structures of these images and their quality, not for diagnostic purposes.

All observers (three males and two females) are experienced in radiographers and their age range from 30 to 40 years. Two observers have PhD in diagnostic radiography while the other three have a Master's degree in diagnostic radiography. At the time of the assessment, three of the observers had more than eight years' experience as radiographers while the other two had three years. To confirm that all the observers have a normal visual function, they were asked whether their eyesight was a typical vision (20/20), the date of their latest eyesight test and if their eyesight was corrected with glasses or contact lenses. All observers had checked their eyesight within the last 12 months, and they had a typical vision (20/20), two of the observers used glasses, and the rest (three) did not require any eyesight correction. The participated radiographers held qualifications in image reading and reported that they have substantial experience of visually assessing medical images quality for research purposes.

4.9 Implementation of Visual Assessment

Under the visual assessment approach, expert medical image readers (radiographers) were asked to visually compare the images and evaluate the differences through an objective question set (criteria). This seeks to determine the human perceptual boundary and identify where that coincides with the context of the PSNR. The relative VGA trial was conducted with five qualified radiographers on an image set comprising 117 (8 original and 109 modified) images. Observers were required to evaluate each original image against its modified variants by giving their opinion about eight criteria items for each image. This trial was conducted in a room with PCs and computer screens devoted to medical image analysis at the University of Salford. A five-point Likert scale was utilised to rank criteria items, ranging from 1= strongly disagree to 5= strongly agree, producing in a digital form for individual scores. Before starting any evaluation process, it was considered necessary to fulfil the following steps:

- All the criteria were explained to the observers.
- Two 23.2 inches Liquid Crystal Display (LCD) flat monitors were used to view the images. Both screens were calibrated to DICOM Grayscale Standard Display Function (GSDF) to imitate the clinical requirements and optimise the displaying mode that is recommended for obtaining reliable detection and analysis (Norweck et al., 2013).
- The surrounding light was kept dimmed at 20-38 Lux throughout the evaluation operation.
- No time restrictions were imposed on the observers during images assessing.
- No restrictions were imposed on the distance between the observers and monitors.
- No magnification glass was allowed to use by the observers.
- Observers were blinded to image acquiring factors and watermarking techniques.
- No image manipulation was allowed.
- During the evaluation process, the images were randomised to minimise observers' bias.

The whole experiment for each observer took approximately three hours to complete the assessment. Four thousand, six hundred and eighty (4680) scores were gathered from the participants, involving their ratings on the eight criteria items for all experimental images.

4.10 Experimental Results and Discussion

4.10.1 Approach Reliability

After the data have been collected, it is now essential to test the internal reliability of each experimental image to identify the scores that are inconsistent with the measurement. These items can then be excluded to improve assessment validity and reliability (Ho, 2006). Cronbach's alpha is the most common statistical method utilised to measure internal consistency. A lenient cut off point for the Alpha coefficient is 0.6 (Cronbach, 1951). However, an acceptable reliability value has been recommended to be 0.7 and greater (Streiner et al., 2015). Calculating the internal reliability of each experimental image is superfluous due to many images have approximately the same distortion level and scores. Therefore, the Alpha coefficient values for the images located within the same range of PSNR have been measured. The relative VGA approach compares the original images with each other. This is necessary to provide a clear impression of the validity of the assessment process, especially on images that are slightly distorted. In this case, the PSNR values are infinity (Inf) because the MSE value is 0 as there is no numerical difference between the images. All Cronbach's alpha values for the observers' scores are above 0.7 (Table 4-6). This ensures the reliability of the conducted trial.

4.10.2 Data Analysis and Results

The outcomes of both assessments (visual and physical) have been connected to identify the visual degradation boundary in which the observers can identify the noticeable differences between the tested images. The observers' ratings have been only linked to the modified images PSNR values due to the SSIM values of all modified images are either 1 or very close to 1. This seeks to determine to what level of modification the distortion is invisible to the observers. The overall observers' scores for the eight criteria items have been categorised according to the images PSNR values (Fig. 4.10) to define a collective assessment of the perceptual degradation boundary that applied to the generalised case for all images. In addition, the utilised five-point Likert scale was reduced to three-point by gathering the 'strongly disagree' and 'disagree' scales to one scale (disagrees) and gathering the 'strongly agree' and 'agree' scales to one scale (agrees) (Fig. 4.11). This contributes to formulating the final conclusion for identifying the imperceptibility threshold in which the observers cannot recognise any differences between the original and watermarked images.

Table 4-6: Cronbach’s alpha values for the observers’ scores on all experimental images. This checks the internal reliability of each experimental image to exclude the scores that are inconsistent with the approach. An acceptable alpha value has been recommended to be 0.7 and greater.

Images PSNR	Alpha coefficient
Inf	0.928
[86-88)	0.900
[84-86)	0.934
[82-84)	0.903
[80-82)	0.906
[78-80)	0.798
[76-78)	0.776
[74-76)	0.815
[72-74)	0.799
[70-72)	0.776
[68-70)	0.838
[66-68)	0.732
[64-66)	0.794
[63-64)	0.874

In the five-point (Fig. 4.10) and three-point (Fig. 4.11) plots of the Likert assessment for image quality, the range in which there is no uncertainty over the perception of no difference between the source and modified images extends down to PSNR=82 dB. Uncertainty over whether a difference is noticeable starts at around PSNR=80 dB (there are no reports of a perceived difference, but some observers, 2.29% of the overall scores, report they are uncertain of whether there is a difference or not). Considering the mean scores for the criteria, there is also strong evidence indicating that there is no opportunity of detecting any discernible difference for images that have $PSNR \geq 82$ dB. This suggests, for brain MR images watermarking applications, that if a watermark is applied to the 16bpp DICOM image, a subsequent assessment of PSNR=82 dB or greater would mean that there would be no reason to suspect that the watermark would be visually detectable.

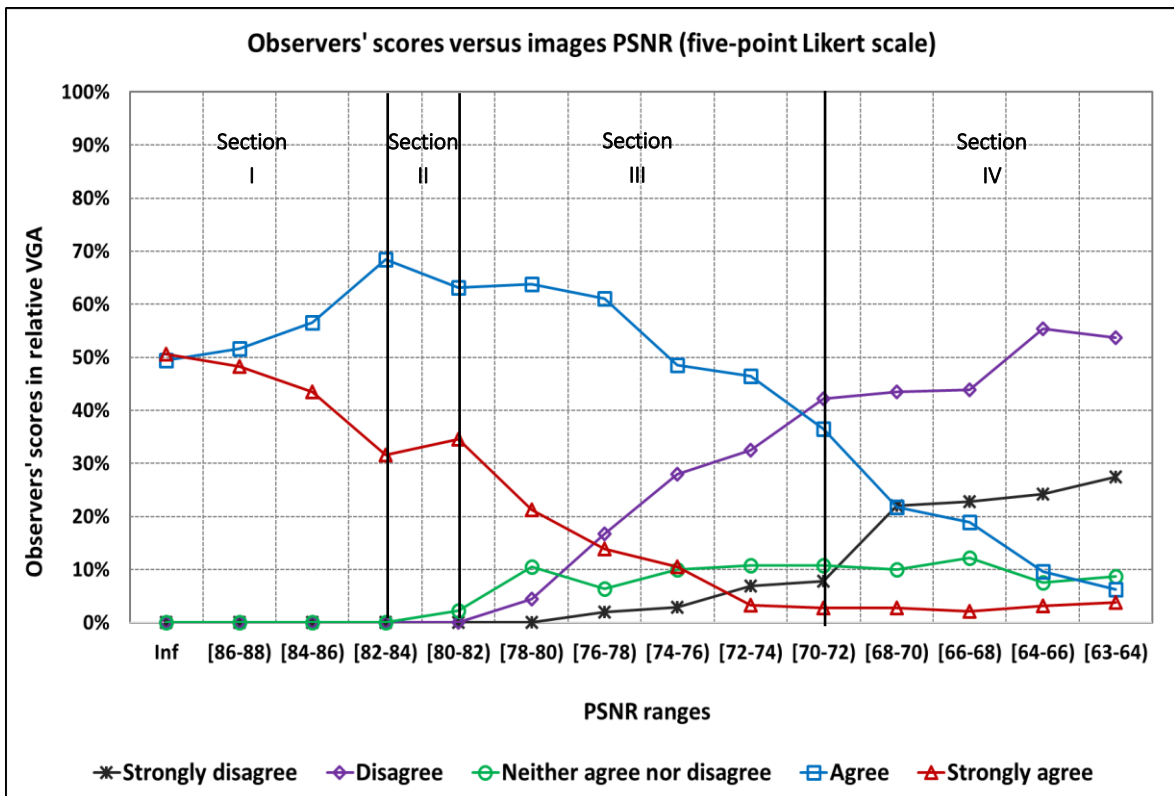


Fig. 4.10: The overall observers' scores for the eight criteria items against images PSNR values by using five-point Likert. The range in which there is no doubt that there is a noticeable difference between the original and modified images extends down to PSNR=82 dB (Section I). Uncertainty over whether a difference is noticeable, 2.29% of the overall scores, starts at around PSNR=80 dB (Section II). Report on existing a noticeable difference between the images starts from PSNR<80 dB (Section III). The certainty that there is a noticeable difference between the images starts at around PSNR=70 dB (Section IV).

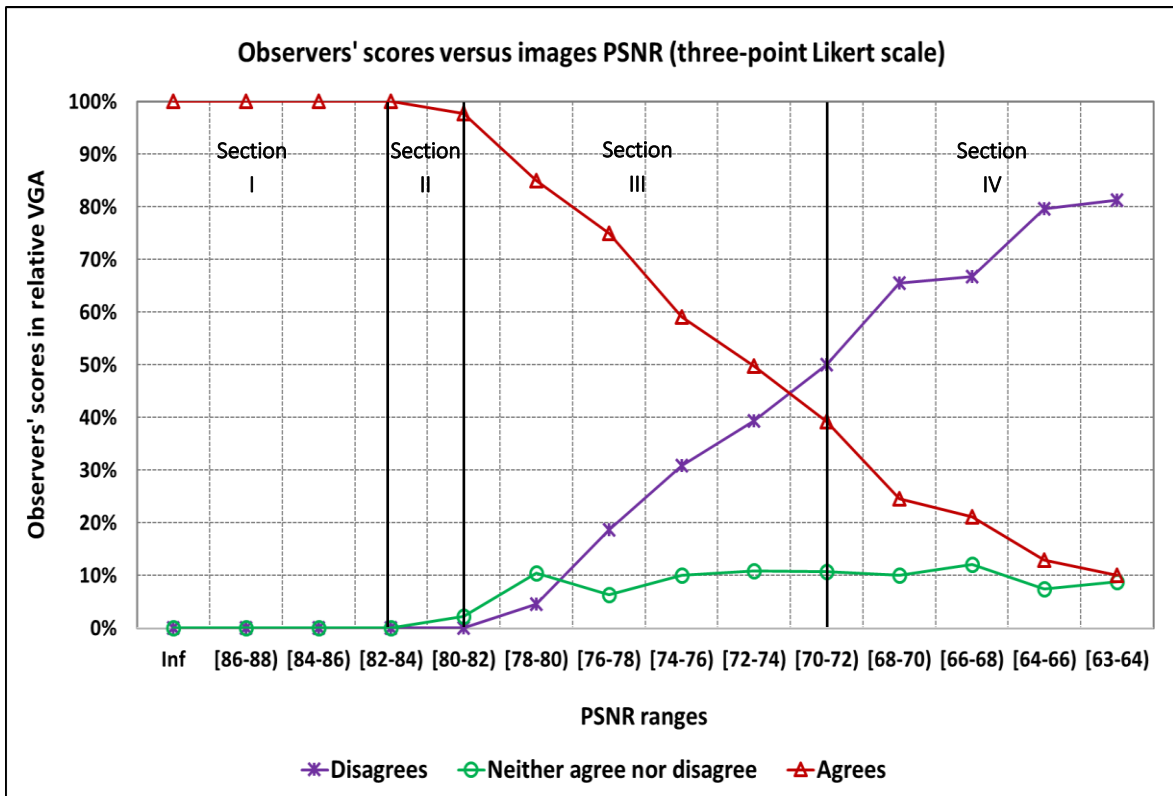


Fig. 4.11: The overall observers' scores for the eight criteria items against images PSNR values by using three-point Likert. The five-point Likert scale has been reduced to three-point to draw the final conclusion and identify the imperceptibility threshold. The range in which the observers cannot perceive any differences between the original and modified images extends down to PSNR=82 dB (Section I). Uncertainty over whether a difference is noticeable, 2.29% of the overall scores, starts at around PSNR=80 dB (Section II). Report on existing a noticeable difference between the images starts from PSNR<80 dB (Section III). The certainty that there is a noticeable difference between the images starts at around PSNR=70 dB (Section IV).

By considering the results of relative VGA trial against the actual PSNR measured for the image set (Table 4-7), this suggests that technique 3, which modifies 2-bits for every 2-pixels, is visually detectable in every case. The other implemented techniques performed better, with technique 1 (1-bit per 2-pixels) being undetectable visually when 10% of the pixels are modified. This equates to hiding 1.6KB of payload into the image. The size of the DICOM header data is highly variable and depends on the imaging modality, capture device and institutional practice for the composition of the data encoded (Varma, 2012). Disconnection of the image from this header, or obliteration of the header renders the image useless for medical purposes, so encoding this information as the watermark is highly advantageous. While there are few studies on the typical size of the header, one does suggest that data in the range 0.5-4 KB (per image) is normal, depending on the encoding scheme and Application Programming Interface (API) used (Ismail et al., 2014). Even the best case

for these encoding techniques (technique 1 at 20% of pixels modified - 3.2 KB of payload, technique 2 at 10% of pixels modified - 2.4 KB of payload) is insufficient for the maximum full header to be used as the watermark. However, careful selection of the metadata fields and compression of the raw metadata could bring this down to an achievable descriptor of the patient data, sufficient to connect image and metadata, for the watermark payload.

Mean and Standard Deviation (SD) were also computed to measure the observer evaluation of each score and to assess confidence in statistical conclusions (Fig. 4.12 and Fig. 4.13).

Table 4-7: Aggregated (mean) PSNR values for all experimental images with the SD considered. Green cells denote the region in which no perceivable difference in the images was noticed, orange, where some uncertainty exists.

Modified pixels	Technique 1 1-bit per 2-pixels		Technique 2 3-bits per 4-pixels		Technique 3 2-bits per 2-pixels	
	Mean+SD	Mean-SD	Mean+SD	Mean-SD	Mean+SD	Mean-SD
10%	87.58	83.43	85.24	80.66	78.04	73.86
20%	84.47	80.27	82.33	77.89	74.95	70.58
30%	82.36	78.22	80.13	75.80	72.88	68.70
40%	80.76	76.85	79.13	74.52	71.50	67.55
50%	80.59	76.20	78.29	74.07	71.04	66.76
60%	78.90	75.05	76.61	72.51	69.07	65.04
70%	78.28	74.00	75.65	71.37	68.22	64.26
80%	77.70	73.75	75.15	71.27	68.09	63.91
90%	77.60	73.62	74.84	71.12	68.05	64.00
100%	77.56	73.46	74.55	70.82	68.03	63.92

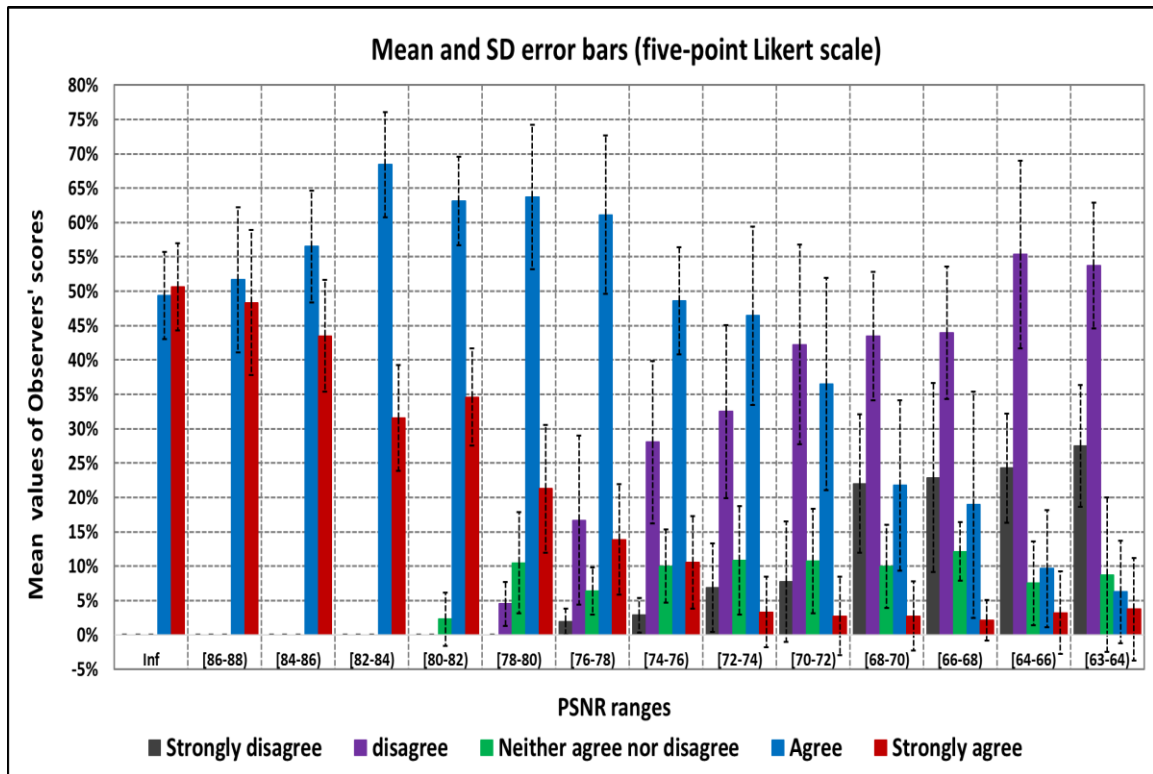


Fig. 4.12: The mean and SD error bars for the overall observers' scores for the eight criteria items against images PSNR values by using a five-point Likert scale. This contributes to indicate the error or uncertainty in the reported measurement to give a general idea of how precise the measurement is.

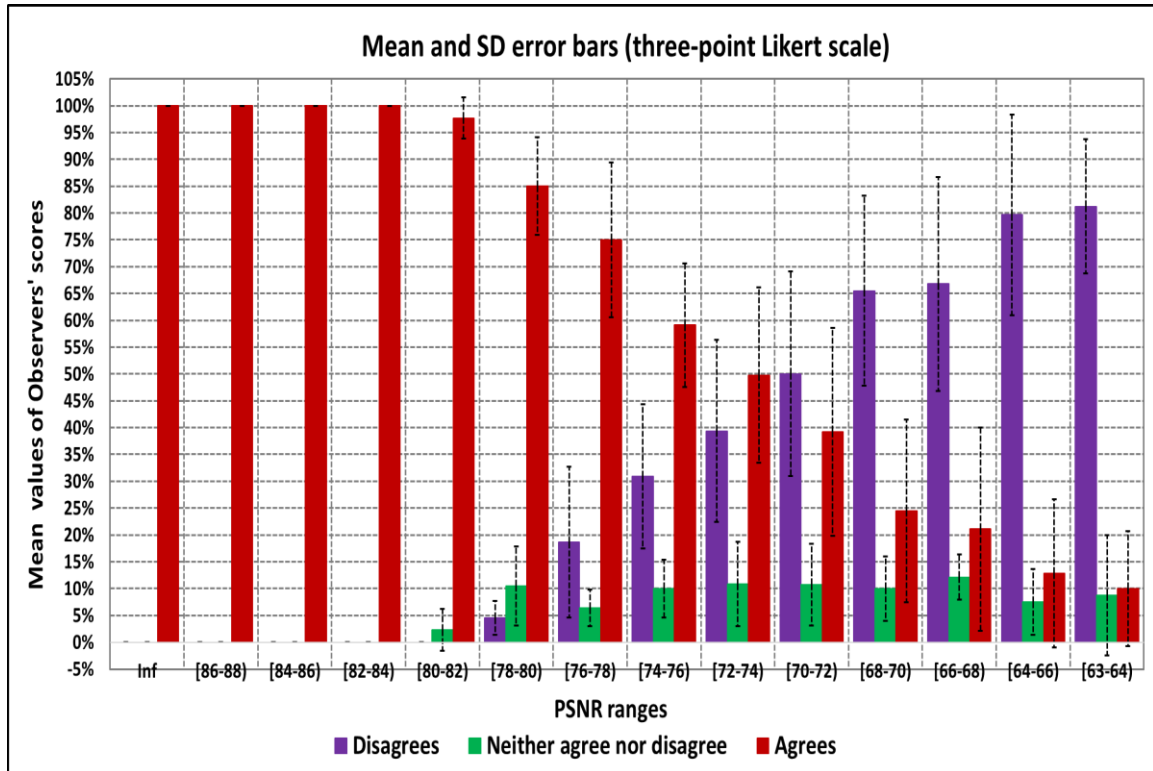


Fig. 4.13: The mean and SD error bars for the overall observers' scores for the eight criteria items against images PSNR values by using a three-point Likert scale. The certainty that there is no noticeable difference between the images extends down to PSNR=82 dB (SD error bars= 0). Uncertainty over whether a difference is noticeable starts at around PSNR=80 dB.

4.10.3 Comparison with Other Approaches

Although comparing the performance of the proposed approach is difficult due to the lack of investigations that used standard criteria to evaluate the visualisation of the anatomical detail of brain MR images, the proposed approach has been compared to other studies stated in the literature (Table 4-8).

In Zain et al. (2009) approach, the radiologists diagnosed a random collection of original and watermarked images, which was then compared to the ground truth diagnosis. The study did not take into account the visual distortions of the anatomical details of the images that can appear without impacting the diagnosis. The aim of Giakoumaki et al. (2010) and Das and Kundu (2013) approaches is to define the difference between original and watermarked images not to determine the level of visual perception of distortion. Furthermore, the number of assessors is small which may affect the evaluation outcomes and therefore leads to wrong conclusions. In Dowling et al. (2007), Maeder et al. (2008), and Zear et al. (2018) approaches, the perception of distortion boundaries have been determined through identifying the differences between the original and modified images. A significant difference in the values of imperceptibility threshold can be observed due to the large variability in the observers' scores. This happened due to the observers do not have experiences to conduct similar investigations. Moreover, the sample size of images used in these studies to determine the perception threshold is small. Therefore, increasing the images sample size and using further calibration have been suggested for future research.

The proposed approach has identified the threshold at which the observers can detect the slight differences between the anatomical details of the brain. Qualified radiographers have evaluated the differences in the anatomical structure between the original and manipulated images based on universal criteria. The result of imperceptibility threshold is much higher than the approaches under comparison, and no variability has been observed in the observers' scores. This is due to adopting standard criteria for evaluating the anatomical details of the brain and involving participants who have experiences in conducting related investigations.

Table 4-8: Performance comparison of the proposed approach against approaches identified in the literature based on various criteria. The proposed approach has identified a high imperceptibility threshold in comparison to the other approaches due to using standard criteria for evaluating the anatomical details of the brain and involving participants who have experiences in conducting related investigations.

Approach	No. of images	Images modalities	Images format	No./Experience of observers	Standard criteria?	Objective assessment	Subjective assessment
Dowling et al. (2007)	60	MRI CT	DICOM	20 volunteers	No	PSNR (30-75 dB)	PSNR threshold (57 dB)
Maeder et al. (2008)	32	Mammogram	-	12 semi-skilled researchers	No	PSNR (44.59-64.92 dB)	PSNR threshold (45.5 dB)
Zain et al. (2009)	225	X-rays Ultrasound CT	-	3 radiologists (each evaluated 75 images)	No	Average PSNR (54.15 dB)	No effect on medical diagnosis
Giakoumaki et al. (2010)	120	CT MRI MRA Ultrasound Dermatological Radiological	JPEG BMP TIF	2 radiologists	No	PSNR (52.78±0.08-72.64 ±0.09 dB)	No variation detected
Das and Kundu (2013)	430	CT MRI USG X-ray Mammogram	BMP TIF GIF DICOM	1 clinician	No	Average PSNR (42.16-44.8 dB)	No noticeable difference found
Zear et al. (2018)	6	CT	-	6 persons	No	PSNR (27.29-43.88 dB)	PSNR threshold (27.29 dB)
Proposed	117	MRI	DICOM	5 radiographers	Yes	PSNR (63.58 -87.99 dB)	PSNR threshold (82 dB)

4.11 Chapter Summary

This study has conducted a relative VGA trial to determine the range of modification, for brain MR images, within which changes to the image data (pixels) are unperceivable to the observer. This seeks to define a perceptual boundary, below which change is noticeable, to determine heuristic guidelines for the method of watermarking and the level of modification that can be applied to encode a known magnitude of payload data in an imperceptible manner. Relating this to objective measures for image fidelity (PSNR) is then undertaken to define quantitative criteria to guide the selection of watermark encoding technique and enable an objective post modification assessment of the watermarked image to ensure the condition of imperceptibility is met. The outcomes propose that, when applying digital watermarking to medical images, the modification of the images to a level of PSNR=82 dB or greater, between the reference and watermarked images, is undetectable to all observers, and modification level to a PSNR=80 dB should not be noticeable in the vast majority of cases. This translates to a watermark payload of 1.6Kb (approx.) in the 512x512 pixel (16bpp grayscale) images used in the study. While this is insufficient to encode a typical DICOM header collection of metadata into these images, careful selection of the metadata components and compression should enable sufficient information to be encoded to ensure the image pixel data can be re-connected to the patient record, if required, and enable the authenticity and integrity evaluation that the wider research is seeking. These images are relatively small, by modern standards, and are a specific requirement of the research, but more typical 1024x1024 images should enable a potential 4x increase in payload, which is close to the typical magnitude of a single image DICOM header.

Providing a reliable and dependable method for digital watermarking of images within the medical imaging workflow is intended to enhance the security of data within the complex document management pipeline, thereby reducing the risk of data being compromised and enhancing trust in the medical imaging system. The definition of a reversible and unperceivable watermark, which can be evaluated by objective measures before the image is released into the clinical process, ensures that security can be achieved and, importantly, the original (raw) image data can always be recovered when required for critical activities such as diagnosis.

CHAPTER FIVE

Reversible Watermarking Approach Based on Difference Expansion Technique

Reversible and imperceptible watermarking is recognised as a robust approach to confirm the integrity and authenticity of medical images and verify that alterations can be detected and tracked back. In this chapter, a novel blind reversible and imperceptible watermarking approach is presented to detect both intentional and accidental changes within brain MR images. The scheme segments images into two parts; ROI and RONI. Watermark data, which includes both authentication and integrity information, is encoded into the ROI part using reversible watermarking based on the Difference Expansion (DE) technique. Experimental results demonstrate that the proposed watermarking method, whilst fully reversible, can also realise a watermarked image with low degradation for reasonable and controllable embedding capacity. This is fulfilled by concealing the data into ‘smooth’ blocks, which indicates the regions that have small differences between the adjacent pixels’ values, inside the ROI section, and through the elimination of the large location map required for extracting the watermark and retrieving the original image at extraction. The proposed approach delivers highly imperceptible watermarked images evaluated through implementing a visual trial based on relative VGA assessment. This trial defines the level of modification that can be applied to medical images without perceptual distortion. Integrity and authenticity of medical images are also ensured through detecting subsequent changes enacted on the watermarked images. This enhanced security measure, therefore, enables the detection of image manipulations, by an imperceptible approach, that may establish increased trust in the digital medical workflow.

5.1 Introduction

Irreversible watermarking methods encode watermark data into the entire cover image by replacing some of its details, typically Least Significant Bits (LSBs), or degrading some details when using lossy compression methods (Li et al., 2018). These techniques are not suitable for medical domains as they are not accepted by radiologists with unmodified images being favoured for medical investigations (Tan et al., 2011). Medical images have two parts; ROI and RONI. ROI region comprises the informative part of the image which is utilised for diagnosis and must be conserved without any degradation. However, RONI

includes the non-critical part of the image (e.g. background). Occasionally this region may contain grey level parts of slight interest (Parah et al., 2017). Using the ROI part for hiding the watermark may deform the pixel intensities in this section which may lead to misinterpretations and consequently misdiagnosis. RONI watermarking techniques embed data in regions that are considered unimportant in medical examination. However, this can only be performed if a RONI exists. The amount of data, that can be embedded, highly depends on the RONI size and ROI may not be preserved against malignant operations (Qasim et al., 2018a).

In medical applications, there are typically strict restrictions on data reliability that preclude any modifications, such as watermarking, that have a perceptible visual impact. Modifying a patients' medical image could affect their life by causing errors in reading and interpretations, which may lead to incorrect diagnosis and treatment. Therefore, fully reversible watermarking techniques, which can completely recover both the original unmodified image and the embedded watermark, are developed. Reversible watermarking approaches can be categorised into four groups (Section 3.3.3); compression based (Arsalan et al., 2012, Celik et al., 2005), histogram modification based (Gao et al., 2017, Nguyen et al., 2015, Khan and Malik, 2014), quantisation based (Ko et al., 2012b, Ko et al., 2012a) and Difference Expansion (DE) based (He et al., 2017, Lei et al., 2014). Reversible watermarking based on the DE technique are recommended by many recent studies, and typically exceed alternate reversible methods in terms of higher payload capacity and lower complexity (He et al., 2017, Roček et al., 2016, Lei et al., 2014). The weakness of the DE watermarking technique is the reduction of the hiding capacity due to the need for a location map denoting the pixels where data is embedded. This location map needs to be encoded alongside the watermark into the image because it is required to extract the encoded data at extraction. This huge additional information reduces the embedding capacity and increases the distortion level of watermarked images (Qasim et al., 2018a).

In this chapter, a novel reversible watermarking approach based on the DE technique is developed which has the ability to confirm the authenticity and integrity of medical images and can be used to detect manipulations. The proposed approach automatically segments the image into two parts: ROI and RONI with the watermark encoded into smooth blocks (3x3 pixels) inside the ROI. The main contributions of the proposed approach are:

- Hiding of the watermark in smooth regions inside the ROI part of the image. Smooth regions are defined as blocks that have the least differences between their pixels' values. This makes the deformation less visually perceptible.
- Evaluation of image distortion through a visual trial, based on relative VGA. This enables identification of the level of modification that can be applied to medical images before modification is visually perceptible.
- Retrieval without location mapping. This significantly enhances hiding capacity whilst also reducing potential image degradation.

5.2 Proposed Scheme

In this research, a blind fragile, reversible and invisible watermarking approach based on DE is proposed for encoding the DICOM metadata and Digital Signature (DS) of the whole image into the cover image to confirm authenticity and integrity of both image pixel data and image header. The scheme embeds the data into smooth blocks inside the ROI to achieve a watermarked image with low distortion. At extraction, the whole original image is fully recovered without the need for location map. The proposed method has been evaluated based on defined medical image watermarking requirements and compared to recent reversible watermarking approaches to verify its efficiency.

Conventional watermarking approaches based on DE embed 1-bit of watermark data into the difference value of two pixels. Locations of the pixels, used to encode the watermark, are required to detect/extract the watermark and reconstruct the reference image. The amount of additional information locating the relevant pixels reduces hiding capacity and increases the potential for image distortion. The proposed watermarking approach encodes the watermark into smooth regions inside the ROI without needing a location map. This achieves a high capacity watermarking with low distortion. The proposed method comprises three main steps; watermark creation, embedding, and extraction/verification.

5.2.1 Watermark Creation

Several approaches can be used to generate watermark data for confirming the authenticity and integrity of medical images (Coatrieux et al., 2006). Some of the authentication data is modified when the image is exchanged. In this case, the embedded and recalculated authentication data would be different, rendering authenticity confirmation impossible. This makes a careful selection of the authentication watermark is a necessity.

5.2.1.1 Authentication Watermark

In addition to the image raw data, DICOM defines a structure for describing the image. This structure is located in the image's header and called metadata. DICOM metadata comprises tables of attributes which record key information including the time of image acquisition, device parameters, imaging conditions, diagnosis result, and essential patient details such as the name, ID number, age, gender, weight, and height (Larobina and Murino, 2014). Some metadata fields are changed each time the image is distributed whilst others remain constant. Therefore, only information related to the patient and image (i.e. the constant data) must be used to ensure authenticity. In this research, only essential metadata fields, which contain the patient information and data describing the image that do not change during distribution, were employed in the authentication watermark (AW) (Table 5-1). There is no necessity to utilise all columns, and only the value field is needed to create the watermark for ensuring the authentication.

5.2.1.2 Integrity Watermark

The Digital Signature (DS) of the original medical image is calculated utilising Message Digest 5 (MD5) algorithm. The MD5 is a cryptographic hash function that generates a 128-bit Message Authentication Code (MAC). Any change to the image leads to change in the hash code. Comparing the base and retrieved codes enables the identification of image manipulation (Abd-Eldayem, 2013). In this research, the DS of the entire image is computed and encoded into the medical image to offer strict integrity watermark (IW).

5.2.1.3 Watermark Compression

The size of the generated watermarks (AW and IW) for ensuring the authenticity and integrity of the medical images is approximately 1KB. Compression of this data may reduce the distortion level and enhance the hiding capacity. Many compression techniques exist that can be used to compress the digital data (Uthayakumar et al., 2018, Hussain et al., 2018). In this research, Run Length Encoding (RLE) is used to compress the watermark data since it is easy and quick to implement, making it a good alternative to other complex compression algorithms. (Liew et al., 2013).

Table 5-1: A section of metadata fields selected from a DICOM data dictionary. These data were utilised as a watermark to ensure the authentication of images and comprise only essential metadata fields that do not change during exchanging. These data do not relate to a real patient.

Tag	Description	VR	Value
0008,0020	Study Date	DA	01012018
0008,0030	Study Time	TM	103045
0008,0060	Modality	CS	MR
0008,0070	Manufacturer	LO	SIEMENS
0008,0080	Institution Name	LO	Venice Hospital
0008,0090	Physician's Name	PN	Doctor Bellario
0010,0010	Patient Name	PN	Launcelot Gobbo
0010,0020	Patient ID	LO	999999
0010,0030	Patient Birth Date	DA	25121950
0010,0040	Patient Sex	CS	M
0018,0015	Body Part Examined	CS	Brain

5.2.2 Embedding Process

The embedding process initially segments the cover image into ROI and RONI (Fig. 5.1). In this research, the entire brain region was considered as the ROI due to its importance in diagnosis. The smooth blocks inside the ROI section are determined and the generated watermark is encoded into these blocks using a reversible watermarking method based on DE.

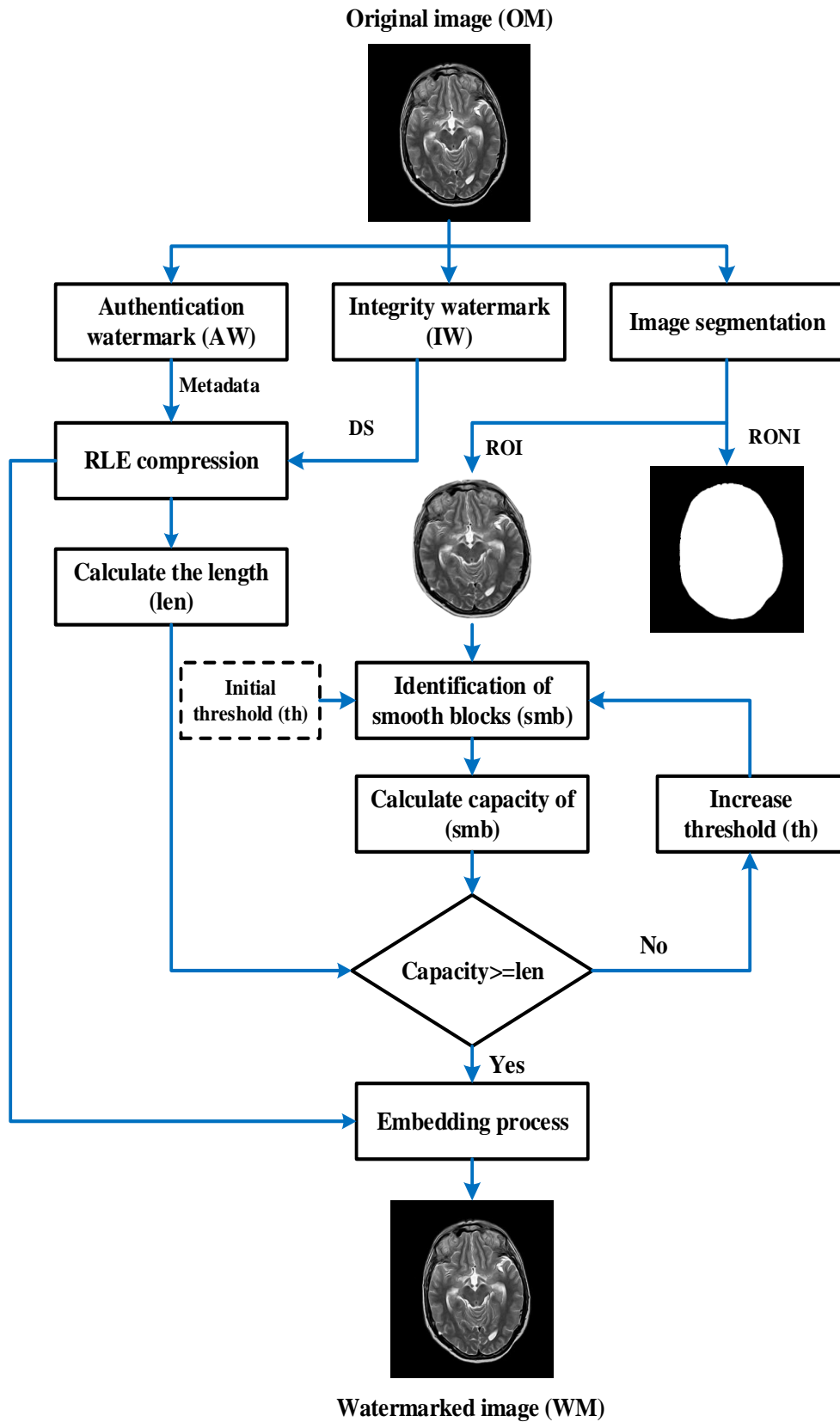


Fig. 5.1: Process diagram for the watermark embedding process. Starts with segmenting the cover image into ROI and RONI. Smooth blocks inside ROI are then identified. Watermark is encoded into the smooth blocks inside the ROI.

5.2.2.1 Image Segmentation

Prior knowledge indicates that the background intensity values of the brain MR slices are usually small compared to the intensity values of the foreground (Hasan et al., 2016b). In this research, histogram thresholding was adopted as a segmentation technique to isolate background and identify the image ROI. This method is based on thresholding values (T). If the intensity value of a pixel is greater than T then the pixel is considered as a brain region (ROI), otherwise, it is assumed to be part of the background (RONI). The T value can be identified either manually or automatically by applying established approaches (Hasan et al., 2016a). The T value was chosen experimentally (75) after applying a range of threshold values on many various images and visually evaluating these. A set of morphological operators, erosion, dilation and holes filling, are utilised to eliminate holes occurring in the segmented region (Fig. 5.2). Erosion is an operation used to decrease the size of the foreground objects and increase the size of the background. Dilation is an operation employed to increase the size of the foreground objects in binary images. A hole filling operator was applied to automatically fill the holes that were considered as background region in the binary image and surrounded by linked borders of foreground regions (Soille, 2013).

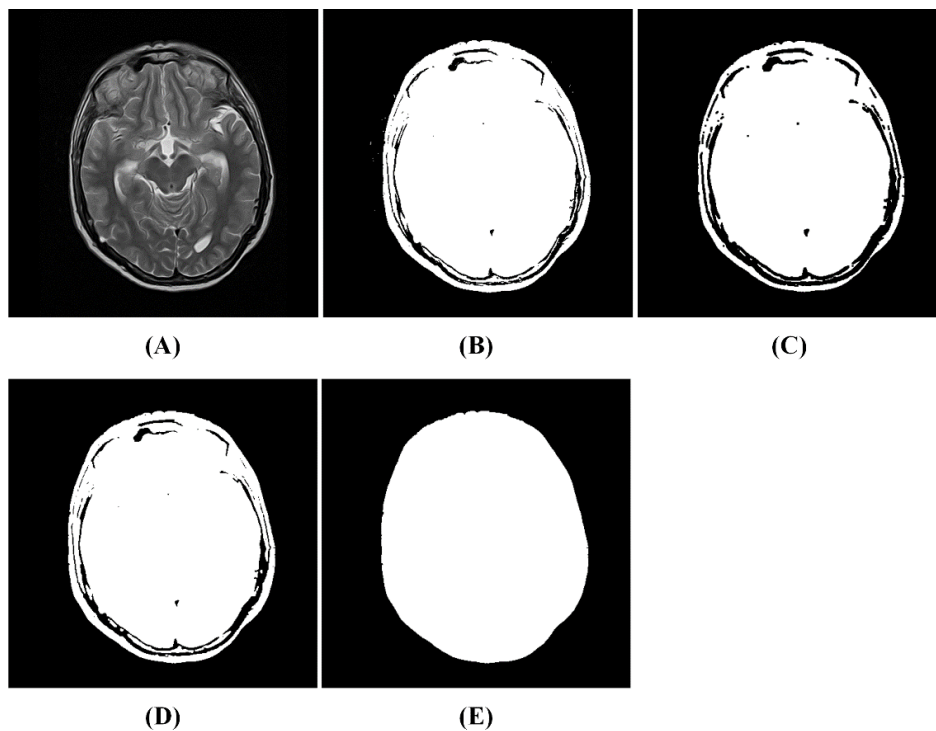


Fig. 5.2: An example of MR slice segmentation, **A)** Original image, **B)** Segmented, **C)** Eroded, **D)** Dilated, and **E)** Filled holes. A binary matrix of 1 and 0 values represents the foreground (ROI) and the background (RONI) respectively.

5.2.2.2 Smooth Regions Identification

Most medical images have a large smooth area, which is defined as the regions that have little significant difference between the adjacent pixels' intensity values, compared to other images. Embedding watermark into these regions is less noticeable to the human eye (Al-Qershi and Khoo, 2011b). Consequently, the watermark was encoded in smooth areas inside the ROI to decrease the degradation of the watermarked image. If adopting one of the existing techniques to determine the smooth regions, then when trying to identify the smooth regions to extract the encoded data, some of the identified smooth blocks will not precisely match the original blocks. Consequently, there is no guarantee that all pixels employed to discover the watermark will be similar to those utilised in the hiding process. This leads to the inability of the algorithm to extract the encoded data and recover the original image precisely.

A simple new algorithm (Algorithm1) is proposed in this research to determine the smooth regions inside the ROI of the medical image, such that when applying this algorithm to the watermarked image, it generates the same smooth blocks used at both embedding and extraction. This enables a precise extraction of the embedded data in the watermarked image without the need for any additional information (e.g. location map). The algorithm segments the ROI into non-overlapping blocks of 3x3 pixels which are separately evaluated and classified as either smooth or non-smooth blocks (Fig. 5.3). The absolute difference values between the corner pixels (P_1 , P_3 , P_7 , P_9) are calculated, and the average of these differences is computed and compared to the threshold value. The threshold value is increased based on the length of the watermark, created previously, to identify smooth blocks inside the ROI.

P₁ (i-1,j-1)	P₂ (i-1,j)	P₃ (i-1,j+1)
P₄ (i,j-1)	P₅ (i,j)	P₆ (i,j+1)
P₇ (i+1,j-1)	P₈ (i+1,j)	P₉ (i+1,j+1)

Fig. 5.3: An example of a 3x3 block of pixels inside the ROI part. All blocks are individually treated and categorised as an either smooth or non-smooth by using the Smooth Region Identification algorithm.

In Algorithm1, ROI denotes the ROI part of the image, L indicates the length of the watermark, and Fin_Th represents the final threshold used to identify the smooth blocks.

Algorithm 1 Smooth Regions Identification

Input: Region of Interest part ROI , length of watermark data L

Output: Final threshold Fin_Th

```

1: Initialise temporary threshold,  $Th=0$ 
2: Initialise total number of smooth blocks,  $S=0$ 
3: Segments ROI into non-overlapping blocks of 3x3 pixels (Fig. 5.3)
4: for each block do
5:     Calculate absolute difference ( $Dif1$ ) between  $P_1$  and  $P_3$ 
6:     Calculate absolute difference ( $Dif2$ ) between  $P_1$  and  $P_7$ 
7:     Calculate absolute difference ( $Dif3$ ) between  $P_1$  and  $P_9$ 
8:     Calculate absolute difference ( $Dif4$ ) between  $P_7$  and  $P_7$ 
9:     Calculate absolute difference ( $Dif5$ ) between  $P_3$  and  $P_9$ 
10:    Calculate absolute difference ( $Dif6$ ) between  $P_7$  and  $P_9$ 
11:    Calculate the average ( $Avg$ ) of the difference values ( $Dif1$  to  $Dif6$ )
12:    if  $Avg \leq Th$  then
13:        Increase the total number of smooth blocks,  $S=S+1$ 
14:    end if
15: end for
16: Calculate the capacity of smooth blocks,  $S=S*4$  //Each block can carry 4-bits of the watermark
17: if  $S < L$  then //Check the hiding capacity
18:     Increase the temporary threshold,  $Th=Th+1$ 
19:     go to step 4 //Repeat the process of smooth blocks identification
20: else
21:     Assign the temporary threshold to the final threshold,  $Fin\_Th=Th$ 
22: end if

```

5.2.2.3 Watermark Data Encoding

This research extends Alattar (2004a) technique to embed 4-bits from the watermark data into 5-pixels, instead of encoding 3-bits into 4-pixels, using a reversible watermarking based on the DE technique. The watermark data, which includes integrity and authenticity watermarks, is encoded into the five pixels (P_2, P_4, P_5, P_6, P_8) of all identified smooth blocks (Fig. 5.3). The corner pixels (P_1, P_3, P_7, P_9) are kept unchanged. These corner pixels are used at extraction to identify the smooth blocks used in the encoding process for hiding the watermark data. The final threshold value, which was previously calculated using the

smooth region identification algorithm, and the length of the watermark are embedded into the RONI section using 1-bit per 2-pixels reversible watermarking algorithm based on the DE technique (Maity and Maity, 2012). This threshold value is required at the extraction to identify the same smooth blocks used in the embedding process. This enables a precise extraction of the embedded data as well as retrieving the original unmodified image at extraction without the need for any auxiliary information in the form of the location map.

For each identified smooth block, the embedding algorithm deducts the value of the centre pixel (P_5) from pixels (P_2, P_4, P_6, P_8). Four new values are generated by encoding 4-bits of the watermark data into the differences values which previously calculated using the LSB technique. Finally, the inverse DE transform is applied to the generated new values, which carries the watermark bits, to produce the watermarked pixels.

In the encoding algorithm (Algorithm2), Smb denotes the smooth blocks inside ROI, We is a binary array that includes the watermark data, L indicates the length of the watermark (We), $WP_2, WP_4, WP_5, WP_6, WP_8$ are the watermarked pixels value of each smooth block (Smb), a, b, c, d, e are any integer values, and $\lfloor \dots \rfloor$ is a floor function which indicates “the greatest integer less than or equal to”.

5.2.3 Extraction and Verification Process

The process of extraction and verification starts by segmenting the watermarked image into ROI and RONI (Fig. 5.4). The final threshold and length of the embedded watermark are extracted from the RONI to identify smooth blocks inside the ROI. Concealed data is extracted from the pixels that have been employed in the embedding process, and the original pixels values are reconstructed.

Matching to the encoding process, the extraction algorithm deducts the value of the centre pixel (P_5) from pixels (P_2, P_4, P_6, P_8) for each smooth block. 4-bits of the watermark data are retrieved, and four new values are generated by extracting the LSB from the differences values. Finally, the inverse DE transform is applied to the generated new values to reproduce the original unmodified watermarked pixels.

In the extraction algorithm (Algorithm3), Smb identifies the smooth blocks inside the ROI, Fin_Th is the final threshold, Len indicates the length of the embedded watermark (we), Wx is a binary array includes the extracted watermark, $OP_2, OP_4, OP_5, OP_6, OP_8$ are the

original pixels value of each smooth block (Smb), a, b, c, d, e are the same integer values used in the encoding process, $\lfloor \dots \rfloor$ is a floor function which indicates “the greatest integer less than or equal to”, and LSB is the Least Significant Bit of binary representation of value.

The extracted watermark is decompressed using the same RLE decompression algorithm as for compression. It is divided into two watermarks; the authentication watermark (AW), and the integrity watermark (IW). These watermarks are compared to the recalculated metadata and DS of the extracted DICOM image to confirm authenticity and integrity of the image. This can be achieved by calculating the number of error and correct bits between the extracted and recalculated watermarks.

Algorithm 2 Encoding Process

Input: Smooth blocks Smb , watermark data We , length of watermark data L

Output: Watermarked pixels ($WP2, WP4, WP5, WP6, WP8$)

```

1: Initialise watermark counter,  $i=1$ 
2: Assign integer values to  $a, b, c, d, e$ 
3: for each smooth block ( $Smb$ ) do
5:     Calculate  $V1$  by deducting  $P_5$  from  $P_2$ 
6:     Calculate  $V2$  by deducting  $P_5$  from  $P_4$ 
7:     Calculate  $V3$  by deducting  $P_5$  from  $P_6$ 
8:     Calculate  $V4$  by deducting  $P_5$  from  $P_8$ 
9:     Encode the 1st watermark bit,  $N1=2*V1+We(i)$ 
10:    Encode the 2nd watermark bit,  $N2=2*V2+We(i+1)$ 
11:    Encode the 3rd watermark bit,  $N3=2*V3+We(i+2)$ 
12:    Encode the 4th watermark bit,  $N4=2*V4+We(i+3)$ 
13:    Calculate watermarked value of  $P_5$ ,  $WP5=\left\lfloor \frac{a*P5+b*P2+c*P4+d*P6+e*P8}{a+b+c+d+e} \right\rfloor - \left\lfloor \frac{b*N1+c*N2+d*N3+e*N4}{a+b+c+d+e} \right\rfloor$ 
14:    Calculate watermarked value of  $P_2$ ,  $WP2=N1+P_5$ 
15:    Calculate watermarked value of  $P_4$ ,  $WP4=N2+P_5$ 
16:    Calculate watermarked value of  $P_6$ ,  $WP6=N3+P_5$ 
17:    Calculate watermarked value of  $P_8$ ,  $WP8=N4+P_5$ 
18:    Increase the watermark counter to encode the next 4-bits,  $i=i+4$ 
19:    if  $i>L$  then                                     // Check the end of the watermark data
20:        Exit for
21:    end if
22: end for

```

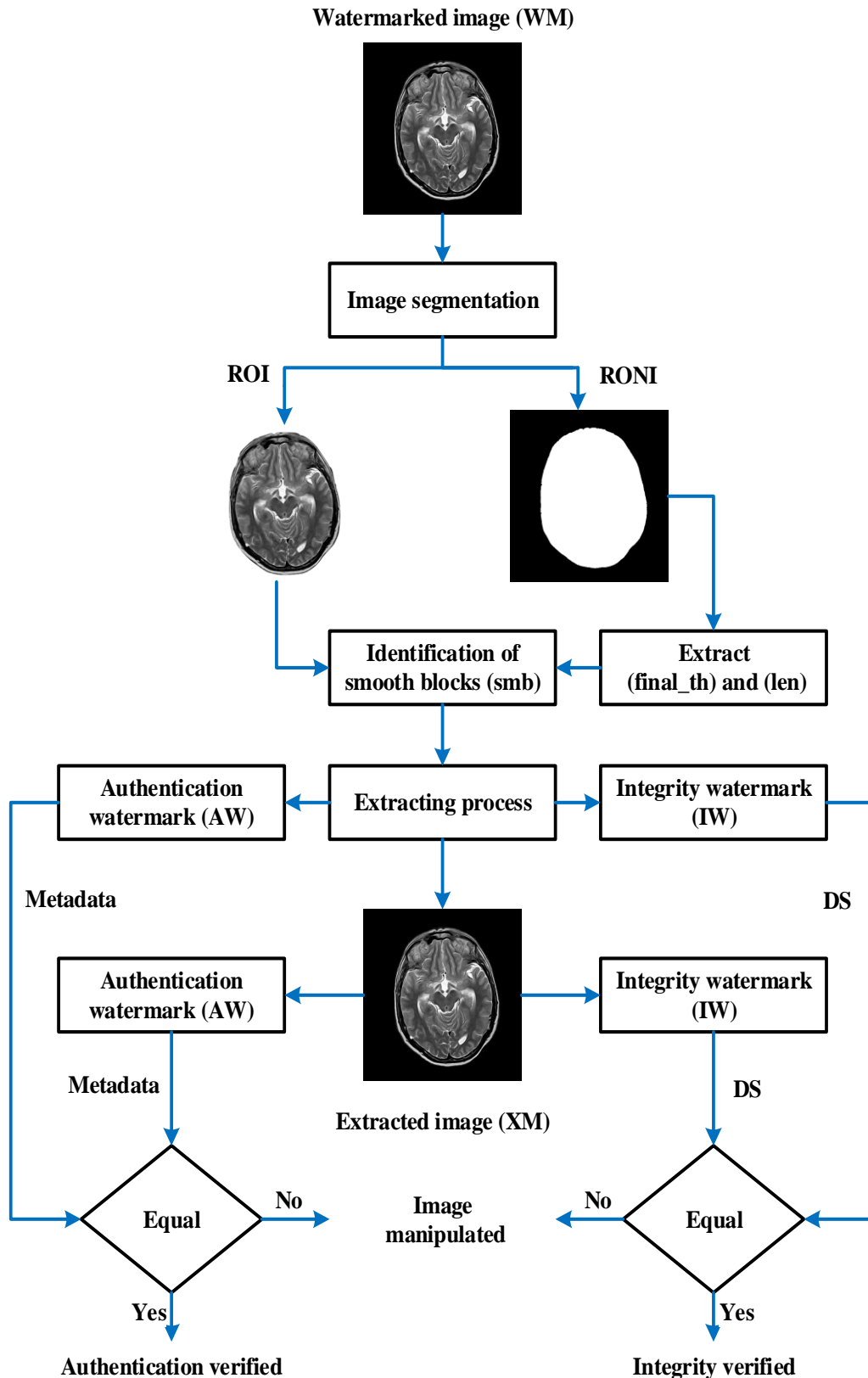


Fig. 5.4: Process diagram for the watermark extraction and verification process. Starts with segmenting the watermarked image into ROI and RONI. Smooth blocks inside the ROI are then identified to extract the encoded watermark. The extracted watermark is compared to the recalculated watermark of the extracted image to verify the authenticity and integrity of the image.

Algorithm 3 Extraction Process

Input: Smooth blocks Smb , Final threshold Fin_Th , length of watermark data L

Output: Original pixels ($OP2, OP4, OP5, OP6, OP8$), watermark data Wx

- 1: Initialise watermark counter $i=1$
 - 2: Assign integer values to a, b, c, d, e
 - 3: **for** each smooth block (Smb) **do**
 - 4: Calculate $V1$ by deducting P_5 from P_2
 - 5: Calculate $V2$ by deducting P_5 from P_4
 - 6: Calculate $V3$ by deducting P_5 from P_6
 - 7: Calculate $V4$ by deducting P_5 from P_8
 - 8: Extract the 1st watermark bit, $Wx(i)=LSB(V1)$ // LSB is the Least Significant Bit
 - 9: Extract the 2nd watermark bit, $Wx(i+1)=LSB(V2)$
 - 10: Extract the 3rd watermark bit, $Wx(i+2)=LSB(V3)$
 - 11: Extract the 4th watermark bit, $Wx(i+3)=LSB(V4)$
 - 12: Calculate a new value for P_2 , $NP2=\lfloor \frac{V1}{2} \rfloor$
 - 13: Calculate a new value for P_4 , $NP4=\lfloor \frac{V2}{2} \rfloor$
 - 14: Calculate a new value for P_6 , $NP6=\lfloor \frac{V3}{2} \rfloor$
 - 15: Calculate a new value for P_8 , $NP8=\lfloor \frac{V4}{2} \rfloor$
 - 16: Calculate original value of P_5 , $OP5= P_5 + \left\lfloor \frac{b*V1+c*V2+d*V3+e*V4}{a+b+c+d+e} \right\rfloor - \left\lfloor \frac{b*NP2+c*NP4+d*NP6+e*NP8}{a+b+c+d+e} \right\rfloor$
 - 17: Calculate original value of P_2 , $OP2=NP2+P_5$
 - 18: Calculate original value of P_4 , $OP4=NP4+P_5$
 - 19: Calculate original value of P_6 , $OP6=NP6+P_5$
 - 20: Calculate original value of P_8 , $OP8=NP8+P_5$
 - 21: Increase the watermark counter to extract the next 4-bits, $i=i+4$
 - 22: **if** $i>L$ **then** // Check the end of the watermark data
 - 23: **Exit for**
 - 24: **end if**
 - 25: **end for**
-

5.3 Experimental Results and Discussion

To assess the performance of the proposed scheme, twenty-five brain MR scans in DICOM format (16bpp, 512×512 pixels) were used. Sixteen images (Fig. 5.5) are provided by the MRI unit of Al-Kadhimiya Teaching Hospital (Iraq), from patients' records for use in this research conducted at the University of Salford (Hasan and Meziane, 2016). Nine images (Fig. 5.6) are selected from a publicly available and standardised medical images dataset downloaded from The Cancer Imaging Archive (TCIA) (Clark et al., 2013). Several

parameters have been used to conduct the experiment and evaluate the system performance (Table 5-2). The Experimentation has been carried out using MATLAB R2016a working on MS Window 7 platform on a PC with Core i7-4790 Intel CPU and 16 GB RAM.

Table 5-2: The parameters used to conduct the experiment and evaluate the proposed system performance.

No	Parameter	Value
1	Images format	DICOM (16bpp)
2	Images modality	Brain MRI
3	Images size	512x512 pixels
4	Watermark data	Authentication watermark (Metadata), Integrity watermark (DS)
5	Performance evaluation criteria	Imperceptibility, reversibility, capacity, robustness

5.3.1 Proposed System Performance Measurement

The proposed technique is assessed based on four principal requirements of image watermarking approaches: imperceptibility, reversibility, capacity, and robustness (Qasim et al., 2018a, Mousavi et al., 2014). Imperceptibility represents the highest requirement of watermarking systems. A digital watermark is defined as imperceptible if the original and watermarked images are perceptually indistinguishable. Imperceptibility is a factor of human cognition that needs to be appraised within the human context. A visual assessment trial has been conducted in the previous chapter which seeks to define the level of modification that can be applied without perceptual distortion. The outcomes related to objective measures including PSNR for image fidelity. The results demonstrated that the modification of the images to a level of PSNR=82 dB or better is unnoticeable to all observers, and modification level to a PSNR=80 dB should not be noticeable in the vast majority of cases. Reversibility ensures the extraction of the watermark by precisely recovering the unmodified original image. The capacity refers to the number of watermark bits that can be concealed into the cover image. Robustness states the ability of resistance against different image processing operations such as rotating, resizing, adding noise, etc. Not all applications require robust watermark, in some applications, it is necessary to be fragile to detect alteration that can be applied to the images (Qasim et al., 2018a).

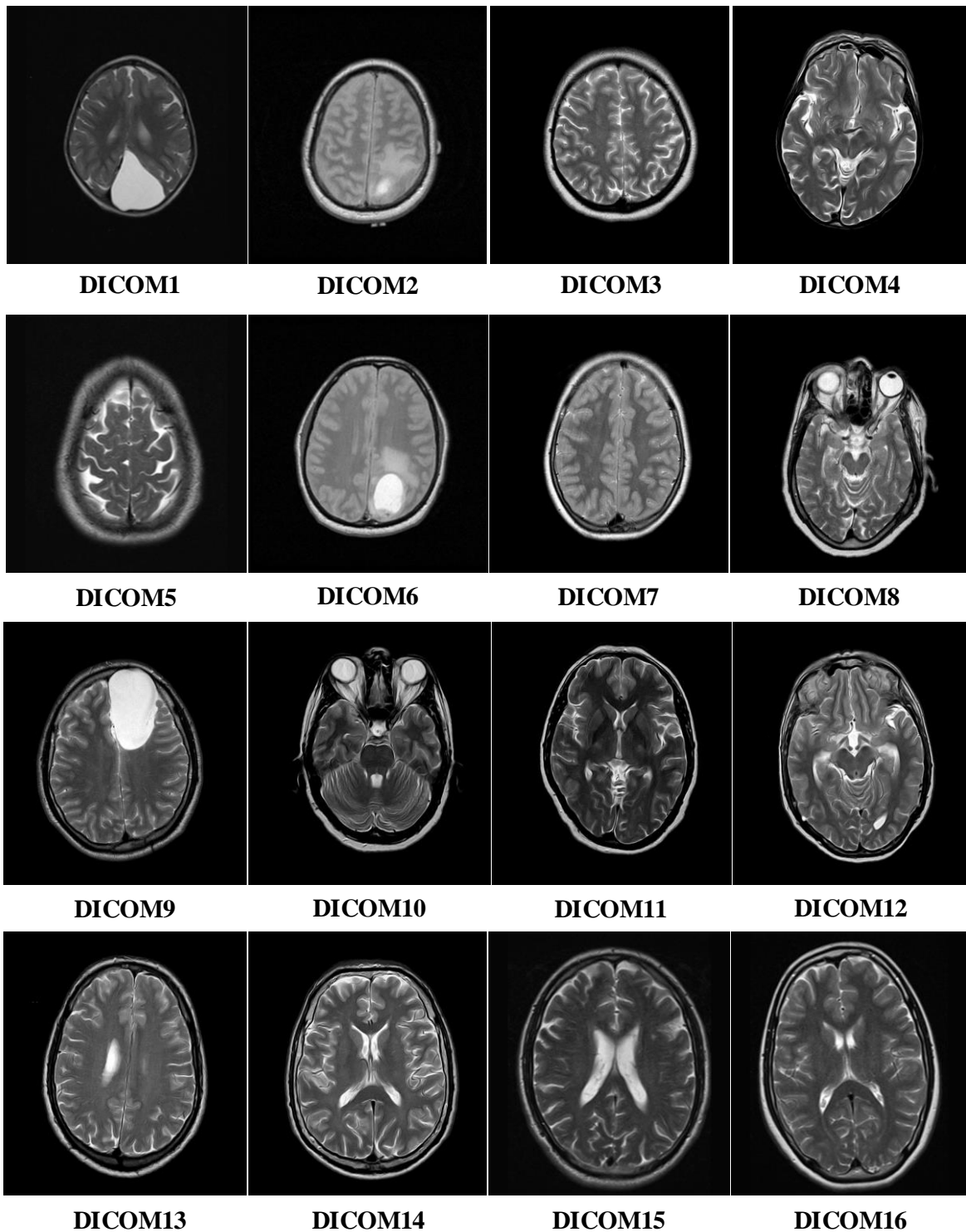


Fig. 5.5: The sixteen brain MR scans in DICOM format (16bpp, 512×512 pixels) provided by the MRI unit of Al-Kadhimiya Teaching Hospital (Iraq) and utilised to assess the performance of the proposed technique (Hasan and Meziane, 2016). These images have been independently diagnosed and categorised into normal and abnormal pathologies by the clinicians and contain different sizes of tumours/lesions. The images include different sizes of ROI (the informative part of the image which is utilised for diagnostic) and RONI (the non-critical part of the image, e.g. background).

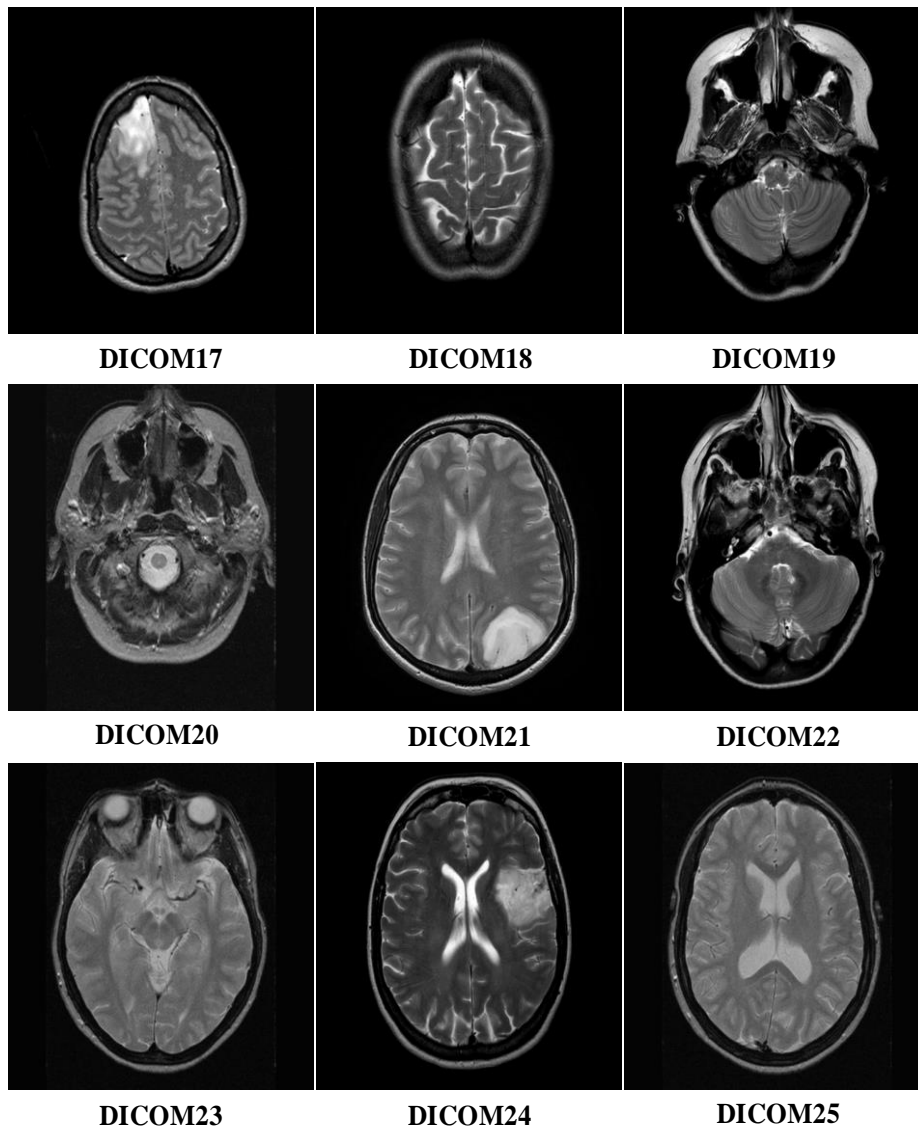


Fig. 5.6: The nine brain MR scans in DICOM format (16bpp, 512×512 pixels) selected from a publicly available and standardised medical images dataset downloaded from TCIA website and utilised to assess the performance of the proposed technique (Clark et al., 2013). These images contain different sizes of tumours/lesions and different sizes of ROI and RONI.

5.3.1.1 Imperceptibility

Imperceptibility between the original, watermarked and extracted images has been measured utilising commonly used physical measures including PSNR, SSIM, RMSE, and IF (Section 2.5.1). The goal of these metrics is to evaluate the visual quality of a modified image, against its unmodified version. A higher PSNR value denotes lower distortion. SSIM value of 1 refers that the tested images are equal. RMSE value close to 0 indicates low image distortion. The value of IF equal to 1 points out that the two images are identical.

Examples of original DICOM images and their corresponding watermarked, extracted and the difference between the original and extracted images (Fig. 5.7) indicate that there is no opportunity to perceive any differences between the original and watermarked images. In addition, the results of imperceptibility between the various original, watermarked and extracted images, using PSNR, SSIM, RMSE and IF (Table 5-3) show that the PSNR values between the original and watermarked images are high, SSIM values are equal to 1, RMSE values close to 0, and IF values are either 1 or very close to 1. This indicates that the distortion of the watermarked image is very low, and the watermark was encoded invisibly within the images. Therefore, the proposed method achieved the highest requirement of the digital watermarking schemes which is the imperceptibility.

5.3.1.2 Reversibility

Reversibility of the proposed system has been assessed, in the extraction, for both the retrieved image and the extracted watermark.

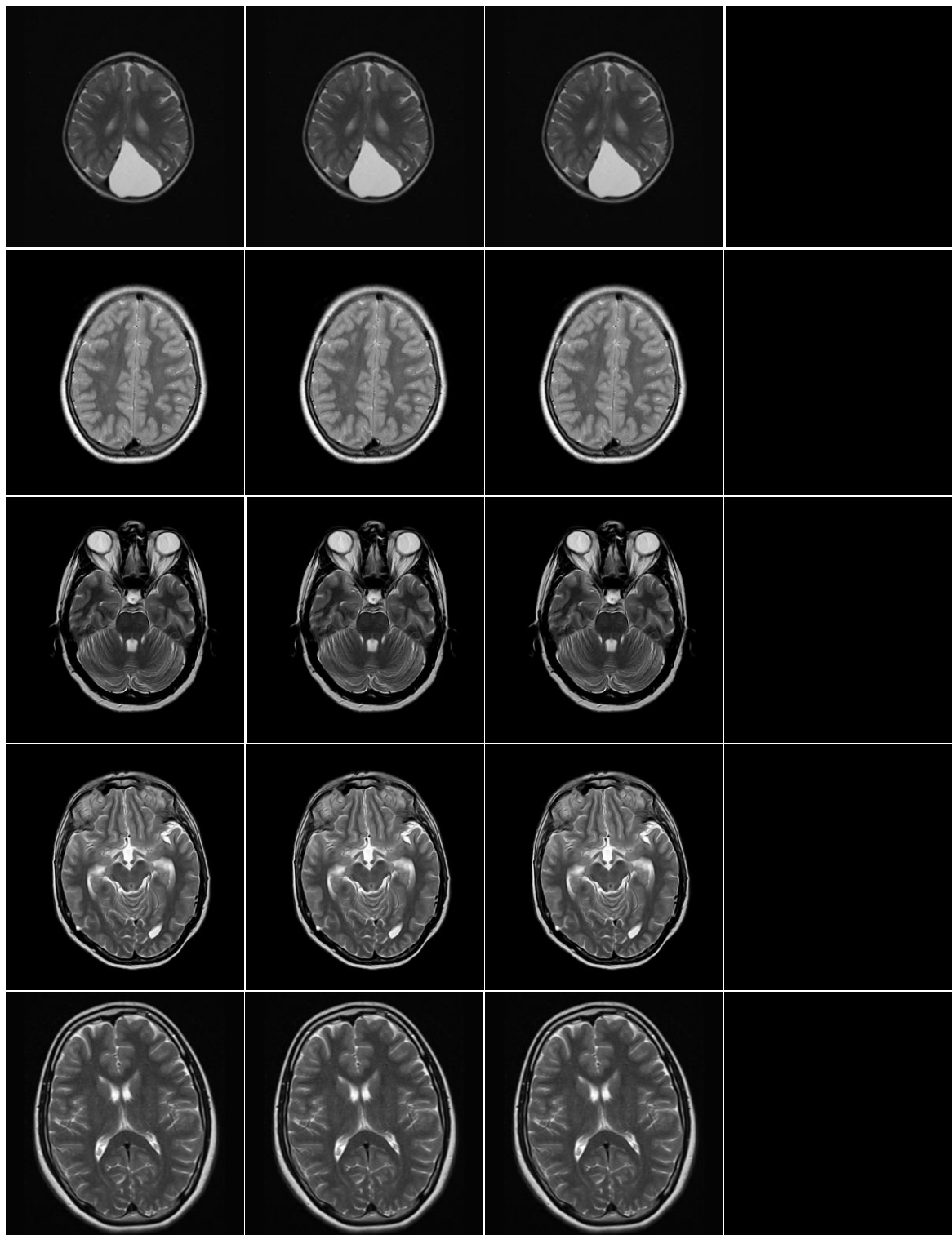
5.3.1.2.1 Image Reversibility

The proposed technique does not require any additional information to detect/extract the encoded watermark and reconstruct the reference image. This is due to the ability of exactly identifying the same smooth blocks inside ROI in both the embedding and extraction process. The result demonstrates that there is no numerical difference between the original and extracted images (Fig. 5.7). PSNR between the reference and extracted images are infinity (MSE values between the images are 0), SSIM and IF values are equal to 1, and RMSE values are equal to 0 (Table 5-3). Consequently, after extracting the watermark, the extracted image is precisely identical to the reference image.

5.3.1.2.2 Watermark Reversibility

The similarity between the embedded and extracted watermarks has been measured utilising two commonly used physical metrics; BER and AR (Section 2.6). These metrics calculate the number of error bits and the number of correct bits between the original and extracted watermark (Selvam et al., 2017).

The results demonstrate that the BER values are equal to 0, and the AR values are equal to 1. This indicates that the embedded watermark can be recovered at the extraction without any loss.



**Original images
(OM)**

**Watermarked images
(WM)**

**Extracted images
(XM)**

**Difference between OM
and XM images**

Fig. 5.7: Examples of the original DICOM images and their corresponding watermarked and extracted images after applying the proposed watermarking approach. No visual difference between the original and watermarked images can be observed which indicates that the distortion of the watermarked image is very low, and the watermark was encoded invisibly within the images. There is no numerical difference between the original and extracted which confirms the reversibility of the proposed approach.

Table 5-3: Imperceptibility between the original, watermarked, and extracted images using PSNR, SSIM, RMSE and IF metrics after applying the proposed watermarking approach. These results indicate that the distortion of the watermarked image is very low, and the watermark was encoded invisibly within the images. There is no numerical difference between the original and extracted which confirms the reversibility of the proposed approach.

Images	Watermark length (bits)	Watermarked images				Extracted images			
		PSNR	SSIM	RMSE	IF	PSNR	SSIM	RMSE	IF
DICOM1	8224	99.94	1	0.0109	0.9999	∞	1	0	1
DICOM2	7496	94.93	1	0.0345	0.9998	∞	1	0	1
DICOM3	7328	94.57	1	0.0375	0.9998	∞	1	0	1
DICOM4	7288	96.72	1	0.0229	0.9999	∞	1	0	1
DICOM5	8296	94.10	1	0.0418	0.9999	∞	1	0	1
DICOM6	7440	97.78	1	0.0179	0.9999	∞	1	0	1
DICOM7	7472	94.91	1	0.0347	0.9998	∞	1	0	1
DICOM8	7368	93.23	1	0.0510	0.9998	∞	1	0	1
DICOM9	7352	96.15	1	0.0261	0.9999	∞	1	0	1
DICOM10	7384	95.69	1	0.0290	0.9999	∞	1	0	1
DICOM11	7384	97.77	1	0.0180	0.9999	∞	1	0	1
DICOM12	7576	96.39	1	0.0247	0.9999	∞	1	0	1
DICOM13	7352	98.51	1	0.0151	0.9999	∞	1	0	1
DICOM14	7312	97.29	1	0.0200	0.9999	∞	1	0	1
DICOM15	8256	97.68	1	0.0183	1	∞	1	0	1
DICOM16	8296	96.95	1	0.0217	1	∞	1	0	1
DICOM17	9336	95.12	1	0.0191	0.9998	∞	1	0	1
DICOM18	7648	95.17	1	0.0170	0.9999	∞	1	0	1
DICOM19	7688	92.50	1	0.0365	0.9998	∞	1	0	1
DICOM20	7424	93.07	1	0.0281	0.9998	∞	1	0	1
DICOM21	8104	92.18	1	0.0670	0.9998	∞	1	0	1
DICOM22	7632	95.22	1	0.0130	0.9999	∞	1	0	1
DICOM23	7432	94.04	1	0.0179	0.9999	∞	1	0	1
DICOM24	7624	96.73	1	0.0152	0.9999	∞	1	0	1
DICOM25	7456	94.64	1	0.0136	0.9999	∞	1	0	1

5.3.1.3 Capacity

The capacity of the watermarking system is determined by calculating the number of image pixels required for embedding the data (Eq. 5.1) (Selvam et al., 2017).

$$Capacity = \frac{NP}{TP} \quad (5.1)$$

Where NP is the number of pixels required for embedding the watermark and TP is the total number of pixels.

The proposed scheme encodes the watermark into the ROI part of the medical image. Therefore, the hiding capacity depends on the ROI size. The size of the watermark, used in this research for ensuring the authenticity and integrity of the medical images, is approximately 1KB. This indicates that the proposed scheme can encode the watermark even the size of ROI is 8% of the image size. The capacity of the proposed system is estimated by calculating the number of pixels required for embedding different magnitudes of data. Distortion level of embedding various payload into the twenty-five DICOM images is measured using PSNR (Table 5-4). It is clear that the hiding capacity rises with increasing ROI size.

5.3.1.4 Robustness

This research ensures the authenticity and integrity of DICOM images. Authenticity and integrity of the pixel data and header information of the watermarked image are confirmed, if and only if, the embedded watermark and original image can be retrieved correctly and exactly matched. Manipulations of the image data also corrupt the embedded watermark resulting in a mismatch between original and retrieved watermarks. PSNR and BER are used to assess reversibility and ability to recover the embedded watermark after applying image processing operations simulating image data modifications. Malicious manipulations have also been applied including adding a new part to the image and removing an existing part from the image (e.g. lesion). The resultant PSNR between the original and the extracted images are not infinity, and BER values between the embedded and extracted watermarks are not equal to 0 (Table 5-5). This demonstrates that the proposed system is fragile against various manipulations.

Table 5-4: PSNR values after applying the proposed approach for hiding various payload. The hiding capacity and distortion level rise with the increase of the size of the ROI part of the medical images since the proposed scheme encodes the watermark into the ROI. (N/A not available).

Images	ROI size	Capacity 0.05bpp	Capacity 0.1bpp	Capacity 0.15bpp	Capacity 0.2bpp	Capacity 0.25bpp	Capacity 0.3bpp
DICOM1	27%	95.26	82.40	N/A	N/A	N/A	N/A
DICOM2	30%	90.10	80.90	N/A	N/A	N/A	N/A
DICOM3	35%	90.92	84.66	77.09	N/A	N/A	N/A
DICOM4	35%	93.05	86.01	74.57	N/A	N/A	N/A
DICOM5	36%	90.52	83.33	75.48	N/A	N/A	N/A
DICOM6	36%	93.25	85.68	74.23	N/A	N/A	N/A
DICOM7	37%	91.74	86.46	79.62	N/A	N/A	N/A
DICOM8	39%	89.84	84.10	78.31	N/A	N/A	N/A
DICOM9	41%	92.99	87.95	82.21	N/A	N/A	N/A
DICOM10	42%	91.76	85.48	79.26	N/A	N/A	N/A
DICOM11	42%	94.20	88.34	81.25	N/A	N/A	N/A
DICOM12	43%	93.05	87.08	80.85	N/A	N/A	N/A
DICOM13	46%	95.46	90.61	85.38	77.06	N/A	N/A
DICOM14	50%	94.00	88.35	82.21	75.34	N/A	N/A
DICOM15	59%	94.92	88.81	84.11	78.89	74.07	N/A
DICOM16	59%	93.71	87.56	82.56	76.54	70.63	N/A
DICOM17	26%	91.72	82.47	N/A	N/A	N/A	N/A
DICOM18	34%	91.08	84.88	N/A	N/A	N/A	N/A
DICOM19	40%	88.41	81.57	74.78	N/A	N/A	N/A
DICOM20	47%	89.29	84.20	79.95	N/A	N/A	N/A
DICOM21	49%	87.89	82.29	76.95	71.12	N/A	N/A
DICOM22	49%	91.12	85.04	79.57	72.57	N/A	N/A
DICOM23	50%	90.43	85.36	81.44	76.40	N/A	N/A
DICOM24	50%	92.99	87.59	82.72	75.65	N/A	N/A
DICOM25	51%	90.92	86.21	82.27	77.22	N/A	N/A

Table 5-5: Reversibility evaluation of both the original image and embedded watermark after applying various manipulations to the watermarked images. Manipulations of the images corrupt the embedded watermark resulting in a mismatch between the original and extracted images as well as the original and retrieved watermarks. This confirms the fragility of the approach which is essential for ensuring the integrity and authenticity of images.

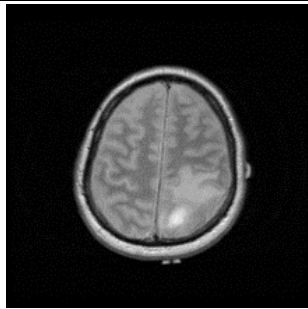
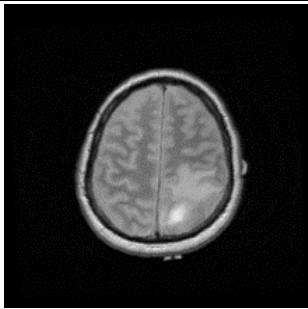
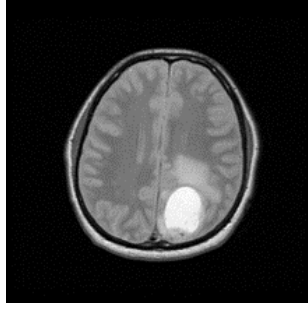
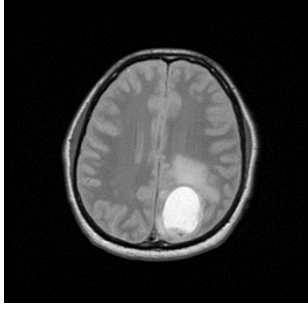
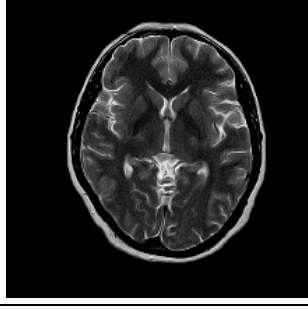
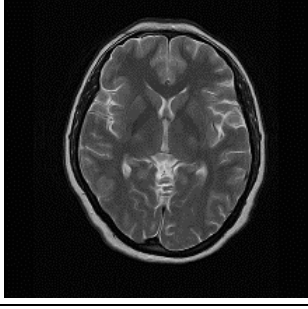
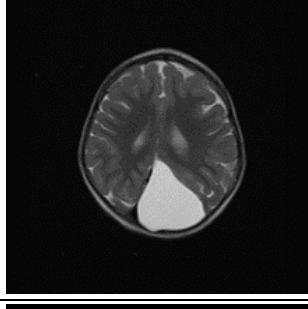

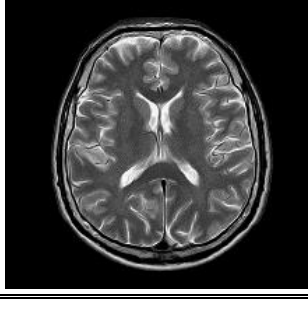
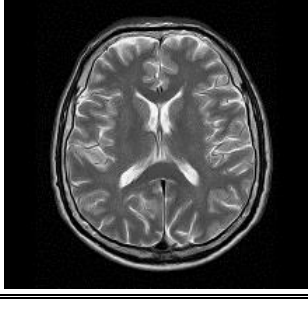


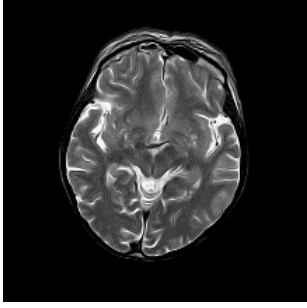
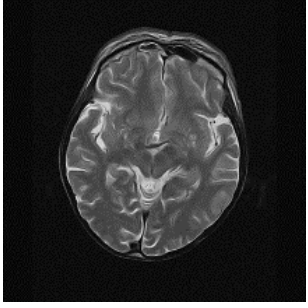
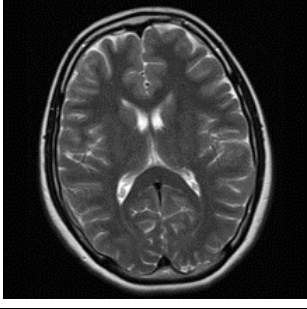
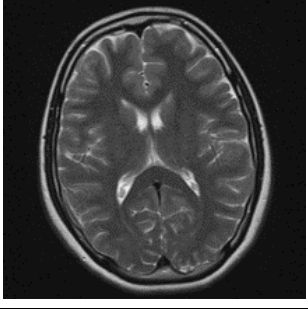

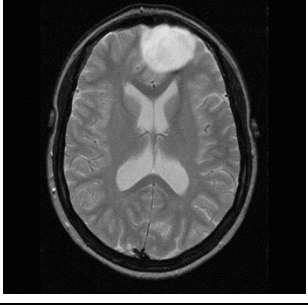
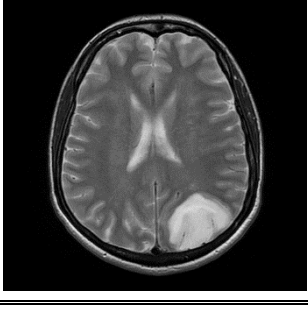
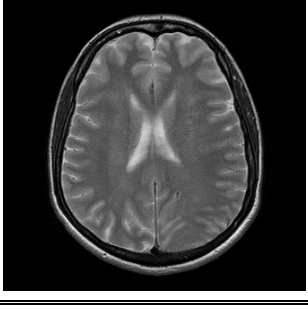
Manipulation	Watermarked image	Manipulated image	PSNR	BER
Rotate (2°) and cropping			58.53	0.3837
Crop (90%) and resize			80.89	0.3718
Adjust brightness (±5)			82.35	0.2451
Adjust intensity			7.06	0.3926
Gaussian filter (σ=0.5)			83.15	0.4981

Table 5-5: Continued.

Manipulation	Watermarked image	Manipulated image	PSNR	BER
Median filter			79.22	0.3857
Gaussian noise (SNR=5 dB)			79.66	0.4967
Salt and pepper noise (d=0.0005)			76.45	0.4315
Adding region/lesion			17.70	0.4239
Removing region/lesion			16.92	0.4833

5.3.2 Comparison with Existing Approaches

This research aims to ensure trust in digital medical workflows by enabling robust authenticity and integrity controls within medical images. The highest requirement of digital watermarking utilised for the purpose of integrity and authentication is imperceptibility (Qasim et al., 2018a). Many reversible approaches have been presented in the literature to confirm the authenticity and integrity of medical images (Yang et al., 2018, Balasamy and Ramakrishnan, 2018, Parah et al., 2017, Gao et al., 2017, Eswaraiah and Reddy, 2014a, Das and Kundu, 2013). However, most of them have been applied to 8-bit medical images. Therefore, the performance of the proposed watermarking approach is compared with several reversible watermarking schemes recently proposed in the literature and applied to 16-bit medical images to make the comparison objective (Table 5-6). The comparison is conducted by relating the hiding capacity to the level of distortion of watermarked images (e.g. PSNR, SSIM, RMSE and IF).

Table 5-6: Performance comparison of the proposed scheme against approaches identified in the literature. The results demonstrate that the proposed scheme surpassed the other techniques in terms of visual quality of watermarked images. (N/A not available).

Scheme	Location map	Capacity	Visual quality of watermarked images
Roček et al. (2016)	Required	N/A	PSNR=81 dB SSIM=0.99997
Selvam et al. (2017)	Not required	0.0625-0.25bpp	PSNR (60.42-65.23 dB) SSIM (0.9832-1) RMSE (0.0321-0.0891) IF (0.9178-0.9836)
Pan et al. (2018)	Required	0.007-0.027bpp	PSNR (67.57-76.5 dB) SSIM=1
Atta-ur-Rahman et al. (2018)	Not required	N/A	PSNR=72.98 dB
Chen et al. (2018)	Required	0.088-0.148bpp	PSNR (58.32-70.38 dB)
Ma et al. (2019)	Required	0.01-0.27bpp	PSNR (52-68 dB) SSIM (0.983-1)
Proposed	Not required	0.034-0.25bpp	PSNR (70.63-99.94 dB) SSIM= 1 RMSE (0.0109-0.0510) IF= 1

As shown in the results, the distortion level achieved in the related works ranges from (52 to 81 dB PSNR, 0.983 to 1 SSIM, 0.0321 to 0.0891 RMSE, and 0.9178 to 0.9836 IF) and the hiding capacity ranges from 0.007 to 0.27bpp of the original image size. It can be noticed that (Roček et al., 2016) scheme achieved a higher PSNR value (81 dB) but hiding capacity is not mentioned which also case in (Atta-ur-Rahman et al., 2018) scheme. These approaches have been excluded in subsequent comparison. A higher hiding capacity has been realised by Ma et al. (2019) at 0.27bpp but the distortion level of watermarked images is very low (PSNR=52 dB). Additionally, the location map of pixels used to carry the watermark data is required at the extraction to retrieve the encoded data, which negatively affects the hiding capacity of the approach. The proposed approach surpassed the other techniques by achieving a high visual quality of watermarked images up to (PSNR=99.94 dB at 0.034bpp and PSNR=70.63 dB at 0.25bpp) whilst enhancing the hiding capacity through eliminating the need for the location map of pixels.

In order to highlight the results of the comparison shown in Table 5-6, Fig. 5.8 depicts the results in a two-dimensional chart to represent the relation between hiding capacity and imperceptibility (PSNR) between the proposed approach and the related works under comparison. This clearly signifies that the proposed approach surpasses the others in terms of the visual quality of watermarked images. Only the scheme proposed by Ma et al. (2019) achieved a higher hiding capacity (0.27bpp) than the proposed approach; however, the visual quality of watermarked images is very low (PSNR=52 dB).

Furthermore, a DICOM15 image, which achieved the highest embedding capacity, is used to compare the performance of the proposed approach with other DE-based reversible watermarking schemes. These schemes comprise Tian (2003), Alattar (2004a), Chiang et al. (2008), Al-Qershi and Khoo (2011b) (scheme 1) and Al-Qershi and Khoo (2011b) (scheme 2). DE-based watermarking approaches, found in the literature, can perform equally but most of them lack the simplicity of the proposed approach (He et al., 2017, Kumar and Natarajan, 2016, Lei et al., 2014). Visual quality of watermarked images is tested after hiding various payload magnitudes (0.05bpp, 0.1bpp, 0.15bpp, 0.2bpp, 0.25bpp). The results clearly signify that the proposed algorithm achieves a watermarked image with lower distortion in terms of PSNR (Fig. 5.9) and IF (Fig. 5.10) in comparison to other approaches.

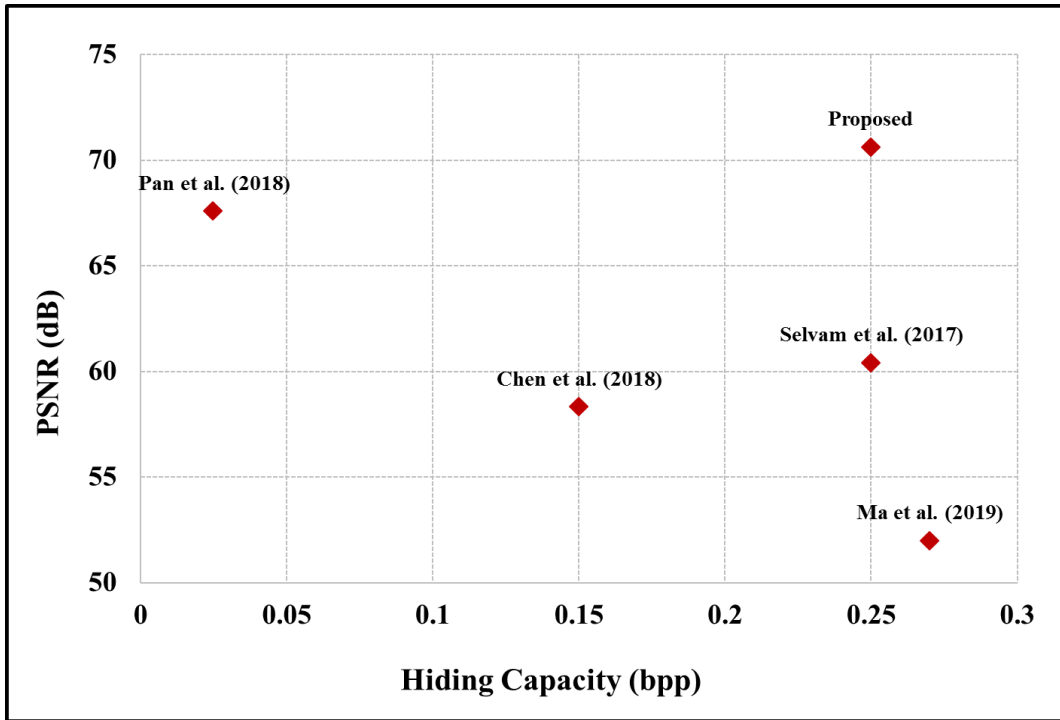


Fig. 5.8: Comparison between the proposed approach and other reversible watermarking schemes presented in the literature in terms of distortion level (PSNR) versus hiding capacity. These schemes include Selvam et al. (2017), Pan et al. (2018), Chen et al. (2018), and Ma et al. (2019). The results clearly signify that the proposed approach surpasses the other approaches in terms of the visual quality of watermarked images. Only Ma et al. (2019) scheme achieved a higher hiding capacity but the distortion level of watermarked images is very high.

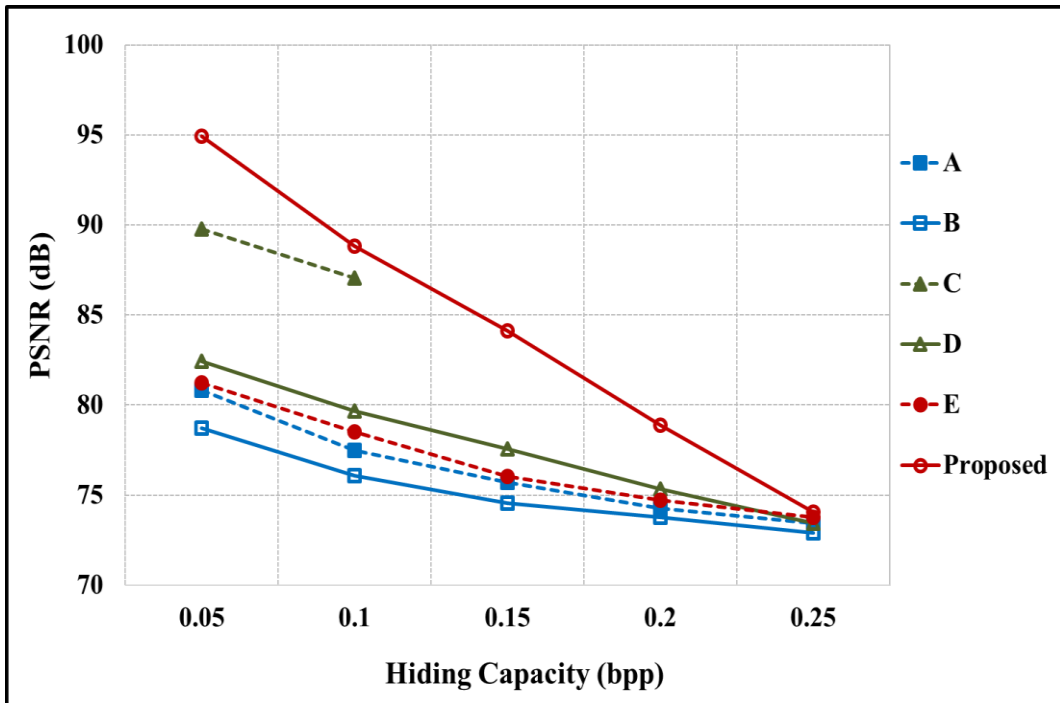


Fig. 5.9: Evaluation of distortion level (PSNR) versus payload capacity for the proposed scheme against other DE-based reversible watermarking schemes using the DICOM15. These schemes comprise: **A)** Tian (2003), **B)** Alattar (2004a), **C)** Chiang et al. (2008), **D)** Al-Qershi and Khoo (2011b) (scheme 1), and **E)** Al-Qershi and Khoo (2011b) (scheme 2). The distortion level is evaluated after hiding various payload magnitudes. The results indicate that the proposed algorithm achieves a watermarked image with lower distortion.

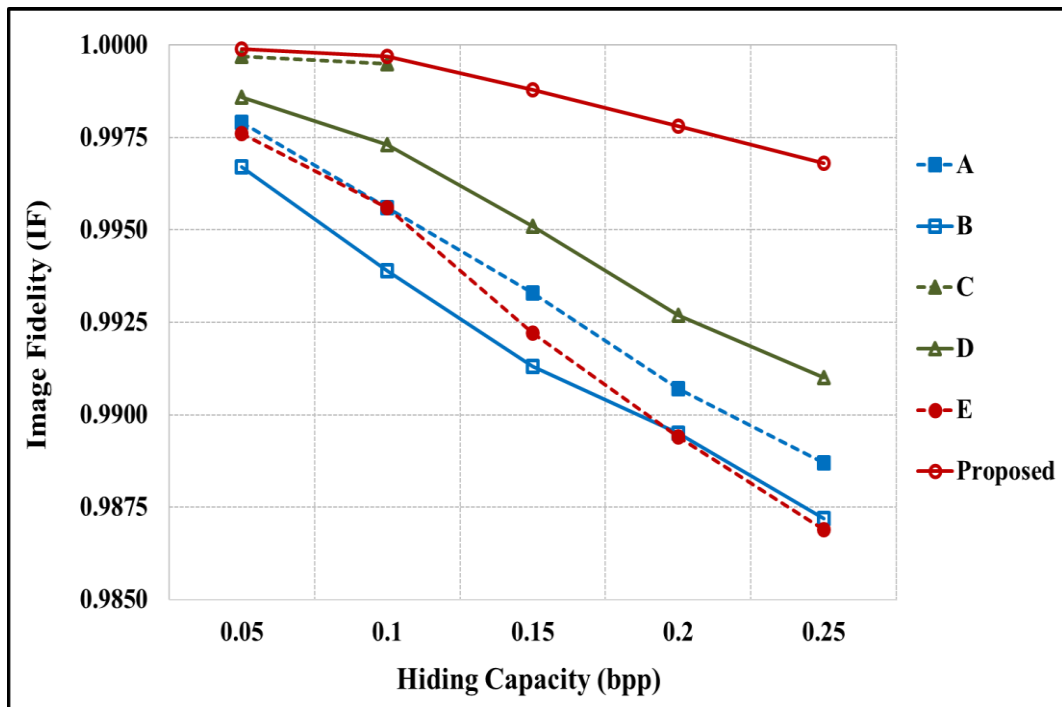


Fig. 5.10: Evaluation of distortion level (IF) versus payload capacity for the proposed scheme against other DE-based reversible watermarking schemes using the DICOM15. These schemes comprise: **A)** Tian (2003), **B)** Alattar (2004a), **C)** Chiang et al. (2008), **D)** Al-Qershi and Khoo (2011b) (scheme 1), and **E)** Al-Qershi and Khoo (2011b) (scheme 2). The distortion level is evaluated after hiding various payload magnitudes. The results indicate that the proposed algorithm achieves a watermarked image with lower distortion.

5.4 Chapter Summary

In this chapter, a novel blind, reversible and imperceptible watermarking method is proposed for ensuring the integrity and authenticity of brain MR images and detecting manipulations. The proposed scheme automatically segments the image into two sections; ROI and RONI. An extended reversible watermarking method based on the DE technique is utilised to encode 4-bits of the watermark data in each smooth block of 3x3 pixels selected from the ROI. The exact original images are retrieved after extracting the embedded watermark successfully. The need for a location map of the employed pixels is eliminated in the embedding and extraction processes to enable, control and facilitate maximising the hiding capacity whilst reducing image distortion. Based on the methodology of the DE technique, which hides the data in the difference value between two pixels, the proposed scheme encodes the watermark into the smooth blocks inside the ROI to decrease the degradation of the watermarked images. This has been evaluated through a visual approach to defining a perceptual boundary, below which change is noticeable. This defines a clear metric to

determine the level of modification that can be applied for encoding a known magnitude of payload data in an imperceptible manner.

Experimental results indicate that the proposed method yields superior performance to the other state-of-art schemes in terms of distortion level. It achieves excellent visual image quality regarding PSNR, SSIM, RMSE, and IF, and the proposed watermarking approach is ideal for medical images even if the size of the ROI part of the images is small.

The next phase of this research is integrating the proposed watermarking technique into the digital medical imaging workflow. This is essential to evaluate and validate the ability of the approach to deal with the security threats that can face medical images during routine clinical practices such as viewing, exchanging, and archiving.

CHAPTER SIX

Integration of the Proposed Watermarking Approach into Medical Imaging Systems

This chapter presents the process of integrating the proposed watermarking approach into medical imaging workflow to evaluate, validate and verify its applicability and appropriateness to medical domains. This is significant to ensure the ability of the proposed approach to tackle security risks that may face medical images during routine medical practices. This work considers two key objectives within the aim of defining a secure and practical digital medical imaging system: current medical digital workflows are deeply analysed to define security limitations in Picture Archiving and Communication Systems (PACS) of medical imaging; the proposed watermarking approach is then theoretically tested and validated in its ability to operate in a real-world scenario (e.g. PACS). These have been undertaken through identified case studies related to manipulations of medical images within PACS workflow during acquisition, viewing, exchanging and archiving. This work assures the achievement of the identified requirements of digital watermarking when applied to digital medical images and provides robust controls within medical imaging pipelines to detect modifications that may be applied to medical images during viewing, storing and transmitting.

6.1 Introduction

Medical imaging systems, PACS, act as integrated systems for managing, archiving and exchanging digital medical images. The propagation of PACS is associated with the development of various digital acquisition equipment that contributed to reducing the maintenance issues and improving the performance of various services provided by radiology departments. These acquisition devices create digital images across diverse modalities including X-ray, ultrasound, CT and MRI (Godinho et al., 2015), which are, typically, stored and broadcasted within the digital medical workflow based on DICOM standard (Pianykh, 2009). A generic PACS infrastructure (Fig. 6.1) comprises three main components, connected by a high-speed communication network, including acquisition devices, repositories, and viewing workstations (Huang, 2011).

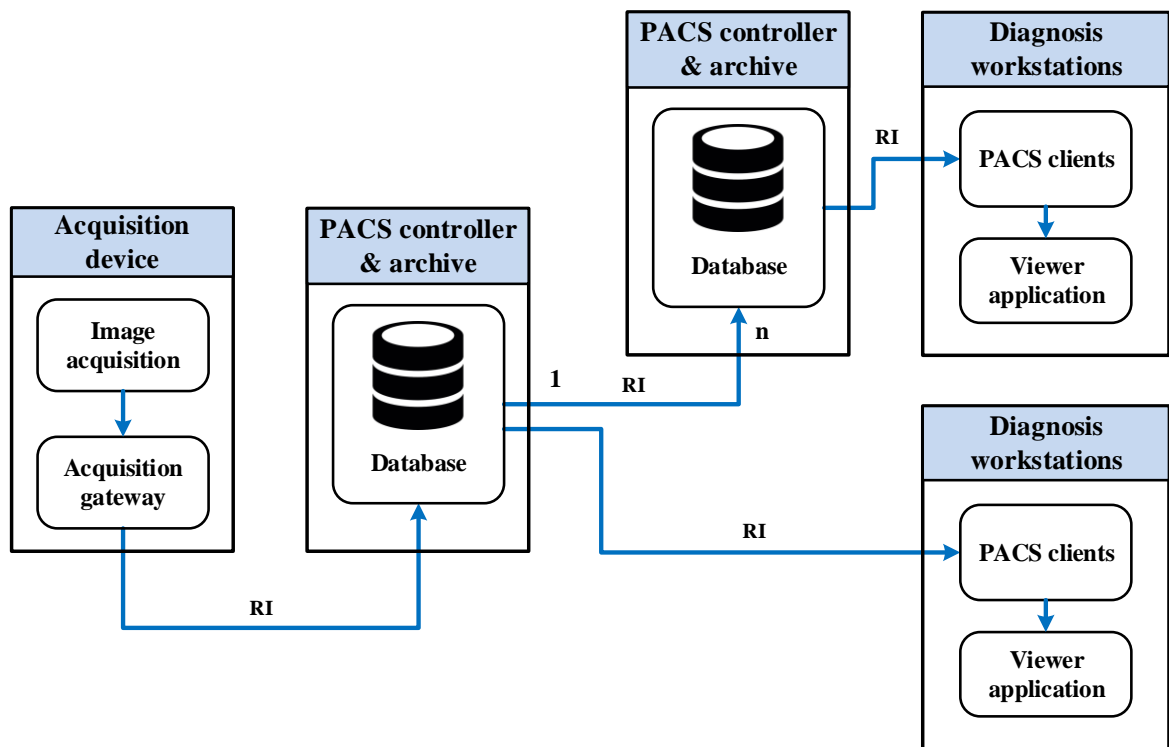


Fig. 6.1: A generic PACS infrastructure which comprises three main components connected by a high-speed communication network including acquisition devices, archive server, and diagnosis workstations. Acquisition gateway acts as a buffer between acquisition devices and the PACS server to provide various tasks. RI denotes row images produced by the acquisition system. Internal PACS may connect to a different number of PACS (1 to n) within or outside the internal system.

Acquisition gateway acts as a buffer between acquisition devices and the PACS server to perform three major tasks (Liew and Zain, 2010):

- Collect medical images from acquisition machines.
- Transform the images from manufacturer specifications to standard DICOM formats.
- Transmit the medical images to the PACS server and controller.
- Implement image pre-processing and data security operations.

PACS controller and archive server perform more complex tasks (Liew and Zain, 2010):

- Receive, accumulate, and transfer the medical images.
- Update and archive database of the medical images.
- As an interface for connecting Radiology Information Systems (RIS).

The basic workflow of radiology departments comprises three main phases; admission, examination, and payment. In the admission phase, the patient's data is recorded in the RIS. Then, the actual practice is performed through the examination phase. Firstly, the acquisition machines generate the images for the patient and archived them in the main PACS repository. A clinician retrieves/downloads the images from the PACS to conduct the required investigation and write a medical report. The produced report is saved afterwards either in the RIS or the PACS. The last phase, which is the payment process, mainly interacts with the RIS (Godinho et al., 2015).

6.2 Security Flaws in Medical Imaging Systems

In modern radiology departments, a hierarchical scheme can be considered as a pyramid with hospitals at the base and the general PACS at its top. Images taken in a hospital are archived in the PACS. Within a few minutes, these images are transferred to an upper PACS, which collects data arrived from similar departments in different hospitals. These images stay in this system for several hours, typically staying for the night, during which time their integrity is not maintained accurately. The images are then transmitted to a hierarchically higher PACS until they reach the top-PACS. In the top-PACS, the data are eternally saved and collected in tapes, physical drives or optical supports. This operation is called consolidation (Fontani et al., 2010).

Transmission of medical images between hospitals, located at various locations, and different administrative organisations has become a common practice for many purposes including diagnosis, treatment, external second opinion, sending to another healthcare provider, and patient data request (Memon et al., 2011). Many cases of manipulations on the medical images can be applied, but the concern is how they can be discovered? Indeed, by merely seeing the images, detecting some reasonable alterations that include fully counterfeit abnormalities would be impossible (Qasim et al., 2018a). Digital watermarking is recognised as a robust approach for protecting the medical images and detect the applied alterations. Three objectives can be achieved by using digital watermarking (Liew and Zain, 2010):

- Data hiding: to avoid the separation between image and patient's information as well as reducing the required storage space.
- Data integrity: to ensure that the image has not been changed without authorisation.
- Data authenticity: to verify information source and confirm that the image belongs to the correct patient.

6.3 Design and Evaluation Criteria for Medical Images Watermarking

On the practical side, there is a reluctance in using digital watermarking in medical domains due to most of the proposed watermarking approaches not considering strict requirements of the medical imaging workflow. Applying a digital watermarking to medical imaging comprises two phases; design phase and evaluation phase (Fig. 6.2). In the design phase, the optimal criteria required to be identified correctly based on the essential requirements of medical domains. Evaluation criteria are also fundamental to verify the suitability of the proposed watermarking technique for medical imaging workflow. The design and evaluation parameters for image watermarking are mainly related to its substance components; watermark creation, watermark embedding, and watermark extraction.

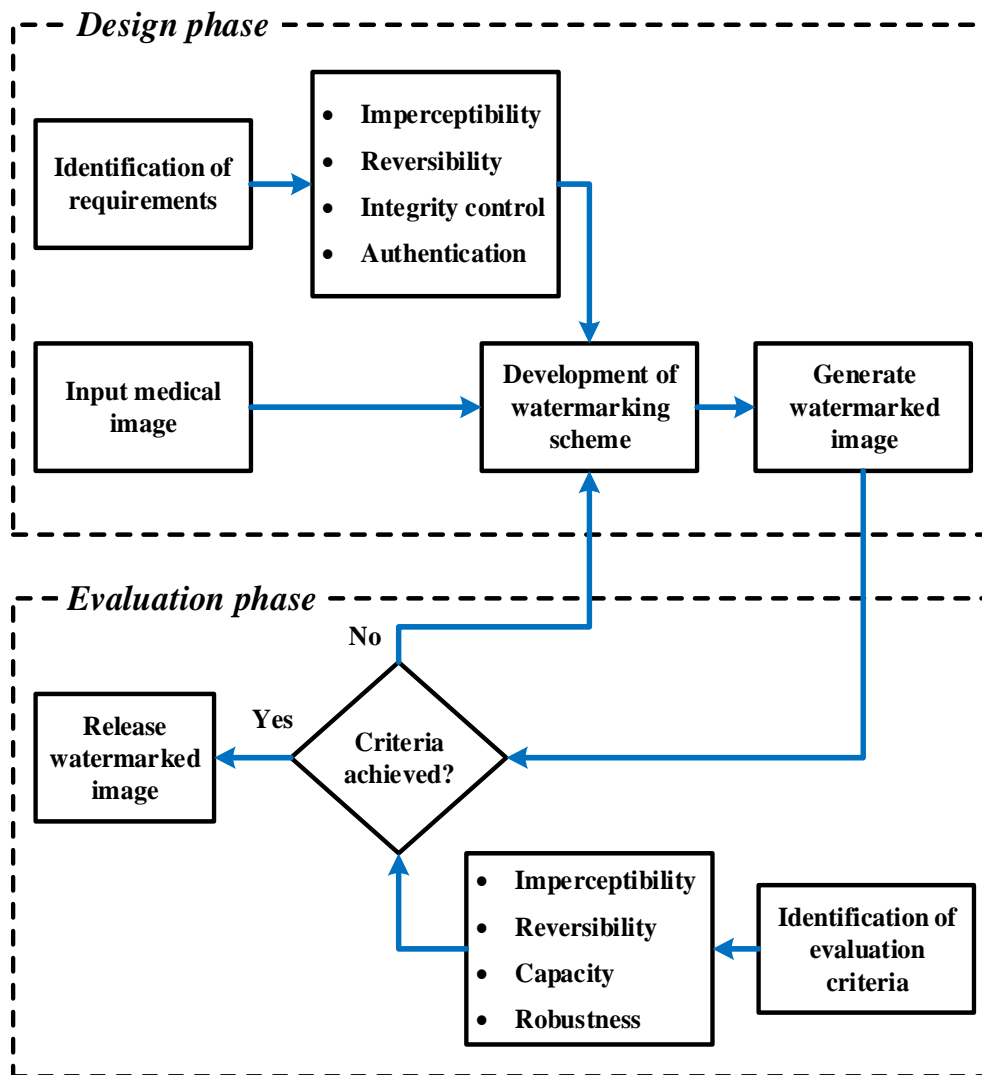


Fig. 6.2: The design and evaluation phases for the proposed watermarking approach. In the design phase, the essential requirements of the medical workflow are identified before developing a watermarking scheme. In the evaluation phase, the evaluation criteria are identified, and the watermarked images are assessed based on these criteria before releasing the images into medical imaging workflow.

6.3.1 Design Phase

Identification of the design requirements is crucial for defining the tools through which an appropriate system can be developed for the desired application. Particular requirements must be taken into account when applying digital watermarking techniques to medical images such as imperceptibility, reversibility, integrity control and authentication (Mousavi et al., 2014).

In some applications, there is a necessity to encode watermark data into a digital object, in an invisible manner, for the purposes of ensuring authentication, integrity, ownership identification and so on. This can be fulfilled by carrying out a slight change to the source image taking into consideration the other features such as capacity and robustness. However, the original unmodified data cannot be retrieved after removing the embedded data. This cannot be accepted in some critical applications like medical diagnosis, military investigations and legal issues where the end-user needs to be confident of the image he is watching to make a decision. Therefore, reversible watermarking methods have been developed which can recover the original unmodified image, alongside the hidden data after extracting the encoded data (Qasim et al., 2018a).

Imperceptibility between an original image and its watermarked version can be determined either physically or visually. Physical assessment methods are simple and effective tools for assessing visual image quality. However, they do not consider all clinical features that are significant for medical practices. Therefore, they should be accompanied by experts' view to verify their validity (Båth, 2010). Various physical measures can be used to evaluate the reversibility of both the retrieved image and extracted watermark (Selvam et al., 2017).

Several requirements are also significant when proposing digital watermarking for the purpose of medical images authenticity and integrity (Pushpala and Nigudkar, 2005):

- Although this is not a rigorous condition in reversible watermarking techniques, the watermarked image should visually be the same as the original image.
- The size of the watermarked image should not modify/increase because of encoding the watermark data.

- Even a single bit modification to a watermarked image must lead to unsuccessful verification.
- The proposed watermarking approach should be performed while exchanging image data in DICOM format in the medical workflow.
- The watermarking technique should be usable as a separate module pluggable to PACS workflow.

6.3.2 Evaluation Phase

In order to utilise digital watermarking in medical environments to ensure the authenticity and integrity of medical images, evaluation criteria need to be identified first to verify that all the defined criteria have been fulfilled before releasing the watermarked image into the medical pipelines. Four principal requirements can be utilised to assess the performance of the proposed watermarking technique; imperceptibility, reversibility, capacity, and robustness (Qasim et al., 2018a, Mousavi et al., 2014).

Irreversible watermarking approaches are subjected to non-acceptance by clinicians while the original unmodified images are favoured for diagnosis purposes. Reversible watermarking methods not considering imperceptibility issue since original unmodified images can be recovered at extraction. However, this feature has been considered in this research because there could be a need to urgently work on the watermarked image before extracting the encoded data. The reversibility of the proposed approach has been evaluated, at extraction, to verify the ability to retrieve the original unmodified images. Physical measures, as well as visual trial, have been implemented to evaluate the watermarked images to ensure that the requirement of imperceptibility has been met.

Low capacity watermarking techniques are preferred for authenticity and integrity applications to achieve high invisibility. The size of the watermark, used in this research to ensure the authenticity and integrity of medical images, after using a lossless compression technique (RLE) is approximately 1KB. The proposed watermarking approach embeds the watermark data into the informative section of medical images (ROI), which is crucial in medical investigations, to protect it against manipulations. Therefore, the proposed approach can be implemented to encode the watermark data into medical images even the size of the ROI part is small.

This research aims to confirm the authenticity and integrity of medical images. Therefore, a fragile watermarking technique is preferred to discover the slight manipulations that may occur on medical images. Any manipulations applied to the watermarked images must corrupt the embedded data resulting in a mismatch between the original and the extracted watermarks. Authenticity and integrity of watermarked images are verified if and only if the encoded data and the original unmodified image can be precisely retrieved. In this research, several physical measures have been utilised to compare the embedded and extracted watermarks as well as the original and retrieved images after applying various image processing operations to simulate image data manipulations to verify the fragility of the proposed approach against manipulations.

6.4 Integration of the Proposed Approach into Medical Imaging

After the proposed watermarking approach has been designed, developed and evaluated in terms of achieving all the identified medical imaging requirements, it is essential to integrate the approach into medical systems or PACS infrastructures (Fig. 6.3). The proposed scheme can be introduced into the PACS workflow as follows:

Acquisition Phase

- Acquisition gateway receives the raw images from acquisition machines and transforms them into standard DICOM format.
- Watermark data is encoded into the raw images as soon as they are received from the acquisition gateway. Each image is watermarked independently.
- Watermarked images are verified to ensure their integrity before they are being transferred to the PACS server.

Archiving Phase

- Local PACS receives the watermarked images from the acquisition phase and verify the integrity and authenticity of these images before archiving.
- Each PACS includes two databases; one for storing the verified images and another for storing the unverified images. The watermarked images are archived in one of these databases according to the verification result.
- The watermarked images are also verified when received by another internal/external PACS before archiving.

Viewing Phase

- The watermarked images are downloaded from the database of verified images when requested by a clinician.
- Watermark data is extracted and validated, and original unmodified images are retrieved.
- Original images are shown to the radiologist alongside the verification report. This gives the clinician the certainty of being viewing images that have not been manipulated (neither by an attacker nor by the watermarking technique).
- In case of urgent requests, watermarked images are shown to the radiologist and the verification process is managed independently. The radiologist is immediately notified if the verification process reveals a manipulation.

6.5 Validation of the Proposed Medical Imaging Workflow

Validation of watermarking approaches is a challenging issue that has not been widely investigated in the literature. There is no current standard on the usage of watermarking in medical imaging and development of a watermarking approach for a healthcare provider depends on its infrastructure and its related entities. Ethical and legislative concerns about modifying image are decreasing the applicability of digital watermarking for medical images. Therefore, this work concentrates on designing a framework for validating the applicability of the proposed watermarking technique to medical environments. To achieve this, security threats that may face medical images during their exchange over medical pipelines need to be identified first to ensure the ability of the approach to tackle the determined security risks and provide a secure climate for medical imaging workflow. An in-depth survey is conducted to analyse the security flaws in the medical imaging systems and the process of integrating the proposed technique into medical domains is then validated. Two studies have been found; one related to manipulation of medical images within the PACS database (Fontani et al., 2010) and another study related to tampering with images during transmission (Selvam et al., 2017). In addition, two potential security issues have also been identified in this research. The first issue related to the manipulation of images after capturing and before transmission to the PACS. The second issue related to the modification of images in the workstations when the images are requested for examinations. This section comprises two main parts: the security hazards that may face the medical images during routine practices are reviewed, and the ability of the proposed approach to tackle these threats is then discussed to provide a protected medical imaging workflow.

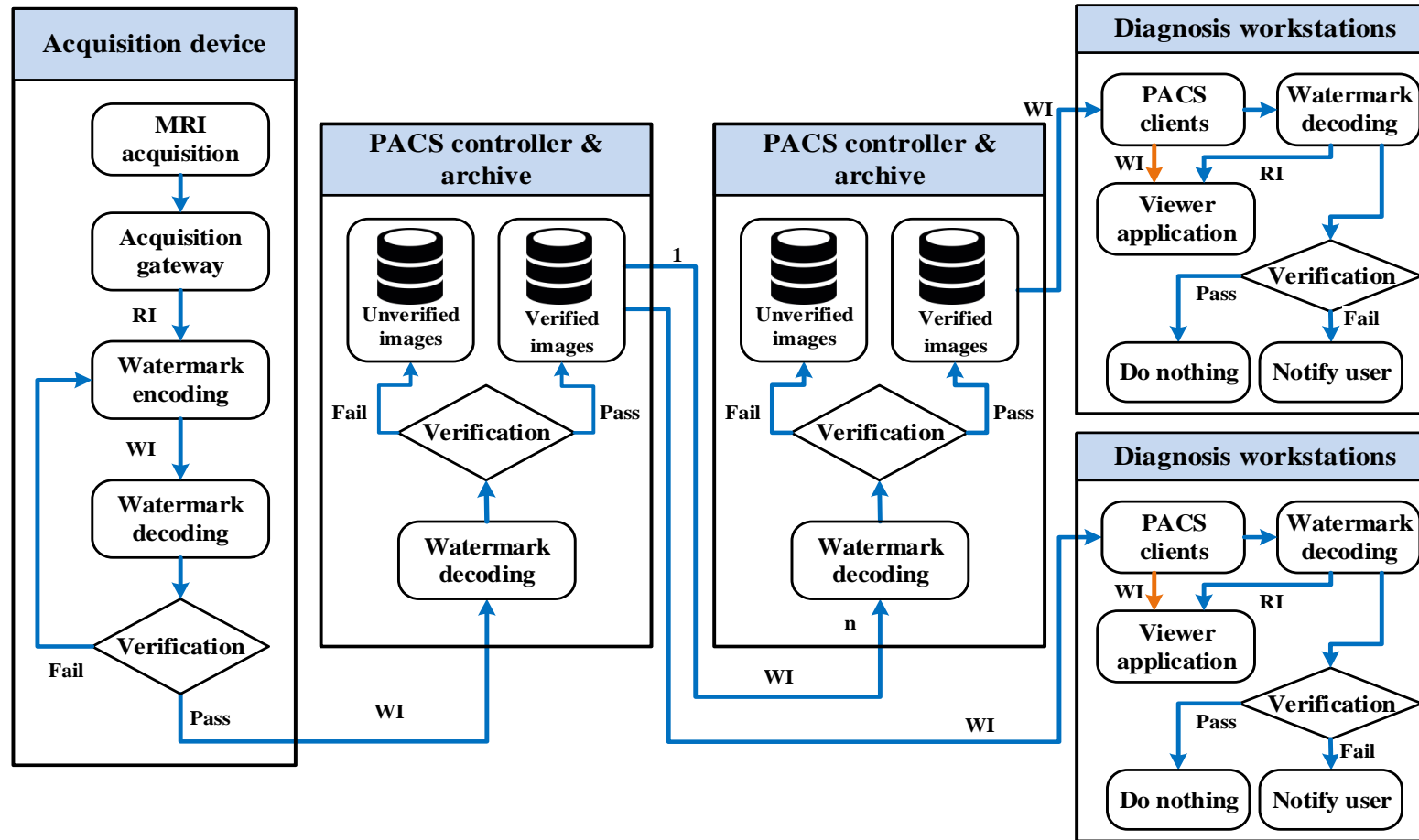


Fig. 6.3: Integration of the proposed watermarking approach into PACS infrastructures. Watermark data is encoded into the raw images (RI) as soon as they are received from the acquisition gateway. Watermarked images (WI) are verified before archiving and during viewing to confirm integrity and authenticity.

6.5.1 Security Threats in Medical Imaging Workflow

Despite the many advantages that modern healthcare systems offer, they are vulnerable to a wide range of security threats that can take place on each level of medical imaging workflow including image acquisition, transmission, viewing, and archiving (Fig. 6.4).

6.5.1.1 Scenario One (S1) – Acquisition Phase

Acquisition devices capture digital images of patients according to the required examination. The captured images are gathered by the acquisition gateway and stored in a cache before transmission to the PACS for archiving and using for medical investigations. During this time, the images can be manipulated which can, therefore, impact the originality of the image data utilised for diagnosis purposes.

6.5.1.2 Scenario Two (S2) – Transmission Phase

Most of healthcare providers concentrate on protecting images within their data centres, but also there are many circumstances in which the images are subjected to manipulate through exchanging within the hospital's internal network or when transmitted to another hospitals or clinicians. This is a critical issue where various operations can be applied to manipulate the images.

6.5.1.3 Scenario Three (S3) – Viewing Phase

Medical images are downloaded from the PACS database to diagnosis workstations when requested for medical examinations. These images can be modified and re-archived in the PACS database or re-send to another user. In this case, there is no ability to detect the manipulations as there is no verification system neither in the PACS nor in the workstations.

6.5.1.4 Scenario Four (S4) – Archiving Phase

This is the most serious scenario of security threats which can be applied to the PACS database where medical images are archived for short-term or permanently. These threats need to be identified first to provide a secure platform for medical imaging workflow that can address these threats. To achieve this, a research paper has been considered as a case study to identify security risks that may face medical images stored in the PACS database (Fontani et al., 2010). This aids in analysing the PACS workflow and understanding the security requirements derived from the medical side to determine a suitable approach for integrating the proposed watermarking technique into medical imaging. The selected

research declares three main critical situations that may face medical images inside the PACS database.

- **Critical Situations 1 (CS1):** Medical images inside PACS can be manipulated due to the difficulty of predicting security issues for each intermediate system.
- **Critical Situations 2 (CS2):** PACS technicians, which have access to both metadata as well as image pixels, are permitted to modify the images as required for adjusting potential flaws in patients' images before the consolidation process.
- **Critical Situations 3 (CS3):** In case of modifying medical images in top-PACS, it will be impossible to automatically discover the manipulation in hospital systems, which requested the images, because authorised archives are stored offline and images are not quickly accessible.

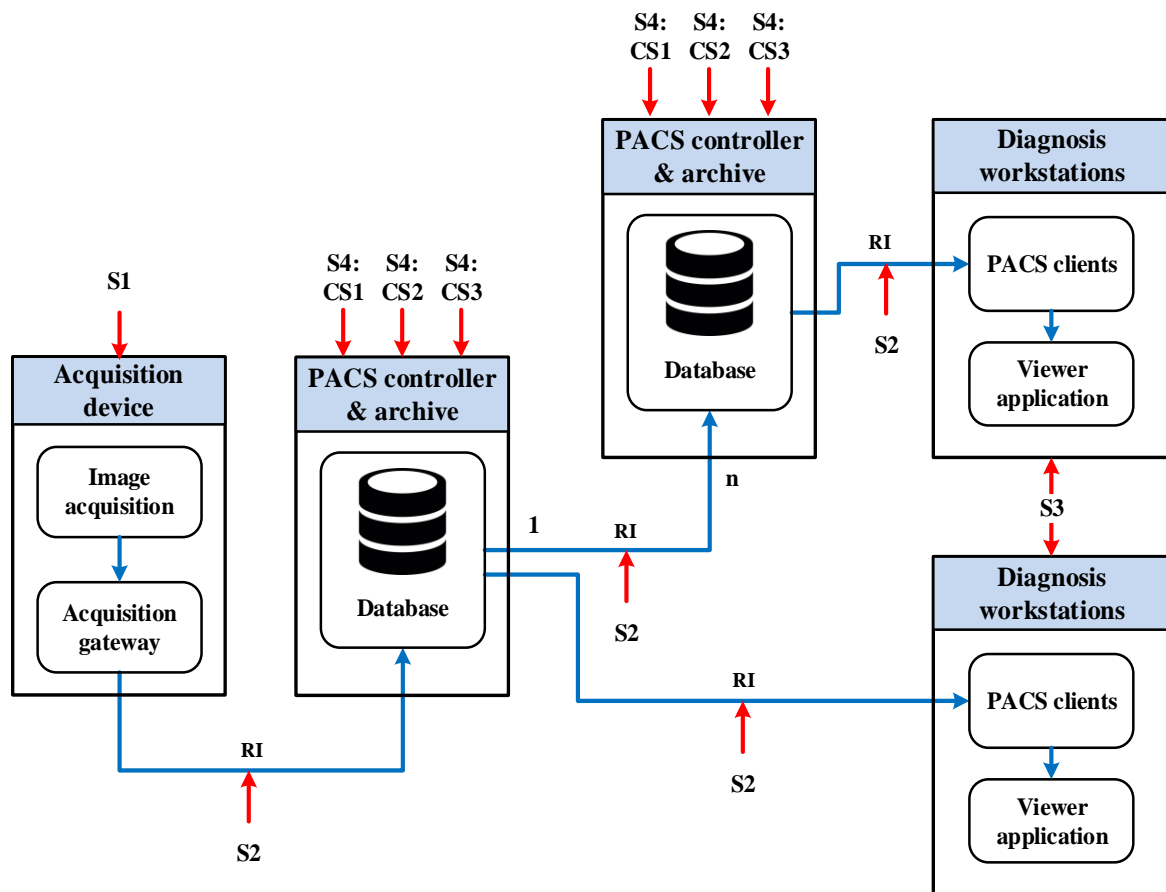


Fig. 6.4: Security threats that may face medical imaging during routine medical practices. Various scenarios (S1, S2, S3, S4) can be applied to manipulate medical raw images (RI) within medical imaging workflow during acquisition, transmission, viewing and archiving.

6.5.2 Validation of the Proposed Integration Process

In order to verify the capacity of the proposed watermarking approach to work in the digital medical imaging workflow, its ability to deal with the identified security threats and realise the defined medical imaging requirements need to be tested and verified. The ability of the approach to detect manipulations of medical images during routine medical practices, for each identified scenario of security threats, has been examined and validated (Fig. 6.5)

6.5.2.1 Scenario One (S1) – Acquisition Phase

The proposed approach suggests encoding watermark data into medical images as soon as they are captured in the acquisition phase. After watermarked images are transferred to the PACS server, they are verified instantly to confirm their validity and integrity to detect manipulations that may be applied during the acquisition process. The proposed approach stores both the verified and manipulated images in two different databases to allow the database administrator to conduct required investigations.

6.5.2.2 Scenario Two (S2) – Transmission Phase

The integrity of watermarked images is verified with each transmission before they are stored in the PACS database or shown to viewers. Any manipulation to images during transmission can be immediately detected. The manipulated images are inserted into the database, which is dedicated to storing the unverified images, when received by local or external PACS. In the workstations, the diagnosis phase, the manipulated images are shown to clinicians alongside a notification demonstrating that the displayed images are unauthorised and have been tampered.

6.5.2.3 Scenario Three (S3) – Viewing Phase

Matching to the transmission phase, modification of images, that may happen during the viewing phase at diagnosis workstations, can be discovered when re-archived in the PACS or re-sent to another workstation for viewing.

6.5.2.4 Scenario Four (S4) – Archiving Phase

Watermarked medical images, which are saved permanently inside the PACS database, may face three critical situations (CS1, CS2, CS3). The proposed approach has the ability to address all of these critical situations by detecting modifications during transmission to another internal or external PACS or when requested for viewing at diagnosis workstations.

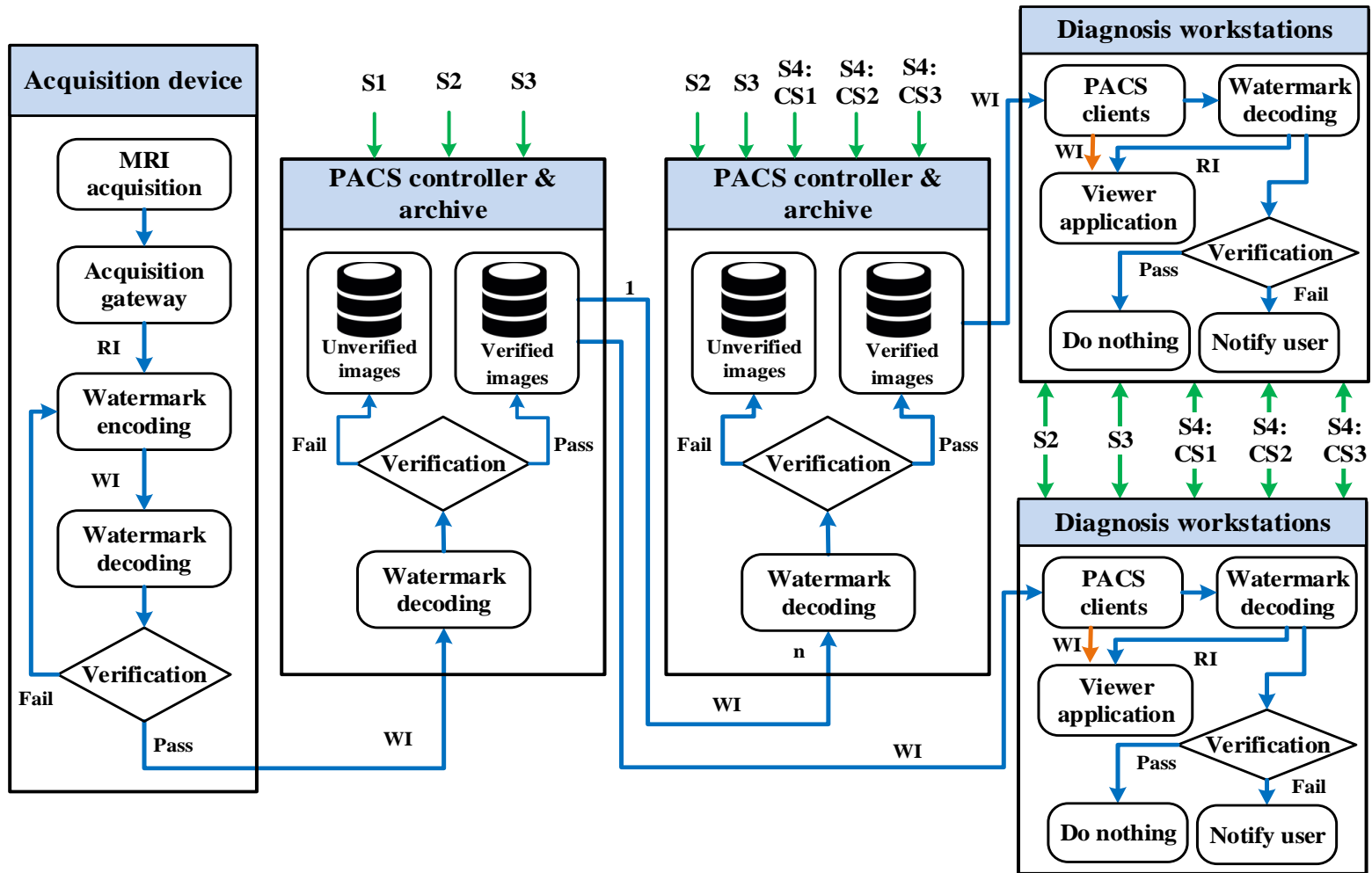


Fig. 6.5: Validation of the ability of the proposed approach to tackle the identified security threats (scenarios) that may face medical images during routine medical practices. Manipulations of medical images can be detected in all phases of medical workflow including acquisition, exchanging, viewing and archiving.

6.6 Chapter Summary

Modern healthcare systems act as integrated platforms for capturing, transmitting and storing medical images. During routine medical practices, many operations can be applied to these images through which the image data is modified. Therefore, the need for ensuring the integrity and authenticity of these images has become crucial. Digital watermarking is recognised as a sturdy technique for enhancing trust within the medical imaging by detecting the manipulations. However, there is a hesitation of accepting digital watermarking in medical fields due to the majority of existing approaches not taking into account the essential requirements of the medical imaging workflow.

In this chapter, the essential requirements of medical imaging have been identified and reviewed and the proposed watermarking approach, which was developed to detect manipulations, has been integrated into medical imaging systems to provide a secure platform for medical images workflow. This has been theoretically validated because of the reluctance of using digital watermarking in medical domains due to the ethical and legal concerns about modifying patients' images. To accomplish this, security threats, drawn from case studies and this research, that may face medical images during the routine medical practices have been identified to verify the ability of the approach to address these threats through detection of manipulations of medical images during acquisition, transmission, viewing, and archiving.

CHAPTER SEVEN

Discussion

This chapter presents a critical evaluation of the research undertaken and reviews the aim and objectives of the work carried out. The relevance of digital watermarking in medical imaging systems is demonstrated to validate its ability to address security threats that may face medical images during the routine medical workflow. The methodology is reviewed, and its impact on the research is discussed. The principal contribution chapters are considered and summarised, with reference to how they have addressed the identified research questions to achieve the objectives of this study.

7.1 Critical Evaluation of Research

This research concentrates on enhancing trust in digital medical environments by applying robust controls within the medical imaging workflow to ensure the authenticity and integrity of medical images. The approach undertaken was to investigate the existing digital watermarking techniques and identify the essential requirements of medical imaging workflow to, therefore, propose an efficient watermarking approach that can fulfil the fundamental requirements of clinical workflow.

A definitive review article (Mousavi et al., 2014) has presented a comprehensive survey on digital watermarking techniques applied to medical images to provide an obvious scene for interested researchers by analysing the strengths and weaknesses of various existing approaches. This article has defined four particular requirements that must be considered when applying digital watermarking to medical imaging. These requirements include imperceptibility, reversibility, integrity control and authentication, therefore, this research sought to develop a watermarking approach that can fulfil these key requirements.

7.1.1 Imperceptibility

Imperceptibility is the most significant requirement of invisible watermarking techniques since any slight modification to original images could lead to serious consequences relating to diagnosis and treatment. Embedded watermark is defined as imperceptible if original and modified images are perceptually indistinguishable and this is significant for the secrecy and confidentiality of the encoded data. In medical domains, the question of how much data could be encoded within the medical image without impacting its visual quality became a

significant issue and require to be investigated before releasing the modified images into the medical workflow. This is also important to determine a set of guidelines for encoding the watermark, in terms of technique and level of modification, to verify that the modified image has no noticeable difference to the original. Imperceptibility of watermarking approaches can be assessed either physically or visually and visual measure are most appropriate for evaluating the visual quality of watermarked medical images. However, they need special conditions and preparations for implementing making them expensive, complicated and time-consuming.

In this research, both assessment methods were adopted to evaluate the distortion level of the watermarked images, but a special concern was given to the visual evaluation. Relative VGA was chosen to visually evaluate the images due to its ability to determine even slight changes between anatomical structures of tested images. Three different reversible watermarking methods, based on the DE technique, have been applied to eight different medical images to generate a set of watermarked images with various distortion levels. Standard PSNR and SSIM metrics have been used to physically measure the distortion level between the original images and their corresponding watermarked versions. In the visual assessment, all watermarked images were compared to a reference image by inviting five qualified radiographers, who are experienced in diagnostic radiography, to assess the differences between the tested images based on eight criteria derived from standard guidelines for assessing the visual anatomical details of brain radiographs (Menzel et al., 2000). A five-point Likert scale, ranging from strongly disagree to strongly agree, was used to grade the criteria items. Relating this to objective measures for image fidelity (PSNR) is then undertaken to define quantitative criteria to guide the selection of watermarking technique and enable an objective post modification assessment of the watermarked image to ensure the condition of imperceptibility is met. The outcomes propose that, if a watermarking technique is applied to 512x512 pixel (16bpp grayscale) brain MR images used in the investigation, a subsequent assessment of PSNR=82 dB or greater would mean that there would be no reason to doubt that the watermark would be visually noticeable, and modification level to a PSNR=80 dB should not be detectable in the vast majority of situations.

This research has undertaken a robust and reliable approach for evaluating the imperceptibility issue of watermarked images. However, some limitations can be observed and require to be taken into consideration in future studies:

- This sample size of images can be considered as an issue for limitation, although a relatively large sample size of images was generated after implementing the three different watermarking methods.
- The physical measures used to assess the image distortion were based on PSNR and SSIM values only. These metrics are efficient, simple and easy to implement. However, it would be beneficial to consider including other objective measures.
- The sample size of observers can be considered as a limitation and increasing the number of participants may provide more accurate results and conclusions.
- The sample of participants was deemed to be sufficient for this trial since it sought to evaluate the differences in the anatomical structures of tested images. However, involving more experienced images' readers (e.g. radiologists) may enhance the outcomes by evaluating the impact of the encoded watermark on the diagnosis.
- The visual degradation boundary (PSNR) was only evaluated for brain MR images in DICOM format (16bpp, 512×512 pixels) and this may differ if other image characteristics were used. Therefore, additional investigation and validation are required to confirm either the calculated threshold of PSNR value or evaluate a correct PSNR for the particular image characteristics.

7.1.2 Reversibility

Modification of image data, as a result of embedding a digital watermark, no matter how slight the modification is may cause distortion to original images. In medical domains, if an image is manipulated during the workflow a breakdown in trust regarding the integrity of the images is formed. Any small modification to the medical images could cause an error in diagnosis and treatment with possible life-threatening ramifications, or legal consequences. Therefore, retrieving the original unmodified image after extracting the embedded data is necessary and must be considered when utilising digital watermarking in medical domains. Fully reversible watermarking approaches can tackle this issue by applying a technique that can recover both the encoded data and the entire original image after extracting the watermark successfully. Reversible watermarking can be classified into four categories; compression based, histogram modification based, quantisation based, and DE-based. Reversible watermarking based on the DE technique have overridden the other reversible methods in terms of providing greater hiding capacity and lower computational complexity (Qasim et al., 2018a, Khan et al., 2014). However, reversible watermarking techniques based on DE require the location map of pixels used for encoding the watermark at extraction. This

huge amount of side information reduces the hiding capacity and increases the distortion level of watermarked images.

In this research, a reversible watermarking approach based on the DE is proposed which can recover the exact original image without the need for any auxiliary data (e.g. location map). This significantly improves embedding capacity whilst also decreasing potential image distortion. The proposed approach automatically divides the medical images into two sections; ROI and RONI, with the watermark data encoded into smooth blocks (3x3 pixels) inside the ROI part to realise watermarked images with lower degradation. The ability of the proposed approach to retrieve the original unmodified images was evaluated at extraction using several mathematical metrics including PSNR, SSIM, RMSE, and IF. The obtained results confirmed the reversibility of the approach and the complete original image can be restored without any loss after extracting the encoded data.

7.1.3 Integrity Control and Authentication

Integrity control refers to the ability to ensure that images have not been manipulated, while authentication denotes the ability to verify that images belong to the correct patient. Images integrity can typically be accomplished by hiding the DS or MAC of images. Images authenticity can be achieved by hiding the EPR data or using the full DICOM header or some of its fields to ensure that the images belong to the right patient. At extraction, the integrity and authenticity of medical images can be verified by retrieving the encoded data precisely. Manipulations of the images must distort the hidden data resulting in a mismatch between the original and retrieved watermarks. Therefore, a fragile watermarking method is favoured to detect the slight modifications that may apply to medical images.

A fragile and reversible watermarking approach was developed in this study to encode the essential metadata fields, extracted from the DICOM header, and DS of the entire images into medical images to confirm integrity and authenticity of the images raw data as well as header information. Twenty-five brain MR images in DICOM format (16bpp, 512×512 pixels) were utilised to evaluate the performance of the proposed method based on four identified essential requirements of medical image watermarking to verify its efficiency and applicability. These requirements comprise imperceptibility, reversibility, capacity, and robustness (Qasim et al., 2018a, Mousavi et al., 2014).

7.1.3.1 Imperceptibility

Reversible watermarking not taking into consideration the imperceptibility issue since the original images can be retrieved at extraction. However, this issue has been considered in this study because in some urgent situations there may be a need to work on the watermarked data before extracting the embedded data. PSNR, SSIM, RMSE, and IF metrics were used to estimate the distortion level of watermarked images and this was also evaluated through the visual assessment (relative VGA). The obtained results indicate that the degradation of the watermarked images is very trivial and cannot be visually detected, and the proposed approach achieved the most important requirement of digital watermarking schemes which is the imperceptibility.

7.1.3.2 Reversibility

Reversibility of the approach was assessed at extraction to verify the ability to retrieve both the encoded data and original unmodified image by utilising various mathematical metrics. PSNR, SSIM, RMSE and IF were used to compare the differences between the original and extracted images, while BER and AR metrics were used to compute the number of incorrect and correct bits between the encoded and extracted watermarks. The obtained results confirm the reversibility of the approach and the original images and watermarks can be fully retrieved without any loss.

7.1.3.3 Capacity

The capacity of watermarking schemes can be measured by calculating the number of pixels required for encoding watermark data. The proposed approach conceals the watermark in the ROI section of medical images making the embedding capacity depends on the size of the ROI part. The size of the watermark data, used in this study to verify the integrity and authentication of medical images, is approximately 1KB after adopting a lossless compression technique based on RLE. Therefore, the medical images can carry the watermark data even the size of the ROI section is 8% of the whole image and the hiding capacity rises with the increasing of the ROI size.

7.1.3.4 Robustness

Fragile watermarking techniques are preferred for integrity and authenticity applications to detect alterations that may occur in medical images. Any modification of medical images must corrupt the encoded watermark leading to a mismatch between the embedded and

extracted watermarks. Therefore, integrity and authenticity of images are verified, if and only if, the encoded watermarks and original images can be recovered precisely and exactly matched. To assess the fragility of the proposed approach, various image processing operations were applied to the watermarked images simulating image manipulations. PSNR was used to evaluate the ability to recover the original images and BER was used to evaluate the ability to retrieve the original watermarks after applying the manipulations. The results confirm that this approach is fragile against the applied operations and it can detect even the slight modifications.

In this research, a novel reversible and invisible watermarking approach was developed to verify the integrity and authenticity of brain MR images for discovering image manipulations. The performance of the approach was evaluated based on the fundamental requirements of the medical domains to confirm its applicability and suitability to medical imaging. However, some issues can be considered as limitations and need to be taken into account in future studies:

- The proposed technique was only applied to MR images. Evaluating the performance of the approach through utilising different modalities (X-ray, Ultrasound and CT) is necessary to ensure its efficiency and applicability to various medical images.
- The proposed approach ensures the integrity and authenticity of images through detecting image data manipulations during the routine medical workflow. However, developing the proposed technique to retrieve the altered regions of images would improve the performance of the approach.

7.1.4 Relevance of Digital Watermarking in Medical Imaging Systems

Medical imaging systems are integrated systems for capturing, exchanging and archiving medical images. Transmission of medical images between hospitals and organisations, located at different locations, is a common habit for many reasons including diagnosis, treatment, external second opinion, and transferring to a second healthcare provider. During use and exchange, these images can be manipulated which may lead to errors in diagnosis and treatment with potentially life-threatening implications, or legal consequences. Therefore, it is substantial to integrate the proposed watermarking approach into the medical imaging systems to check its capacity to deal with the security hazards that may face medical images. To realise that, a theoretical framework has been designed to verify the ability to

utilise the proposed approach in medical domains. Security threats that may occur in medical images during routine workflow were identified and analysed first. Then, the integration of the approach into medical imaging workflow is validated to ensure its ability to tackle the identified security risks.

The proposed integration of the approach within medical imaging workflow assures the ability to address all security threats that may face medical images during acquisition, transmitting, viewing and storing. However, testing the proposed approach in a fully operational PACS, where medical images are archived, retrieved and exchanged, would verify the applicability of the approach in a real-world application scenario of medical imaging.

7.2 Review of Aim and Objectives

This research aimed to ensure trust in digital medical imaging workflow by enabling robust integrity and authenticity controls within medical images. In particular, it was seeking to define and investigate the substantial requirements of medical imaging to develop a watermarking technique that can fulfil these requirements besides ensuring the authenticity and integrity of medical images. Specifically, the objectives of this research were:

- **O1:** Identify and study the essential requirements of medical imaging workflow that are required to be considered when applying digital watermarking to medical imaging.
- **O2:** Develop a novel visual assessment approach to evaluate the differences between the anatomical structure of medical images, modified by varying techniques and magnitudes, to define heuristic guidelines for the watermarking techniques and level of changes that can be applied to hide a known magnitude of payload in an invisible manner.
- **O3:** Develop a novel watermarking approach that can ensure the integrity and authenticity of medical images, by detecting image manipulations, in addition to the achievement of the essential requirements of medical imaging.
- **O4:** Propose and design a theoretical framework to integrate the developed watermarking approach into medical imaging workflow to ensure its ability to operate in a real PACS scenario where medical images are captured, exchanged and archived.

- **O5:** Assessment of the proposed watermarking approach to ensure that the research aim and the essential requirements of medical imaging have been realised before releasing the watermarked images in medical pipelines.

The first objective of this research (**O1**) was achieved by conducting a comprehensive survey (Chapter 3) to identify the strengths and limitations of various existing techniques of digital watermarking that developed to enhance the trust in medical imaging workflow. This contributed to defining the particular requirements of medical images watermarking to select the appropriate techniques and approaches for this research. In medical domains, the question of how much data could be concealed into medical images is significant and require to be inspected before releasing the watermarked images into the medical workflow to define a set of guidelines for determining techniques and level of modification that can be applied without impacting the visual quality of medical images. Achievement of this objective (**O1**) contributed to addressing the third research questions (**Q3:** What are security tools that can be used to ensure the integrity and authenticity of medical images?) and the fourth research question (**Q4:** What are the fundamental requirements of medical imaging workflow when utilising digital watermarking within medical domains?).

The second objective of this research (**O2**) was to define a perceptual boundary, below which change is noticeable, to identify heuristic guidelines for the techniques of watermarking and the level of modification that can be applied to encode a known magnitude of payload data in an imperceptible manner. This objective was attained by implementing a visual assessment based on relative VGA (Chapter 4) to determine the range of modification, for brain MR images, within which changes to the image data (pixels) are unperceivable to the observer. Relating this to objective measures for image fidelity (PSNR) is then undertaken to define quantitative criteria to guide the selection of watermark encoding technique and enable an objective post modification assessment of the watermarked image to verify the condition of imperceptibility is met. Achievement of this objective (**O2**) contributed to addressing the seventh research questions (**Q7:** What is the watermarking modification level that can be applied to medical images so that these images remain acceptable for medical investigations?) and the eighth research question (**Q8:** Which approach is appropriate for assessing the perceptual distortion of watermarked medical images?).

The conducted visual evaluation contributed to the achievement of the third objective (**O3**) through developing an efficient watermarking approach (Chapter 5) to enhance trust within

medical environments by confirming the integrity and authenticity of medical images. The proposed scheme delivers highly invisible watermarked images evaluated through utilising objective measures as well as the implemented visual assessment approach. Integrity and authenticity of medical images were also verified through discovering subsequent manipulations enacted on the watermarked images. This enhanced security measure, therefore, enabled the detection of image manipulations, by an imperceptible and reversible approach, which may establish increased trust in the digital medical workflow. Achievement of this objective (**O3**) contributed to addressing the second research question (**Q2: Have the images been manipulated whether intentionally or accidentally and how to detect these manipulations?**) and the fifth research question (**Q5: Which digital watermarking techniques can satisfy the particular requirements of medical imaging workflow?**).

Achieving objectives four and five (**O4** and **O5**) requires evaluating and validating the applicability of the proposed watermarking approach to medical domains. This was fulfilled by defining security threats that may face medical images during regular medical operations to verify the ability of the proposed approach to address the identified security threats. The watermarking scheme was also evaluated based on the requirements of medical domains to verify its applicability and suitability. The proposed integration of the approach within medical imaging workflow (Chapter 6) validates the ability to reveal manipulations that may occur on medical images whilst meeting the essential requirements of digital medical imaging. Achievement of these objectives (**O4** and **O5**) contributed to addressing the first research question (**Q1: What are the security risks that may face medical images during routine clinical practices?**) and the sixth research question (**Q6: What are the appropriate criteria for evaluating the suitability of the proposed watermarking technique for medical imaging?**).

7.3 Review of Methodology

The methodology applied sought to develop a watermarking approach that can enhance trust in medical domains by enabling strong integrity and authenticity controls within medical images besides fulfilling the essential requirements of digital medical imaging. The methodology applied was implemented, evaluated, improved and validated to present a robust and repeatable methodology for investigating, defining, and validating digital watermarking techniques across the wide range of digital medical imaging modalities for adoption in future researches.

The first phase of this study was to investigate digital watermarking approaches applied to medical imaging to identify problems related to applying digital watermarking to medical images and formulate the research questions and objectives. These formed the foundation of this research, which was conducted through the iterative improvement and evaluation of the developed approach to assess the performance and ensure the achievement of the research aim. Four particular requirements were stated in the literature and suggested to be considered when applying digital watermarking to medical images (Mousavi et al., 2014). These requirements, which include imperceptibility, reversibility, integrity control, and authentication, were considered as the principal key to this research and contributed to the establishment of the research questions and objectives.

Deep investigation into each of these requirements was then undertaken to identify the appropriate techniques and approaches for this research. This investigation led to the need for defining the level of modification that can be applied to medical images without causing visual distortion. This was achieved by conducting a visual assessment to evaluate the visual quality of brain MR images, watermarked by varying methods and magnitude of image modification, to identify where this perceptual boundary exists and relate the point at which change becomes noticeable to the objective measures of the image fidelity evaluation. This aided in selecting the techniques of watermarking and the level of modification that can be applied to encode a known magnitude of payload data in an imperceptible manner. A new reversible and imperceptible watermarking approach was then developed to ensure the integrity and authenticity of brain MR images to confirm that the manipulation of images can be revealed and tracked. The performance of the proposed approach was evaluated based on the four defined essential requirements of medical images watermarking to verify its efficiency and applicability. Integration of the proposed watermarking approach into medical imaging systems was then undertaken to validate its ability to address security threats that may face medical images during routine clinical practices.

Iterative evaluation and development were also undertaken to the proposed approach throughout the research phases to ensure that the aim and objectives of this research have been realised before releasing the watermarked images in the medical workflow. In order to report the identified research problem and obtained outcomes, a number of research papers were published in different journals and conferences to present the conducted research survey, proposed and developed approaches, and evaluation and validation results.

7.4 Research Contributions and Implications

The literature survey of this research (Chapters 3) presents a comprehensive review of recently published studies in the field of digital watermarking applied to medical images for the purpose of integrity and authentication. This investigation contributed to identifying the shortcomings of various existing techniques and provided a clear path for developing approaches to address these limitations and achieve the objectives of this research. This work was published in *Computer Science Review* journal (Qasim et al., 2018a).

The research undertook to implement the visual assessment (relative VGA) to investigate the imperceptibility issue (Chapter 4) was published in *Signal Processing: Image Communication* journal (Qasim et al., 2019b). This investigation presented a novel assessment approach for evaluating and validating the distortion level of watermarked images before they are introduced into the medical imaging workflow. No similar investigation conducted before to visually evaluate the watermarked MR images by using standard quality criteria dealing with the visibility of the anatomical details of the brain.

A new reversible and imperceptible watermarking approach (Chapter 5) was developed to ensure the integrity and authenticity of medical images and to confirm that manipulations, that may occur on images during routine medical operations, can be detected. The performance of the proposed approach was assessed based on the defined principal requirements of medical images watermarking to ensure its validity and applicability to medical imaging workflow. This work was presented at ICAC'18 (Qasim et al., 2018b) and also published in *Multimedia Tools and Applications* journal (Qasim et al., 2019c).

The integration of the proposed watermarking approach into medical imaging systems (Chapter 6) verified and validated the applicability of the approach to medical imaging workflow. This work deeply investigated the security hazards that may face medical images in the PACS workflow during acquisition, viewing, exchanging, and archiving. Then, the developed approach was tested, evaluated, and validated to ensure its ability to operate in a real application scenario (e.g. PACS) to verify that manipulations of medical images can be discovered and tracked. This work verifies the fulfilment of the essential requirements of digital medical imaging as well as enabling robust integrity and authenticity controls within medical imaging workflow. This work was presented at DESSERT'2019 (Qasim et al., 2019a).

An additional contribution to the research includes the development of a novel methodology which is adopted to achieve the aim and objectives of this research. This methodology was implemented, evaluated, and validated to offer a strong and repeatable methodology for investigating digital watermarking techniques across the vast range of medical imaging modalities for following and adopting in future studies.

CHAPTER EIGHT

Conclusion and Future Research

This chapter presents a summary of the final conclusions that can be drawn based on the research presented in this thesis. A statement of novelty and limitations of this research are summarised with some suggestions for future studies.

8.1 Conclusion

This research concentrates on studying digital watermarking to present a systematic way of designing, implementing, evaluating and validating it, with a particular concentrate on providing a secure medical imaging system. Digital watermarking is a promising and evolving technique for enhancing the security of multimedia objects. Digital medical images, on the other hand, are the consequence of the developed imaging technology that has enabled modern health providers to seamlessly present many remote medical services. The exchange of these medical images across hospitals and administrative organisations, located at different sites, has become a common practice for many reasons within the digital medical workflow. Many cases of manipulations can be applied to medical images which may lead to serious consequences on diagnosis and treatment of patients. Thereby, under these circumstances, the ability to ensure the integrity and authenticity of these images is crucial, both within the internal systems and during their transfer to other healthcare providers.

The aim of this research was to ensure trust in digital medical workflows by enabling robust authenticity and integrity controls within medical images. This was achieved by identifying and investigating the essential requirements of the medical imaging workflow before developing techniques and approaches for this study. The process of research was devised to answer the determined research questions (Section 1.3) and accomplish the aim and objectives of this research (Section 1.4), in addition to the fulfilment of the identified requirements of medical imaging (Section 3.2).

The work conducted in this research has produced three substantial contributions. The most evident of these is the development of a novel visual assessment approach for evaluating the visual quality of watermarked images (Qasim et al., 2019b). However, realising this aided in achieving two other contributions; a new imperceptible and reversible watermarking approach for verifying the integrity and authenticity of medical images by revealing

manipulations that may apply to the images during the routine medical workflow (Qasim et al., 2018b, Qasim et al., 2019c), and a novel theoretical framework to verify the ability of the proposed watermarking approach to operating in a real application scenario (e.g. PACS workflow) to detect manipulations of medical images (Qasim et al., 2019a). In addition to these substantive contributions, there is also a methodological contribution in the development of the watermarking approach which was adopted to enhance trust in medical environments. This methodology was designed, implemented, evaluated and validated to present a strong and repeatable methodology for studying, analysing and validating digital watermarking techniques across the wide range of medical imaging modalities for using in future researches.

In the early stages of this study, current medical images watermarking approaches were reviewed and investigated (Chapter 3) to identify the research gap and define the criteria for designing and evaluating this work. This contributed to the identification of the essential medical imaging, and workflow, requirements to develop techniques and approaches required for achieving the research objectives. A decisive review article defined four substantial requirements that must be considered when applying digital watermarking to medical images; imperceptibility, reversibility, integrity control, and authentication (Mousavi et al., 2014). These requirements were considered as the principal key to this PhD study and were studied and investigated in deep to develop, evaluate and validate the proposed approaches (Qasim et al., 2018a).

Unlike reversibility, for which an objective evaluation can be easily implemented, imperceptibility is an aspect of human cognition that requires to be assessed within the human context. Therefore, a visual evaluation approach (Chapter 4) was conducted on 117 brain MR images (8 original and 109 watermarked), modified by using three different reversible watermarking techniques to encode various amount of magnitude to define a perceptual boundary, below which change is perceptible, to determine heuristic guidelines for the method of watermarking and the level of modification that can be applied to embed a known magnitude of payload data in an imperceptible manner. The original and watermarked images were shown to the observers (five qualified radiographers) together at the same time on two separated and identical monitors and the observers were asked to identify the differences between the images based on standard criteria deal with the clarity of the anatomical structures of the brain. Connecting this to physical measures for image fidelity (PSNR) is then undertaken to define quantitative criteria to guide the selection of

watermark encoding technique and enable an objective post modification assessment of the watermarked image to verify the requirement of imperceptibility is met. The results proposed that, when applying digital watermarking to medical images, the modification of the images to a level of PSNR=82 dB or higher, between the original and watermarked images, is invisible to all observers, and modification level to a PSNR=80 dB should not be detectable in the vast majority of situations (Qasim et al., 2019b).

The visual assessment had a great impact on the development of a new reversible watermarking approach (Chapter 5) to ensure the integrity and authenticity of medical images to confirm that manipulations can be revealed and tracked, and this is the main objective of this research. The proposed approach automatically segments images into two parts; ROI and RONI, and the watermark data is encoded into the smooth blocks inside the ROI section by using an extended reversible watermarking method based on DE technique. The precise original images can be retrieved, after retrieving the encoded data successfully, without the need for a location map of the employed pixels to control and maximise hiding capacity whilst reducing image degradation. Experimental results showed that the proposed approach delivered highly imperceptible watermarked images, at PSNR (92.18-99.94 dB), SSIM=1, RMSE (0.0109-0.0670) and IF (0.9998-1), which were also evaluated through the conducted visual trial (relative VGA). This compared favourably to outcomes reported under current state-of-art techniques. Integrity and authenticity of medical images were also ensured through detecting subsequent changes enacted on the watermarked images. This enhanced security measure, therefore, enables the detection of image manipulations, by an imperceptible and reversible approach, that may establish increased trust in the digital medical workflow (Qasim et al., 2018b, Qasim et al., 2019c).

After the proposed watermarking approach has been implemented and evaluated, in terms of achieving the defined essential requirements of medical imaging, its integration within medical systems (Chapter 6) was undertaken to verify its validity and efficiency. To realise this, security threats that may face medical images during routine workflow were identified and investigated first to ensure the ability of the proposed approach to operating in an application scenario (e.g. PACS) for digital medical images where the images are captured, exchanged and archived. Two case studies have been identified; one related to manipulation of medical images within PACS archiving system (Fontani et al., 2010) and another study related to manipulation of medical images during exchanging (Selvam et al., 2017). Furthermore, two potential security issues have also been identified within this research; one

related to manipulation of images immediately after the production and another issue related to the manipulation of images in the PACS workstations where the images are requested for medical investigations. This work sought to verify the achievement of the identified requirements of medical imaging systems as well as the detection of manipulations that may occur on medical images during acquisition, transmission, viewing and storing (Qasim et al., 2019a).

8.1.1 Contributions of Research to Literature

This PhD thesis offers several contributions and achievements in the field of digital watermarking and its application to medical imaging. The research outcomes have been published and presented in several respectable journals and conferences. The main contributions of this study are summarised below:

1. A comprehensive survey (Chapter 3) has been conducted on recent digital watermarking approaches that are aimed to ensure the integrity and authenticity of medical images to define the weaknesses of existing watermarking techniques. This survey contributes to defining the essential requirements of medical imaging to select the appropriate techniques for utilising digital watermarking within medical fields (Qasim et al., 2018a).
2. A novel visual assessment approach (Chapter 4) has been developed and validated to investigate the imperceptibility issue, which represents the essential condition of invisible watermarking approaches. No similar study has been conducted before to visually evaluate the watermarked MR images by using standard quality criteria dealing with the visibility of the anatomical details of the brain. This trial aids in selecting the techniques of watermarking and identifying the level of modification that can be applied to embed a known magnitude of data in an imperceptible manner (Qasim et al., 2019b).
3. A new imperceptible and reversible watermarking approach (Chapter 5) has been proposed to verify the integrity and authenticity of medical images by detecting image manipulations. The watermark data was encoded into the smooth regions inside the ROI part of the image to make the deformation less visually noticeable. At extraction, the encoded data can be retrieved without the need for the location map of pixels used to carry the watermark common in other approaches (Yang et al., 2018, Pan et al., 2018, Roček et al., 2016) to maximise hiding capacity whilst reducing image distortion. (Qasim et al., 2018b, Qasim et al., 2019c).

4. A theoretical framework (Chapter 6) has been developed to test and validate the ability of the proposed watermarking approach to operating in a real application scenario of the medical imaging workflow. No similar study has been conducted before to test digital watermarking in an operational PACS to address security threats that may face medical images during capturing, exchanging and archiving (Qasim et al., 2019a).
5. A new research methodology has been developed, implemented, evaluated, and validated to present a robust and repeatable methodology for investigating and validating digital watermarking approaches over the large range of medical imaging modalities for adopting in future researches.

8.1.2 Limitations of the Research

Although this research proposed robust and reliable approaches for enhancing trust within medical imaging workflow by enabling strong integrity and authenticity controls, several issues can be considered as limitations.

1. The sample size of both the images and observers, adopted in the visual assessment approach, can be considered as a limitation, although a relatively large sample size of images was produced after implementing the watermarking methods.
2. The visual evaluation trial was conducted to identify visual distortion boundary (PSNR) by applying different reversible watermarking techniques to brain MR images in DICOM format (16bpp, 512×512 pixels). The outcomes may differ if other image characteristics were used.
3. The proposed watermarking approach was only implemented, evaluated and validated on brain MRI.
4. The proposed approach can only detect image manipulation without identifying and recovering the altered regions.
5. The proposed watermarking technique does not allow to modify even a single bit of the images. This means that any authorised change to images will be considered as tampering.

6. The proposed technique encodes the watermark data into each image independently. A long time may be required to encode the watermark into a particular patient's images or some of these images.
7. The applicability of the proposed watermarking approach in medical imaging workflow to detect images manipulations was only tested and validated theoretically.

8.2 Future Research Direction

The work presented in this PhD thesis has many contributions to the field of digital watermarking and its application to medical imaging. However, it has opened several possibilities for future studies.

1. Increase the sample size of medical images and involving expert radiologists to visually assess the distortion level of watermarked images. This can be done by adopting the ROC approach to identify whether the modifications applied to medical images impact medical diagnosis, especially the images that have distortion level close to the threshold of imperceptibility.
2. Further investigation and validation are needed to verify either the calculated threshold of visual distortion boundary (PSNR) or evaluate a correct PSNR value for other image characteristics.
3. Develop the proposed watermarking approach and apply it to other medical imaging modalities (e.g. X-ray, Ultrasound and CT) to verify its efficiency and applicability.
4. Extend the proposed watermarking technique for identifying the alteration region and retrieving the manipulated area to improve its performance.
5. As compression is acceptable in DICOM standard, investigation on encoding the watermark in other technique like Discrete Wavelet Transform (DWT) (used in JPEG2000) or Discrete Cosine Transform (DCT) (used in JPEG) should be considered to ensure that the watermark can survive against these compression methods.
6. Develop the proposed watermarking approach and apply it to a set of images (e.g. total patient's images) instead of selecting a single image at a time to reduce the time required for the implementation of the technique.

7. Verify the applicability of the proposed watermarking approach to operate in a fully operational PACS, where medical images are produced, exchanged and archived, to ensure its validity and suitability.
8. It is highly recommended to follow the methodology adopted in this research and apply it to the same dataset of medical images as well as a different dataset to verify its applicability and validity.

APPENDICES

I. Ethical Approval Provided by the University of Salford



Research, Innovation and Academic
Engagement Ethical Approval Panel

Research Centres Support Team
G0.3 Joule House
University of Salford
M5 4WT

T +44(0)161 295 5278

www.salford.ac.uk/

15 January 2019

Asaad Qasim

Dear Asaad,

RE: ETHICS APPLICATION ST1617-58 - A reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images

Based on the information you provided, I am pleased to inform you that your application ST1617-58 has been approved with your new change of title.

If there are any changes to the project and/ or its methodology, please inform the Panel as soon as possible by contacting S&T-ResearchEthics@salford.ac.uk

Yours sincerely,

A handwritten signature in black ink that reads 'A Higham'.

Dr Anthony Higham
Chair of the Science & Technology Research Ethics Panel

II. Research Participant's Consent Form



Research Participant (Volunteer) Consent Form

Visual Evaluation of MRI Brain Images Using Two Alternative Forced Choice Approach

Name of Researcher: *Asaad Qasim*

Please initial box

- I confirm that I have read and understood the information sheet dated 20th February 2017 (version 1.1) for the above study and understand what my contribution will be.
- I have the opportunity to ask questions in person (face to face).
- I understand that the study does not involve any physical or psychological risks.
- I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason.
- I agree to take part in the survey.

Name of Participant:

Signature:

Date:

Name of researcher taking consent:

Signature:

Date:

REFERENCES

- Abd-Eldayem, M. M. 2013. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. *Egyptian Informatics Journal*, 14 (1), 1-13.
- Abdullatif, M., Zeki, A. M., Chebil, J. & Gunawan, T. S. Properties of digital image watermarking. 9th International Colloquium on Signal Processing and its Applications (CSPA), 2013 Kuala Lumpur, Malaysia. IEEE, 235-240.
- Agung, B. & Permana, F. P. Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression. International Conference on Communication, Networks and Satellite (ComNetSat), 2012 Bali, Indonesia. IEEE, 167-171.
- Al-Haj, A. 2015. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. *Journal of digital imaging*, 28 (2), 179-187.
- Al-Qershi, O. M. & Khoo, B. E. 2011a. Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *Journal of digital imaging*, 24 (1), 114-125.
- Al-Qershi, O. M. & Khoo, B. E. 2011b. High capacity data hiding schemes for medical images based on difference expansion. *Journal of Systems and Software*, 84 (1), 105-112.
- Alattar, A. M. Reversible watermark using difference expansion of triplets. International Conference on Image Processing (Cat. No.03CH37429), 2003 Barcelona, Spain. IEEE, 501-504.
- Alattar, A. M. Reversible watermark using difference expansion of quads. International Conference on Acoustics, Speech, and Signal Processing (ICASSP'04), 2004a Montreal, Que., Canada. IEEE, 377-380.
- Alattar, A. M. 2004b. Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing*, 13 (8), 1147-1156.
- Ali, A. H., George, L. E., Zaidan, A. & Mokhtar, M. R. 2018. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimedia Tools and Applications*, 77 (23), 31487-31516.
- Arsalan, M., Malik, S. A. & Khan, A. 2012. Intelligent reversible watermarking in integer wavelet domain for medical images. *Journal of Systems and Software*, 85 (4), 883-894.
- Arya, P., Tomar, D. S. & Dubey, D. 2015. A review on different digital watermarking techniques. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8 (10), 129-136.
- Atta-ur-Rahman, Sultan, K., Aldhafferi, N., Alqahtani, A. & Mahmud, M. 2018. Reversible and fragile watermarking for medical images. *Computational and mathematical methods in medicine*, 2018 1-7.
- Balasamy, K. & Ramakrishnan, S. 2018. An intelligent reversible watermarking system for authenticating medical images using Wavelet and PSO. *Cluster Computing*, 1-12.
- Bâth, M. 2010. Evaluating imaging systems: practical applications. *Radiation protection dosimetry*, 139 (1-3), 26-36.

- Brar, A. S. & Kaur, M. 2015. High capacity, reversible data hiding using cdcs along with medical image authentication. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8 (1), 49-60.
- Burgess, A. 1995. Image quality, the ideal observer, and human performance of radiologic decision tasks. *Academic radiology*, 2 (6), 522-526.
- Caldelli, R., Filippini, F. & Becarelli, R. 2010. Reversible watermarking techniques: an overview and a classification. *EURASIP Journal on Information Security*, 2010 2.
- Celik, M. U., Sharma, G., Tekalp, A. M. & Saber, E. 2005. Lossless generalized-LSB data embedding. *IEEE transactions on image processing*, 14 (2), 253-266.
- Chauhan, D. S., Singh, A. K., Kumar, B. & Saini, J. 2019. Quantization based multiple medical information watermarking for secure e-health. *Multimedia tools and applications*, 78 (4), 3911-3923.
- Chen, Y., Li, Z., Wang, L., Wang, N. & Hong, B. High-capacity Reversible Watermarking Algorithm Based on the Region of Interest of Medical Images. 14th IEEE International Conference on Signal Processing (ICSP), 2018. IEEE, 1158-1162.
- Cheung, Y. M. & Wu, H. T. 2007. A sequential quantization strategy for data embedding and integrity verification. *IEEE transactions on circuits and systems for video technology*, 17 (8), 1007-1016.
- Chiang, K. H., Chang-Chien, K. C., Chang, R. F. & Yen, H. Y. 2008. Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *Journal of Digital Imaging*, 21 (1), 77-90.
- Clark, K., Vendt, B., Smith, K., Freymann, J., Kirby, J., Koppel, P., Moore, S., Phillips, S., Maffitt, D., Pringle, M., Tarbox, L. & Prior, F. 2013. The Cancer Imaging Archive (TCIA): maintaining and operating a public information repository. *Journal of digital imaging*, 26 (6), 1045-1057.
- Coatrieux, G., Lecornu, L., Sankur, B. & Roux, C. A review of image watermarking applications in healthcare. International Conference of the IEEE Engineering in Medicine and Biology Society, 2006 New York, USA. IEEE, 4691-4694.
- Coatrieux, G., Maitre, H. & Sankur, B. Strict integrity control of biomedical images. Photonics West 2001-Electronic Imaging, 2001. International Society for Optics and Photonics, 229-240.
- Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y. & Collorec, R. Relevance of watermarking in medical imaging. Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on, 2000. IEEE, 250-255.
- Coatrieux, G., Montagner, J., Huang, H. & Roux, C. Mixed reversible and RONI watermarking for medical image reliability protection. 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007 Lyon, France. IEEE, 5653-5656.
- Cronbach, L. J. 1951. Coefficient alpha and the internal structure of tests. *psychometrika*, 16 (3), 297-334.
- Das, S. & Kundu, M. K. 2013. Effective management of medical information through ROI-lossless fragile image watermarking technique. *Computer methods and programs in biomedicine*, 111 (3), 662-675.

- De Vleeschouwer, C., Delaigle, J. & Macq, B. Circular interpretation of histogram for reversible watermarking. Fourth Workshop on Multimedia Signal Processing (Cat. No.01TH8564), 2001 Cannes, France. IEEE, 345-350.
- De Vleeschouwer, C., Delaigle, J. F. & Macq, B. 2003. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Multimedia*, 5 (1), 97-105.
- DICOM. 2006. *Digital Imaging and Communications in Medicine (DICOM) standard* [Online]. Available: <http://medical.nema.org/dicom/> [Accessed 30/11/2016].
- Dowling, J. A., Planitz, B. M., Maeder, A. J., Du, J., Pham, B., Boyd, C., Chen, S., Bradley, A. P. & Crozier, S. Visual quality assessment of watermarked medical images. Society of Photo-Optical Instrumentation Engineers (SPIE). 2007.
- Durvey, M. & Satyarthi, D. 2014. A review paper on digital watermarking. *International Journal of Emerging Trends & Technology in Computer Science*, 3 (4), 99-105.
- EC. 1996. *European guidelines on quality criteria for diagnostic radiographic images: UR 16260 EN*, Office for Official Publications of the European Communities. Brussels, Luxembourg.
- Eswaraiah, R. & Reddy, E. S. 2014a. Medical image watermarking technique for accurate tamper detection in ROI and exact recovery of ROI. *International journal of telemedicine and applications*, 2014 1-10.
- Eswaraiah, R. & Reddy, E. S. ROI-based fragile medical image watermarking technique for tamper detection and recovery using variance. Seventh International Conference on Contemporary Computing (IC3), 2014b. IEEE, 553-558.
- Feng, J. B., Lin, I. C., Tsai, C. S. & Chu, Y. P. 2006. Reversible watermarking: current status and key issues. *IJ Network Security*, 2 (3), 161-170.
- Fontani, M., De Rosa, A., Caldelli, R., Filippini, F., Piva, A., Consalvo, M. & Cappellini, V. Reversible watermarking for image integrity verification in hierarchical pacs. Proceedings of the 12th ACM workshop on Multimedia and security, 2010 Roma, Italy. ACM, 161-168.
- Fotopoulos, V., Stavrinou, M. L. & Skodras, A. N. Medical image authentication and self-correction through an adaptive reversible watermarking technique. 8th IEEE International Conference on BioInformatics and BioEngineering, 2008. Athens, Greece: IEEE, 1-5.
- Freedman, M. & Osicka, T. 2006. Reader variability: what we can learn from computer-aided detection experiments. *Journal of the American College of Radiology*, 3 (6), 446-455.
- Fung, C., Gortan, A. & Junior, W. G. A review study on image digital watermarking. The Tenth International Conference on Networks, 2011. 24-28.
- Gao, G., Wan, X., Yao, S., Cui, Z., Zhou, C. & Sun, X. 2017. Reversible data hiding with contrast enhancement and tamper localization for medical images. *Information Sciences*, 385 250-265.
- Giakoumaki, A., Perakis, K., Banitsas, K., Giokas, K., Tachakra, S. & Koutsouris, D. 2010. Using digital watermarking to enhance security in wireless medical image transmission. *Telemedicine and e-Health*, 16 (3), 306-313.

- Godinho, T. M., Silva, L. M. & Costa, C. An automation framework for PACS workflows optimization in shared environments. 10th Iberian Conference on Information Systems and Technologies (CISTI), 2015 Aveiro, Portugal. IEEE, 1-7.
- Guru, J. & Damecha, H. 2014. Digital watermarking classification: a survey. *International Journal of Computer Science Trends and Technology (IJCST) vol, 5* 8-13.
- Haouzia, A. & Noumeir, R. 2008. Methods for image authentication: a survey. *Multimedia tools and applications*, 39 (1), 1-46.
- Hasan, A. M. & Meziane, F. 2016. Automated screening of MRI brain scanning using grey level statistics. *Computers & Electrical Engineering*, 53 276-291.
- Hasan, A. M., Meziane, F., Aspin, R. & Jalab, H. A. 2016a. Segmentation of brain tumors in MRI images using three-dimensional active contour without edge. *Symmetry*, 8 (11), 132.
- Hasan, A. M., Meziane, F. & Kadhim, M. A. Automated segmentation of tumours in MRI brain scans. Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC), 2016b Rome, Italy. 55-62.
- He, W., Zhou, K., Cai, J., Wang, L. & Xiong, G. 2017. Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion. *Journal of Visual Communication and Image Representation*, 49 351-360.
- Herrmann, C., Sund, P., Tingberg, A., Keddache, S., Mansson, L. G., Almen, A. & Mattsson, S. Comparison of two methods for evaluating image quality of chest radiographs. Proc. SPIE 2000. 251-257.
- Ho, R. 2006. *Handbook of univariate and multivariate data analysis and interpretation with SPSS*, Boac Raton: Taylor & Francis Group.
- Hogg, P. & Blindell, P. Software for image quality evaluation using a forced choice comparison method. E-poster in UKRC, 2012 Manchester, UK.
- Honsinger, C. W., Jones, P. W., Rabbani, M. & Stoffel, J. C. 2001. Lossless recovery of an original image containing embedded data. U. S. Patent 6,278,791.
- Hore, A. & Ziou, D. Image quality metrics: PSNR vs. SSIM. 2010 20th International Conference on Pattern Recognition, 2010. IEEE, 2366-2369.
- Huang, H. 2011. *PACS and imaging informatics: basic principles and applications*, John Wiley & Sons.
- Hussain, A. J., Al-Fayadh, A. & Radi, N. 2018. Image compression techniques: A survey in lossless and lossy algorithms. *Neurocomputing*, 300 44-69.
- Ismail, M., Ning, Y. & Philbin, J. Separation of metadata and bulkdata to speed DICOM tag morphing. SPIE Medical Imaging 2014: PACS and Imaging Informatics: Next Generation and Innovations, 2014 San Diego, California, United States. International Society for Optics and Photonics, 903905-903905-6.
- Jabade, V. S. & Gengaje, D. S. R. 2011. Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications*, 31 (1), 28-35.
- Jain, P. & Rajawat, A. S. 2012. Fragile watermarking for image authentication: survey. *International Journal of Electronics and Computer Science Engineering*, 1 (3), 1232-1237.

- Kanso, A. & Ghebleh, M. 2015. An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, 24 (1-3), 98-116.
- Katz, J., Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. 2018. *Handbook of applied cryptography*, CRC press.
- Khan, A. & Malik, S. A. 2014. A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection. *Information Sciences*, 256 162-183.
- Khan, A., Siddiqa, A., Munib, S. & Malik, S. A. 2014. A recent survey of reversible watermarking techniques. *Information sciences*, 279 251-272.
- Ko, L. T., Chen, J. E., Shieh, Y. S., Hsin, H. C. & Sung, T. Y. 2012a. Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems. *Computational and mathematical methods in medicine*, 2012 1-8.
- Ko, L. T., Chen, J. E., Shieh, Y. S., Scalia, M. & Sung, T. Y. 2012b. A novel fractional-discrete-cosine-transform-based reversible watermarking for healthcare information management systems. *Mathematical Problems in Engineering*, 2012 1-7.
- Kobayashi, L. O. M., Furuie, S. S. & Barreto, P. S. L. M. 2009. Providing integrity and authenticity in DICOM images: a novel approach. *IEEE Transactions on Information Technology in Biomedicine*, 13 (4), 582-589.
- Krupinski, E. A. & Jiang, Y. 2008. Anniversary paper: evaluation of medical imaging systems. *Medical physics*, 35 (2), 645-659.
- Kumar, V. & Natarajan, V. 2016. Hybrid local prediction error-based difference expansion reversible watermarking for medical images. *Computers & Electrical Engineering*, 53 333-345.
- Kundel, H. L. 2006. History of research in medical image perception. *Journal of the American College of Radiology*, 3 (6), 402-408.
- Larobina, M. & Murino, L. 2014. Medical image file formats. *Journal of digital imaging*, 27 (2), 200-206.
- Ledenius, K., Svensson, E., Stålhammar, F., Wiklund, L. & Thilander-Klang, A. 2014. A method to analyse observer disagreement in visual grading studies: example of assessed image quality in paediatric cerebral multidetector CT images. *The British journal of radiology*.
- Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T. & Lei, H. 2014. Reversible watermarking scheme for medical image based on differential evolution. *Expert Syst. Appl.*, 41 (7), 3178-3188.
- Li, F., Mao, Q. & Chang, C.-C. 2018. Reversible data hiding scheme based on the Haar discrete wavelet transform and interleaving prediction method. *Multimedia Tools and Applications*, 77 (5), 5149-5168.
- Li, Y., Poulos, A., McLean, D. & Rickard, M. 2010. A review of methods of clinical image quality evaluation in mammography. *European journal of radiology*, 74 (3), e122-e131.

- Liew, S. C., Liew, S. W. & Zain, J. M. 2010. Reversible medical image watermarking for tamper detection and recovery with Run Length Encoding compression. *World Academy of Science, Engineering and Technology*, 72 799-803.
- Liew, S. C., Liew, S. W. & Zain, J. M. 2013. Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. *Journal of digital imaging*, 26 (2), 316-325.
- Liew, S. c. & Zain, J. M. 2010. Experiment of tamper detection and recovery watermarking in picture archiving and communication systems. *Journal of Computer Science*, 6 (7), 794.
- Liew, S. C. & Zain, J. M. 2011. Tamper localization and lossless recovery watermarking scheme. *Software Engineering and Computer Systems*. Springer.
- Likert, R. 1932. A technique for the measurement of attitudes. *Archives of psychology*, 140 1-55.
- Lin, C. C., Tai, W. L. & Chang, C. C. 2008. Multilevel reversible data hiding based on histogram modification of difference images. *Pattern Recognition*, 41 (12), 3582-3591.
- Liu, Y., Tang, S., Liu, R., Zhang, L. & Ma, Z. 2018. Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, 97 95-105.
- Loan, N. A., Hurrah, N. N., Parah, S. A., Lee, J. W., Sheikh, J. A. & Bhat, G. M. 2018. Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*, 6 19876-19897.
- Ludewig, E., Richter, A. & Frame, M. 2010. Diagnostic imaging—evaluating image quality using visual grading characteristic (VGC) analysis. *Veterinary research communications*, 34 (5), 473-479.
- Ma, B., Li, B., Wang, X.-Y., Wang, C.-P., Li, J. & Shi, Y.-Q. 2019. Code Division Multiplexing and Machine Learning Based Reversible Data Hiding Scheme for Medical Image. *Security and Communication Networks*, 2019.
- Maccia, C., Ariche-Cohen, M., Nadeau, X. & Severo, G. 1995. The 1991 CEC trial on quality criteria for diagnostic radiographic images. *Radiation protection dosimetry*, 57 (1-4), 111-117.
- Maeder, A., Dowling, J., Nguyen, A., Brunton, E. & Nguyen, P. Assuring authenticity of digital mammograms by image watermarking. International Workshop on Digital Mammography, 2008. Springer, 204-211.
- Maity, H. K. & Maity, S. P. 2012. Intelligent modified difference expansion for reversible watermarking. *The International Journal of Multimedia & Its Applications (IJMA)*, 4 (4), 83-95.
- Manning, D., Gale, A. & Krupinski, E. A. 2005. Perception research in medical imaging. *The British journal of radiology*, 78 (932), 683–685.
- Månsson, L. 2000. Methods for the evaluation of image quality: a review. *Radiation protection dosimetry*, 90(1-2) (1-2), 89-99.
- McCollough, C. H., Bruesewitz, M. R. & Kofler Jr, J. M. 2006. CT dose reduction and dose management tools: overview of available options 1. *Radiographics*, 26 (2), 503-512.

- McDowell, I. 2006. *Measuring health: a guide to rating scales and questionnaires*, Oxford university press.
- Memon, N. A., Chaudhry, A., Ahmad, M. & Keerio, Z. A. 2011. Hybrid watermarking of medical images for ROI authentication and recovery. *International Journal of Computer Mathematics*, 88 (10), 2057-2071.
- Menzel, H., Schibilla, H. & Teunen, D. 2000. European guidelines on quality criteria for computed tomography. *Luxembourg: European Commission publication*, EUR 16262 EN.
- Mohammadi, P., Ebrahimi-Moghadam, A. & Shirani, S. 2014. Subjective and objective quality assessment of image: A survey. *arXiv preprint arXiv:1406.7799*.
- Mostafa, S. A., El-Sheimy, N., Tolba, A., Abdelkader, F. & Elhindy, H. M. 2010. Wavelet packets-based blind watermarking for medical image management. *The open biomedical engineering journal*, 4 93.
- Mousavi, S. M., Naghsh, A. & Abu-Bakar, S. 2014. Watermarking techniques used in medical images: a survey. *Journal of digital imaging*, 27 (6), 714-729.
- Mraity, H., England, A. & Hogg, P. 2014. Developing and validating a psychometric scale for image quality assessment. *Radiography*, 20 (4), 306-311.
- Mustra, M., Delac, K. & Grgic, M. Overview of the DICOM standard. 50th International Symposium ELMAR, 2008 Zadar, Croatia. IEEE, 39-44.
- Nahrstedt, U., Wall, B., Maccia, C., Moores, B. & Padovani, R. 1990. CEC quality criteria for diagnostic radiographic images and patient exposure trial. Report (EUR 12952), Brussels, Luxembourg: Commission of the European Communities (CEC).
- Nambakhsh, M. S., Ahmadian, A. & Zaidi, H. 2011. A contextual based double watermarking of PET images by patient ID and ECG signal. *Computer methods and programs in biomedicine*, 104 (3), 418-425.
- Nasr, K. M. & Martini, M. G. 2017. A visual quality evaluation method for telemedicine applications. *Signal Processing: Image Communication*, 57 211-218.
- Navas, K. & Sasikumar, M. Survey of medical image watermarking algorithms. Proc. International Conf. Sciences of Electronics, Technologies of Information and Telecommunications, 2007 TUNISIA. 25-29.
- Nguyen, T.-S., Chang, C.-C. & Huynh, N.-T. 2015. A novel reversible data hiding scheme based on difference-histogram modification and optimal EMD algorithm. *Journal of Visual Communication and Image Representation*, 33 389-397.
- Ni, Z., Shi, Y. Q., Ansari, N. & Su, W. 2006. Reversible data hiding. *IEEE Transactions on circuits and systems for video technology*, 16 (3), 354-362.
- Norweck, J. T., Seibert, J. A., Andriole, K. P., Clunie, D. A., Curran, B. H., Flynn, M. J., Krupinski, E., Lieto, R. P., Peck, D. J. & Mian, T. A. 2013. ACR–AAPM–SIIM technical standard for electronic practice of medical imaging. *Journal of digital imaging*, 26 (1), 38-52.
- Nyeem, H., Boles, W. & Boyd, C. 2013. A review of medical image watermarking requirements for teleradiology. *Journal of digital imaging*, 26 (2), 326-343.
- Paar, C. & Pelzl, J. 2009. *Understanding cryptography: a textbook for students and practitioners*, Springer Science & Business Media.

- Pan, W., Bouslimi, D., Karasad, M., Cozic, M. & Coatrieux, G. 2018. Imperceptible reversible watermarking of radiographic images based on quantum noise masking. *Computer methods and programs in biomedicine*, 160 119-128.
- Pan, W., Coatrieux, G., Montagner, J., Cuppens, N., Cuppens, F. & Roux, C. Comparison of some reversible watermarking methods in application to medical images. Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2009 Minneapolis, MN, USA. IEEE, 2172-2175.
- Parah, S. A., Ahad, F., Sheikh, J. A. & Bhat, G. 2017. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *Journal of Biomedical Informatics*, 66 214-230.
- Patel, R. & Bhatt, P. 2015. A review paper on digital watermarking and its techniques. *International Journal of Computer Applications*, 110 (1), 10-13.
- Pelli, D. G. & Farell, B. 1995. Psychophysical methods. *Handbook of Optics: Fundamentals, techniques, and design*. Second ed. New York: McGraw-Hill.
- Petrou, M. 2010. Texture in biomedical images. *Biomedical Image Processing*. Springer.
- Pianykh, O. S. 2009. *Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide*, 2nd ed. Springer. Berlin, Germany.
- Polit, D. F. & Beck, C. T. 2004. *Nursing research: Principles and methods (7 ed.)*, Lippincott Williams & Wilkins.
- Priya, R. & Sadasivam, V. 2014. A survey on watermarking techniques, requirements, applications for medical images. *Journal of Theoretical and Applied Information Technology*, 65 (1), 103-120.
- Pushpala, K. & Nigudkar, R. A novel watermarking technique for medical image authentication. Computers in Cardiology, 2005 Lyon, France. IEEE, 683-686.
- Qasim, A. F., Aspin, R. & Meziane, F. 2019a. Integration of Digital Watermarking Technique into Medical Imaging Systems. *10th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2019*. Leeds, United Kingdom.
- Qasim, A. F., Aspin, R., Meziane, F. & Hogg, P. 2019b. Assessment of perceptual distortion boundary through applying reversible watermarking to brain MR images. *Signal Processing: Image Communication*, 70 (C), 246-258.
- Qasim, A. F., Aspin, R., Meziane, F. & Hogg, P. 2019c. ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. *Multimedia Tools and Applications*, 78 (12), 16433-16463.
- Qasim, A. F., Meziane, F. & Aspin, R. 2018a. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27 45-60.
- Qasim, A. F., Meziane, F. & Aspin, R. A reversible and imperceptible watermarking scheme for MR images authentication. Proceedings of the 24th International Conference on Automation and Computing (ICAC'2018), 2018b Newcastle upon Tyne, UK. IEEE.
- Qin, C., He, Z., Yao, H., Cao, F. & Gao, L. 2018. Visible watermark removal scheme based on reversible data hiding and image inpainting. *Signal Processing: Image Communication*, 60 160-172.

- Rathi, S. C. 2012. Medical image authentication through watermarking preserving ROI. *Health Informatics - An International Journal (HIJ)*, 1 (1).
- Richardson, M. L., Frank, M. S. & Stern, E. J. 1995. Digital image manipulation: what constitutes acceptable alteration of a radiologic image? *AJR. American journal of roentgenology*, 164 (1), 228-229.
- Ridzoň, R., Levický, D. & Klenovičová, Z. Attacks on watermarks and adjusting PSNR for watermarks application. *Radioelektronika 2004: 14th international Czech-Slovak scientific conference*, 2004. 27-28.
- Roček, A., Slavíček, K., Dostál, O. & Javorník, M. 2016. A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomedical Signal Processing and Control*, 29 44-52.
- Rubin, D. B. 1996. Multiple imputation after 18+ years. *Journal of the American statistical Association*, 91 (434), 473-489.
- Saberian, M. J., Akhaee, M. A. & Marvasti, F. An invertible quantization based watermarking approach. *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008 Las Vegas, NV, USA. IEEE, 1677-1680.
- Sandborg, M., McVey, G., Dance, D. & Carlsson, G. A. 2000. Comparison of model predictions of image quality with results of clinical trials in chest and lumbar spine screen-film imaging. *Radiation protection dosimetry*, 90 (1-2), 173-176.
- Sandborg, M., Tingberg, A., Dance, D., Lanhede, B., Almén, A., McVey, G., Sund, P., Kheddache, S., Besjakov, J. & Mattsson, S. 2001. Demonstration of correlations between clinical and physical image quality measures in chest and lumbar spine screen-film radiography. *The British journal of radiology*, 74 (882), 520-528.
- Seeram, E., Davidson, R., Bushong, S. & Swan, H. 2014. Image quality assessment tools for radiation dose optimization in digital radiography: An overview. *Radiologic technology*, 85 (5), 555-562.
- Selvam, P., Balachandran, S., Iyer, S. P. & Jayabal, R. 2017. Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. *Optik-International Journal for Light and Electron Optics*, 145 655-671.
- Shet, N., Chen, J. & Siegel, E. L. 2011. Continuing challenges in defining image quality. *Pediatric radiology*, 41 (5), 582-587.
- Shih, F. Y. & Wu, Y. T. 2005. Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, 175 (3), 200-216.
- Smedby, Ö. & Fredrikson, M. 2010. Visual grading regression: analysing data from visual grading experiments with regression models. *The British journal of radiology*, 83 767-775.
- Soille, P. 2013. *Morphological image analysis: principles and applications*, 2nd ed. Springer. Berlin, Germany.
- Stanescu, L., Burdescu, D. D. & Stoica-Spahiu, C. Application for complex querying of the databases obtained by extracting data from DICOM files. *2nd International Conference on Information & Communication Technologies*, 2006 Damascus, Syria. IEEE, 1008-1013.
- Stocksley, M. & Phillips, R. 2005. *Medical imaging-techniques, reflections and evaluation*. Elsevier.

- Streiner, D., Norman, G. & Cairney, J. 2015. *Health measurement scales: a practical guide to their development and use*, USA, Oxford University Press.
- Sund, P., Båth, M., Kheddache, S. & Månsson, L. G. 2004. Comparison of visual grading analysis and determination of detective quantum efficiency for evaluating system performance in digital chest radiography. *European radiology*, 14 (1), 48-58.
- Tabachnick, B. G. & Fidell, L. S. 2013. *Using multivariate statistics (5 ed.)*, Boston, Pearson Education.
- Tan, C. K., Ng, J. C., Xu, X., Poh, C. L., Guan, Y. L. & Sheah, K. 2011. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *Journal of Digital Imaging*, 24 (3), 528-540.
- Tareef, A., Al-Ani, A., Nguyen, H. & Chung, Y. Y. A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding. 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2014 Chicago, IL, USA. IEEE, 5554-5557.
- Thilagavathi, N., Saravanan, D., Kumarakrishnan, S., Punniakodi, S., Amudhavel, J. & Prabu, U. A survey of reversible watermarking techniques, application and attacks. Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), 2015. ACM, 37.
- Thodi, D. M. & Rodriguez, J. J. Prediction-error based reversible watermarking. International Conference on Image Processing, 2004. ICIP '04, 2004 Singapore. IEEE, 1549-1552.
- Thodi, D. M. & Rodríguez, J. J. 2007. Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing*, 16 (3), 721-730.
- Tian, J. 2003. Reversible data embedding using a difference expansion. *IEEE transactions on circuits and systems for video technology*, 13 (8), 890-896.
- Tingberg, A., Herrmann, C., Lanhede, B., Alm, A., Besjakov, J., Mattsson, S., Sund, P., Kheddache, S. & Månsson, L. 2000. Comparison of two methods for evaluation of the image quality of lumbar spine radiographs. *Radiation protection dosimetry*, 90 (1-2), 165-168.
- Toennies, K. D. 2012. *Guide to medical image analysis: methods and algorithms*, Springer Science & Business Media.
- Tsai, P., Hu, Y. C. & Yeh, H. L. 2009. Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing*, 89 (6), 1129-1143.
- Uthayakumar, J., Vengattaraman, T. & Dhavachelvan, P. 2018. A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. *Journal of King Saud University-Computer and Information Sciences*.
- Varma, D. R. 2012. Managing DICOM images: Tips and tricks for the radiologist. *The Indian journal of radiology & imaging*, 22 (1), 4.
- Voloshynovskiy, S., Koval, O., Beekhof, F. & Pun, T. Conception and limits of robust perceptual hashing: towards side information assisted hash functions. IS&T/SPIE Electronic Imaging, 2009. International Society for Optics and Photonics, 72540D-72540D-12.

- Voloshynovskiy, S., Pereira, S., Iquise, V. & Pun, T. 2001. Attack modelling: towards a second generation watermarking benchmark. *Signal processing*, 81 (6), 1177-1214.
- Wang, Z., Bovik, A. C. & Lu, L. Why is image quality assessment so difficult? International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2002 Orlando, FL. IEEE, 3313-3316.
- Xuan, G., Yang, C., Zhen, Y., Shi, Y. Q. & Ni, Z. Reversible data hiding based on wavelet spread spectrum. 6th Workshop on Multimedia Signal Processing, 2004a Siena, Italy. IEEE, 211-214.
- Xuan, G., Yang, C., Zhen, Y., Shi, Y. Q. & Ni, Z. Reversible data hiding using integer wavelet transform and companding technique. International Workshop on Digital Watermarking, 2004b. Springer, 115-124.
- Yang, Y., Zhang, W., Liang, D. & Yu, N. 2018. A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. *Multimedia Tools and Applications*, 77 (14), 18043-18065.
- Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W. & Khamayseh, Y. Comprehensive study of symmetric key and asymmetric key encryption algorithms. 2017 international conference on engineering and technology (ICET), 2017. IEEE, 1-7.
- Zain, J. M. & Fauzi, A. R. Medical image watermarking with tamper detection and recovery. International Conference of the IEEE Engineering in Medicine and Biology Society, 2006 New York, NY, USA. IEEE, 3270-3273.
- Zain, J. M., Fauzi, A. R. & Aziz, A. A. 2009. Clinical assessment of watermarked medical images. *Journal of Computer Science*, 5 (11), 857-863.
- Zarb, F., Rainford, L. & McEntee, M. F. 2010. Image quality assessment tools for optimization of CT images. *Radiography*, 16 (2), 147-153.
- Zear, A., Singh, A. K. & Kumar, P. 2018. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimedia Tools and Applications*, 77 (4), 4863-4882.