# Enhancing Image Security via Block Cyclic Construction and DNA based LFSR

Subhrajyoti Deb, Abhilash Das, Bhaskar Biswas , Joy Lal Sarkar, Surbhi Bhatia Khan, Saeed Alzahrani, Shalli Rani

***Abstract*—The rapidly growing multimedia image data driven by real-time messaging technologies is particularly evident in applications such as autonomous vehicle tracking, smart cities, surveillance systems and many more. Considering images, data privacy and security are of paramount importance. Yet, many existing methods need to pay more attention to the specific challenges posed by chaotic maps, such as limited parameter coverage and insufficient chaotic behaviour. We present a novel method for image encryption that combines a cyclic block function during the confusion phase and a DNA-based Linear Feedback Shift Register (LFSR) in the diffusion phase to render the final cipher image. This process involves diagonal cyclic shifting and swapping of pixel blocks to minimize pixel correlation. DNA cryptography-based LFSR is particularly efficacious in high-quality pseudorandom number generation due to its robust statistical effects. Besides that, DNA-based operations improve the encryption speed, making the process more efficient. The proposed cryptosystem is validated through several methods, including histogram analysis, correlation assessment, entropy measurement, key sensitivity evaluation, and $\chi^2$ testing. Our algorithm offers superior security and efficiency, outperforming established schemes in terms of security and robustness.**

***Index Terms*—Image encryption, Block Cyclic Construction, Confusion, DNA, LFSR, Encryption, Decryption.**

## I. Introduction

The Internet and cloud technology are growing fast, making multimedia data a must in our everyday lives. Notably, images have become crucial for keeping records, sharing stuff, and talking to each other. Their usage is a lot in vehicular technology, military, social media, and healthcare, which shows their importance. Keeping this image data safe is a top priority; for instance, image security is necessary for autonomous vehicles (AVs) to protect visual data from unauthorized access, assuring precise and reliable object detection and decision-making. Comprehensive cryptanalysis evaluations have demonstrated that permutation-based encryption schemes for images and videos may be faulty to furnish sufficient security from a cryptographic perspective, as emphasised by prior research [1]–[3]. Some critical security points possess the partial recovery of plain images under ciphertext-only attacks [4], the incapability to diminish the substantial information redundancy intrinsic in plain images, and the entire insecurity of secret permutations against known or chosen plaintext attacks, entail more robust image encryption methods [5]. For instance, Zhu et al. [6] successfully broke the RT-enhanced chaotic tent map using a CPA. At the same time, KPA has been utilised to investigate various chaotic system-based image encryption techniques [7], [8]. In our proposed Block Cyclic Construction, $\zeta(P)$ uses its low computational complexity of $n \log_2 n$ for confusion. Also, the inverse confusion $\zeta^{-1}(P)$ can be executed with an order of 2, which can prevent CPA. By stacking $m$ multiple images to form a large image matrix and then applying Block Cyclic Construction, the permutation of these stacked images can result in $m!$ possible orderings, making it significantly challenging for an attacker to query all potential arrangements.

Among various cryptographic methods, DNA-based cryptography is recognized for its strong security features and has become a prominent research area with promising results. Simultaneously, continuous efforts seek to refine image encryption algorithms employing DNA-based techniques [9]–[12]. Also, classic cryptosystems convert plaintext into ciphertext using binary values. In recognition, DNA-based encryption utilises a distinct approach by applying DNA codes i.e. nucleotide bases namely A, T, C, and G rather than binary digits. The complicated structure of DNA's cryptosystem has accumulated substantial interest to field experts, especially for protecting images from various attacks in real-time applications [13], [14]. Sony et al. proposed a cryptosystem consisting of a DNA cryptographic algorithm based on Moore machine principles, comprising three stages of encryption: a secret key, an auto-generated Moore machine, and a password integration [15]. Their approach begins by encrypting the message with a dynamically generated secret key. They implemented a codebook lookup table to generate DNA sequence after XORing partitioned 256-bit encrypted block. Various schemes [16]–[18] have integrated chaotic systems with DNA encoding theory to enhance system complexity. Nevertheless, challenges still required to be handled in enhancing security due to the limited dimensions of chaotic systems and constrained key space. Recently, researchers [19]–[23] have presented several new image encryption schemes that incorporate chaotic mapping with DNA encoding, leading to enhanced encryption

Subhrajyoti Deb, Department of CSE, ICFAI University Tripura, India. Email: subhrajyotideb1@gmail.com Corresponding author

Abhilash Das, Department of CSE, Indian Institute of Technology Jammu, Jammu, India. Email: dasgate77@gmail.com

Bhaskar Biswas, Department of CSE, ICFAI University Tripura, India. Email: bhaskar.cse11@gmail.com

Joy Lal Sarkar, Department of CSE, ICFAI University Tripura, India. Email: joylalsarkar@gmail.com

Surbhi Bhatia Khan School of science, engineering and environment, University of Salford, United Kingdom
University Centre for Research and Development, Chandigarh University, Mohali, Punjab. Email: s.khan138@salford.ac.uk

Saeed Alzahrani is the Assistant Professor in the Management Information System Department, College of Business Administration, King Saud University, Saudi Arabia Email: salhariri@KSU.EDU.SA

Shalli Rani Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. Email: Shalli.rani@chitkara.edu.in

Manuscript received 2024

efficiency and strengthened security, thereby drawing substantial interest and attention from researchers across multiple disciplines.

A robust security scheme is essential to protect confidential image data from differential attacks. Recent research works [24]–[26] have investigated various DNA-based cryptographic schemes for secure image data transmission. Nevertheless, most of these methods extend security concerns and suffer from high computational complexity, resulting in elongated encryption and decryption times. As multimedia systems are increasingly used, there is a demand for adequate, robust, and highly secure systems to handle large data volumes. To meet these demands, cryptosystems utilizing LFSR during the diffusion phase may show promising potential [27]–[29]. As this cryptosystem can generate good pseudorandom binary sequences with robust cryptographic properties through a DNA operation-based feedback shift register, which is well-suited for high-throughput image encryption.

In consideration of the preceding discussion, this article provides some significant contributions, outlined as follows:

- A novel technique applying Block Cyclic Construction is employed to address the challenges identified in bitwise confusion. This technique provides highly uniform distribution of bits within the confused pixel, characterized by a non-repetitive pattern. The pixel values undergo a sequence of even distribution of pixels with a swap strategy of same-sized diagonal blocks of pixels where each same-sized block contains an equal number of pixels. Pixel distribution at highest and lowest possible block size is exactly the same. Thus, the highest uneven distribution point is achieved at a medium block size.
- This work presents a novel encryption technique to improve pixel diffusion using an 8-bit keystream generator based on DNA coding based LFSR sequences. Applied to a permuted image, the method enhances image encryption by furnishing better diffusion and security.
- Employing different rule-based DNA processes for the XOR operation, this method can generate encrypted images with high randomization levels while maintaining a high data throughput. The efficiency of its speed is also cited as the effectiveness of its structure.
- The experimental findings reveal that the designed scheme excels state-of-the-art and is resilient against known cryptographic attacks.

The remaining framework of the manuscript is compiled as follows. Section II consists of the preliminaries, and Section III details the suggested cryptosystem. Section IV comprises the experimental outcome and comparison with some existing algorithms with closing discussion drawn in Section V.

## II. Preliminaries

Few preliminaries including DNA cryptography and LFSR are discussed below.

### A. DNA cryptography

In 1994, Adleman introduced DNA cryptography [30], initially focusing on availing DNA molecules' physical and chemical features to design encryption algorithms. Given DNA's robust information storage ability and intricate biological components, it is identified as a favourable cryptographic tool, prompting researchers to study it as a novel encryption method in cryptography as DNA technology advances.

Table I
DNA ENCODING RULES.

| Rule | A | C | G | T |
|---|---|---|---|---|
| **1** | 00 | 01 | 10 | 11 |
| **2** | 00 | 10 | 01 | 11 |
| **3** | 11 | 01 | 10 | 00 |
| **4** | 11 | 10 | 01 | 00 |
| **5** | 01 | 00 | 11 | 10 |
| **6** | 01 | 11 | 00 | 10 |
| **7** | 10 | 00 | 11 | 01 |
| **8** | 10 | 11 | 00 | 01 |

The four nucleobases in DNA can be placed in 24 different forms according to permutation and combination principles. However, in DNA calculation, adherence to the rule of complementarity is essential, with A complementing T and C complementing G, showing the structure of eight encoding and decoding rules summarised in Tables I, and II; also, DNA computation involves operations i.e. Addition (+), Subtraction (-), XOR ($\bigoplus$), Add complement ( ), Sub-complement, AND ($\wedge$), OR ($\vee$), and XNOR among them we have used XOR, AND, and OR operations shown in Table III.

Table II
DNA DECODING RULES.

| Rule | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| **1** | A | C | G | T |
| **2** | A | G | C | T |
| **3** | T | C | G | A |
| **4** | T | G | C | A |
| **5** | C | A | T | G |
| **6** | G | A | T | C |
| **7** | C | T | A | G |
| **8** | C | A | T | G |

Table III
DNA OPERATIONS.

| $\bigoplus$ | **A** | **C** | **G** | **T** | $\wedge$ | **A** | **C** | **G** | **T** | $\vee$ | **A** | **C** | **G** | **T** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | A | C | G | T | | A | A | A | A | | A | C | G | T |
| **C** | C | A | T | G | | A | C | A | C | | C | C | T | T |
| **G** | G | T | A | C | | A | A | G | G | | G | T | G | T |
| **T** | T | G | C | A | | A | C | G | T | | T | T | T | T |

In the case of encoding and decoding of the same data with different rules, it may result in different outcomes. For example, we assume that a decimal number 142 is to be encoded in a DNA sequence. Now we convert 142 in binary `10001110` and encode according to rule 3 to get the DNA sequence 'GTAG'. At the time of decoding, if we use rule 7, `11011011` will be decoded sequence, which is equivalent to 219. According to rule 2, the decoded sequence will be `01110001`, resulting in 113 [31].

### B. Linear Feedback Shift Register (LFSR)

LFSR is a mathematical construct frequently used in cryptography. It is a binary sequence generator composed of a shift register and a feedback function. The register holds a certain number of bits; at each step, all bits are shifted by one position. The feedback function uses specific bits from the register to choose a new bit that's fed back into the first position, affecting the whole sequence—this interplay between shifting and feedback results in a long, periodic series with desirable cryptographic effects [32]. Mathematically, let $k > 0$, a sequence $t_0, t_1, \cdots$ of elements of $\mathbb{F}_q$ satisfying the relation $t_{n+k} = \alpha_{k-1}s_{n+k-1} + \cdots + \alpha_1 t_{n+1} + \alpha_0 t_n + \alpha$, where $\alpha, \alpha_0, \alpha_1, \cdots, \alpha_{k-1} \in \mathbb{F}_q$ The above recurrence relation represents the $t_i$ denotes the $i$th bit and $\alpha_0$ through $\alpha_{k-1}$ are the LFSR coefficients. If $\alpha = 0$, then the relation is homogeneous otherwise inhomogeneous.

## III. Proposed Cryptosystem

### A. Block Cyclic Construction for confusion

We describe the potential of block cyclic construction lucidly. The usefulness of this construction is seen when a plaintext image of higher width and height having equal value is given to the scrambling unit, we call it the block cyclic construction. The scrambling unit scrambles the pixel values among each other. The block cyclic construction transforms the image as shown in Fig. 1. The various levels of scrambling are determined by $\lambda = 2^u$ where $0 \leq u < \log_2(N)$ for a $N \times N$ image matrix. In the consecutive paragraph, we describe the working of the Algorithm 1 and all its aspects. Later, we provide a theoretical bound of the scrambling level for a $N \times N$ image matrix.

We name our scrambling algorithm Recursive `block SWAP` since it recursively swaps diagonal quadrants. Then for each smaller quadrant, it applies the same recursive routine breaking the image matrix into $\log_2(N)$ levels. The quadrants are broken into square matrices which are easy to handle recursively. All the scrambling levels shown in Fig. 1 for the image `boat.jpg` are applied independently for $\lambda = 2^0, \cdots, 2^9$. But we give a note here that the block cyclic construction can be applied in composition. For a block cyclic construction $\zeta^{[\sigma]}$, we represent a composition for $N \times N$ image $P$ as

$$\zeta^{[\sigma_1]} \circ \zeta^{[\sigma_2]}(P) = \zeta^{[\sigma_1 \circ \sigma_2]}(P) \tag{1}$$

For instance, we show the composition of block cyclic construction using `APC.tiff` with $\lambda = 2^2, 2^4, 2^6, 2^7$ in Fig. 2. Now we state one obvious result on the order of composition of the same $\lambda$.

**Lemma.** The block cyclic construction in Algorithm 1 defined by the transformation

$$\zeta^{[\sigma_1]} \circ \zeta^{[\sigma_2]}(P) = P \tag{2}$$

if and only if $\sigma_1 = \sigma_2$.

*Proof.* Consider the input image $P[N][N]$ of $N \times N$ order. According to the Algorithm 1, the $P$ is continuously split into four quadrants until $\sigma_i^2$ with $i \in \{1, 2\}$ pixels are left in each quadrant, giving it the *base* condition. The base condition lies at the bottom at $level$ zero of the recursion tree formed during splits. Then the two pixels at the base are `SWAPPED` for all the pairs. The recurrence relation for the base case and the recursive case is defined by

$$\zeta(P[N][N]) = \begin{cases} \zeta(P[N/2][N/2]) & \text{if } (N/2) > \sigma_i \\ \texttt{SWAP} \text{ the diagonal block} & \text{otherwise} \end{cases}$$

where $N$ can be expressed in powers of 2. The `SWAP` operation is of order 2. Since, every $\lambda$ is inverse of itself i.e. $\lambda$ with order 2, the Eq. 2 follows when $\sigma_1 = \sigma_2 = \lambda = 2^u$ with $1 \leq u \leq \log_2(N)$. □

The corollary below follows the result of the above lemma.

**Corollary.** The composition of block cyclic construction with $\sigma_1$ and $\sigma_2$ is commutative.

$$\zeta^{[\sigma_1]} \circ \zeta^{[\sigma_2]}(P) = \zeta^{[\sigma_2]} \circ \zeta^{[\sigma_1]}(P) \tag{3}$$

**Theorem.** The number of scrambling levels $\Sigma = \{2^0, \cdots, 2^{\log_2 N}\}$ using block cyclic construction cannot exceed $\log_2 N + 1$.

*Proof.* Suppose the block cyclic construction on the plaintext is given by

$$\zeta^{[\sigma_1 \circ \cdots \sigma_i \circ \sigma_j \circ \cdots \sigma_{\log_2 N}]} \tag{4}$$

with $|\Sigma| = \log_2 N + 1$. For if $\sigma_i = \sigma_j$ with $i \neq j$ and $i < j$, then from Lemma III-A it is obvious that

$$\zeta^{[\sigma_1 \circ \cdots \sigma_{i-1} \circ \sigma_{j-1} \circ \cdots \sigma_{\log_2 N}]} \subset \zeta^{[\sigma_1 \circ \cdots \circ \sigma_i \circ \sigma_j \circ \cdots \sigma_{\log_2 N}]} \tag{5}$$

with $|\Sigma| < \log_2 N - 1$. Thus, if any $\sigma_i$ is composed in multiples of two then the scrambling level $\Sigma$ gets used by two levels. □

Block Cyclic Construction can tackle the issues associated with bitwise confusion. This method ensures a remarkably uniform distribution of bits within the perplexed pixel, showcasing a non-repetitive pattern. The pixel values undergo a series of evenly distributed pixels through a swapping strategy involving same-sized diagonal blocks. Each block consists of an equal number of pixels, resulting in identical pixel distribution at both the highest and lowest possible block sizes. Consequently, the highest point of uneven distribution is attained at a medium block size.

**Time complexity.** The time complexity analysis of the recursive `block` function algorithm involves examining both the base and recursive cases. In the base case, when $b_1 - a_1 = \sigma$ and $b_2 - a_2 = \sigma$, the algorithm executes nested loops where the outer loop iterates $\sigma/2$ times and the inner loop iterates $\sigma$ times, resulting in $\sigma^2/2$ iterations. Each iteration performs a constant-time operation, leading to a base case time complexity of $O(\sigma^2)$. In the recursive case, the algorithm divides the current image segment into four quadrants and calls the `block` function on each quadrant. The recurrence relation for the time complexity $T(n)$, where $n$ is the side length of the image, is expressed as $T(n) = 4T\left(\frac{n}{2}\right) + O(\sigma^2)$. Solving this using the Master Theorem, where $a = 4$, $b = 2$, and $f(n) = O(\sigma^2)$, and noting that $\log_b a = \log_2 4 = 2$, we find that $f(n) = O(1)$ (a constant) is less than $n^2$. Therefore, according to the Master Theorem, $T(n) = O(n^2)$.

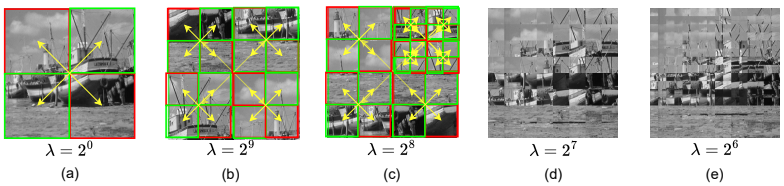



Figure 1. The transitions of the pixels by the Block Cyclic Construction for each $\lambda = 2^0, 2^1, \cdots, 2^9$.

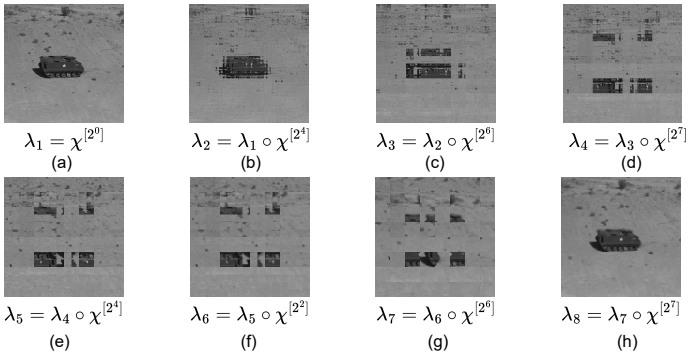



Figure 2. The composition of block cyclic construction using `APC.tiff`.

**Algorithm 1** Recursive `block` function is denoted by $\zeta$. Given input image $t$ with left corner pixel position $(a_1, a_2)$ and bottom right pixel position $(b_1, b_2)$, the algorithm outputs a scrambled image having $\sigma$ scrambling factor.

**Require:** $t$, $(a_1, a_2)$, $(b_1, b_2)$, $\sigma$
**if** $b_1 - a_1 = \sigma$ **and** $b_2 - a_2 = \sigma$ **then**
  **for** $i = a_1$ **to** $(a_1 + b_1)/2$ **do**
    **for** $j = a_2$ **to** $b_2$ **do**
      **if** $a_2 \leq j < (a_2 + b_2)/2$ **then**
        `SWAP` $t[i, j]$ **and** $t[i + \sigma/2, j + \sigma/2]$
      **else**
        `SWAP` $t[i, j]$ **and** $t[i + \sigma/2, j - \sigma/2]$
      **end if**
    **end for**
  **end for**
**else**
  $t \leftarrow \texttt{block}(t, a_1, a_2, (a_1 + b_1)/2, (a_2 + b_2)/2)$ ▷ quadrant 1
  $t \leftarrow \texttt{block}(t, a_1, (a_2 + b_2)/2, (a_1 + b_1)/2, b_2)$ ▷ quadrant 2
  $t \leftarrow \texttt{block}(t, (a_1 + b_1)/2, a_2, b_1, (a_2 + b_2)/2)$ ▷ quadrant 3
  $t \leftarrow \texttt{block}(t, (a_1 + b_1)/2, (a_2 + b_2)/2, b_1, b_2)$ ▷ quadrant 4
**end if**
**return** $t$

Consequently, the overall time complexity of the `block` function algorithm is $O(n^2)$.

### *B. Key stream generation through DNA-LFSR*

The proposed cryptosystem uses a key stream generated by employing an LFSR in conjunction with DNA-encoded streams for each LFSR block, including multiple randomizing operations for improved security.

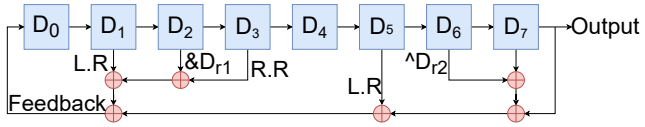



Figure 3. Block diagram of DNA LFSR.

In Fig. 3, we have shown the architecture of the proposed DNA-LFSR, where labelled blocks $D_{0,2,3,\ldots,7}$ denoting different segments of the DNA-LFSR and various operations involved in the feedback generation process. Also, the DNA sequence generation method uses an LFSR-based structure, where each block acquires a unique DNA sequence as input. This DNA LFSR performs as the core component because it can generate pseudo-random sequences with low computational overhead. Our proposed structure includes multiple internal operations designed to improve the randomness of the generated DNA stream, and LFSR consists of eight DNA blocks, each containing a four-character DNA stream (e.g., 'ATGC'). Through this technique, LFSR produces a four-character output DNA sequence in a single cycle. Here, critical operations within this LFSR structure possess a left rotation in $D_1$, a proper rotation in $D_3$, and an AND operation between a random DNA sequence $D_{r1}$ and $D_2$. Besides, a randomly generated DNA sequence $D_{r2}$ undergoes an OR operation with $D_6$, and the consequent sequence is XOR with $D_7$ during the feedback generation process. Results of these operations are XOR and fed back into the loop, providing robust feedback

generation. In diffusion, the proposed integrated combination of LFSR operations and DNA sequences effectively generates a pseudo-random DNA stream that is well-suited for high throughput.

### C. DNA-LFSR based diffusion

The diffusion process is the core part of any cryptosystem. The image produced through the suggested confusion process loses its visual information but retains the statistical data, making it susceptible to potential attacks. The diffusion process eliminates all statistical connections between the input and output, ensuring no similarities exist between input and output. The proposed diffusion step begins by splitting the scrambled image $I_S$ into its constituent `channels` via `split` function. Each channel is then transformed into bit-planes, followed by DNA encoding using random encoding rules. Next, each DNA-encoded bit plane is XOR with a key sequence obtained from the logistic-sine chaotic map (LSCM) [33]. DNA decoding is performed on the XOR components using random rules to get the corresponding enciphered image components. Finally, all the ciphered components are combined to create a cipher image $I_C$. Random rules for DNA encoding, decoding, and the XOR process are derived from the Eq. 6 [33]. The diffusion process is detailed in Algorithm 2 and illustrated in Fig. 4.

$$x_{i+1} = \left( r x_i (1 - x_i) + \frac{(4 - r)\sin(\pi x_i)}{4} \right) \mod 8 \quad (6)$$

**Algorithm 2** Diffusion using DNA-LFSR

**Input:** Scrambled Image $I_S$, DNA encoded Key $k$, and rules from LSCM.
**Output:** Cipher Image $I_C$ of size $m \times n$.
Read the Scrambled Image $I_S$ of size $m \times n$ with `channels` $ch = \{1, 2, 3\}$ i.e. R, G, B.
$ch \leftarrow$ `split`$(I_S)$
**for** $i = 1$ to $m$ **do**
  **for** $j = 1$ to $n$ **do**
    **for** $k = 1$ to $ch$ **do**
      $A(ch(k)[i,j] \leftarrow \text{DNA}_{enc}(I_S(ch(k)[i,j], \text{rule})$.
      /*`DNA encoding`*/
      $B(ch(k)[i,j] \leftarrow \text{XOR}(A(ch(k)[i,j], k, \text{rule})$.
      /*`DNA XOR`*/
      $C(ch(k)[i,j] \leftarrow \text{DNA}_{dec}(B(ch(k)[i,j], \text{rule})$.
      /*`DNA decoding`*/
    **end for**
  **end for**
**end for**
$I_C \leftarrow \bigcup_{k=1}^{3} C(k)[i,j]$.
**return** $I_C$.

## IV. Results and Discussion

This section presents the execution procedure of the suggested encryption algorithm, including results and discussion. The experimental work was done on a Windows 11 platform with a system configuration of Intel(R) Core(TM) i7-10700 CPU and 32GB RAM using MATLAB2023 and Python language. Various test images for experimental work were taken from the standard USC-SIPI image dataset [34].

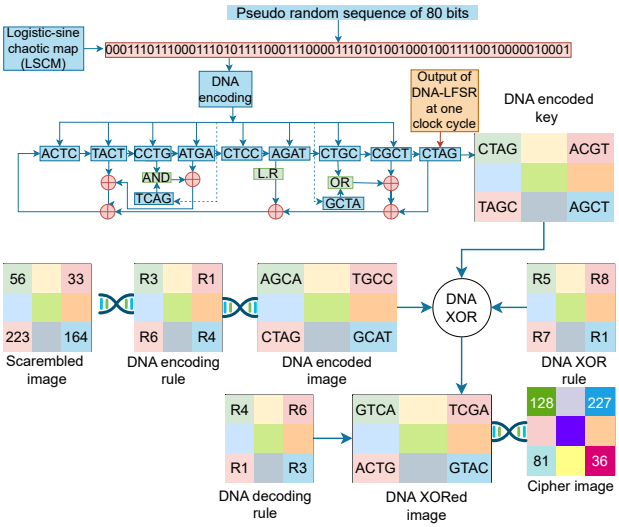



Figure 4. Illustration of the DNA-LFSR based diffusion process.

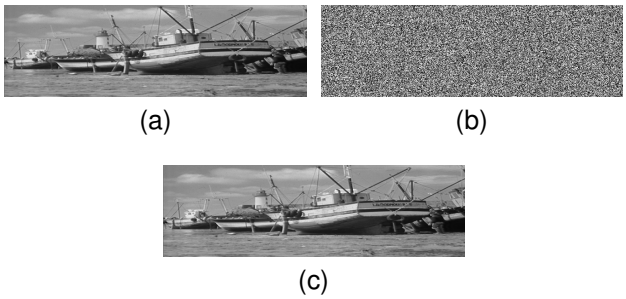



Figure 5. (a) Original image, (b) Encrypted image, and (c) Decrypted image of dimension ($450 \times 200$).

In Figs. 5, and 6 we have shown the visual results of encryption process. Fig. 5 shows a grayscale plain image (`boat.tif`) of dimension $450 \times 200$ and its corresponding encryption and decryption results. In Fig. 6, the visual result of the proposed encryption process applied on RGB image (`house.tiff`) of dimension ($400 \times 150$) are shown.

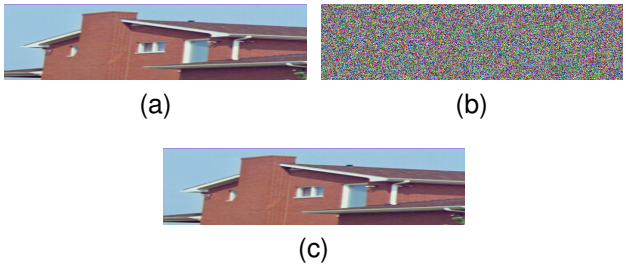



Figure 6. (a) Original image, (b) Encrypted image, and (c) Decrypted image of dimension ($400 \times 150$).

Table IV
$\chi^2$ TEST VALUES OF ORIGINAL AND ENCRYPTED IMAGES.

| Image | Original image $\chi^2$ | Pass/Fail | Encrypted image $\chi^2$ | Pass/Fail |
|---|---|---|---|---|
| Baboon | 1092658.62 | Fail | 257.3138 | Pass |
| House | 325049.15 | Fail | 255.3854 | Pass |
| Peppers | 441923.29 | Fail | 214.1061 | Pass |
| Pirate | 267545.48 | Fail | 268.4160 | Pass |

Table V
CORRELATION COEFFICIENT OF ORIGINAL AND ENCRYPTED IMAGES.

| Image | Original Image | | | Encrypted Image | | |
|---|---|---|---|---|---|---|
| | H | V | D | H | V | D |
| | 0.9415 | 0.9653 | 0.9131 | 0.0047 | 0.0094 | -0.0070 |
| House | 0.9137 | 0.9810 | 0.8975 | 0.0102 | 0.0097 | -0.0041 |
| | 0.9795 | 0.9809 | 0.9649 | -0.0016 | 0.0035 | 0.0088 |
| Boat | 0.9736 | 0.9393 | 0.9247 | -0.0050 | -0.0051 | -0.0020 |
| Pirate | 0.9660 | 0.9649 | 0.9417 | 0.0041 | 0.0051 | -0.0116 |
| Average | 0.9638 | 0.9632 | 0.9375 | 0.0017 | 0.0056 | -0.0050 |

### A. Statistical analysis

This subsection gives our proposed scheme's evaluation metrics for histogram analysis, correlation coefficients, and differential analysis.

*1) Histogram analysis:* The histogram contains the statistical information about the original image. A good image encryption algorithm should be able to produce a well-distributed and equalized flat histogram that does not preserve statistical information.

The $\chi^2$ test is employed to derive numerical outcomes, helping to mitigate potential visual misinterpretations. The Eq. 7 calculates the chi-square values.

$$\chi^2 = \sum \frac{(O_I - E_i)^2}{E_i} \tag{7}$$

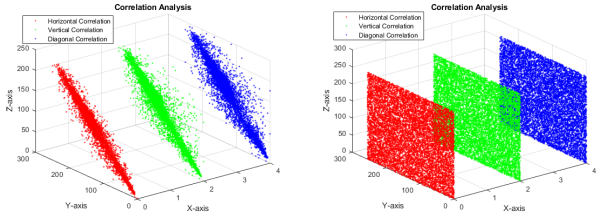
In Eq. 7, $O_i$ is the observed value, and $E_i$ is the expected value. If $\chi^2 \geq 293.24783$, then the histogram distribution is uniform [35]. In Table IV, we have given $\chi^2$ test results of the original and encrypted images. The results show that it can resist statistical attacks.

*2) Correlation coefficient analysis:* The images exhibit a notable correlation between neighbouring pixels. An encryption algorithm must be good enough to disrupt this inherent correlation. The correlation values are calculated using Karl Pearson formula [36] as follows:

$$\rho(x, y) = \frac{cov(x, y)}{\sigma(x)\sigma(y)} \tag{8}$$

In Eq. 8, $x$ and $y$ denote the values of adjacent pixels. In Table V, the correlation coefficient values for horizontal, vertical, and diagonal directions are given.

From Table V, it has been observed that horizontal correlation ranges from $0.9638$ to $0.0017$, which shows a change of around $99.82\%$, in case of vertical correlation ranges from $0.9632$ to $0.0056$ and a change around $99.41\%$ and diagonal correlation changes from $0.9375$ to $-0.0050$ which is around $99.46\%$. The results indicate no correlation between the original and encrypted images. Fig. 7 presents correlation




(a) (b)

Figure 7. Correlation plot of boat. (a) Original image and (b) Encrypted image.

plots for the original and encrypted image (boat), illustrating the horizontal, vertical, and diagonal correlations.

*3) Differential analysis:* The ability of any encryption algorithm to resist a CPA is evaluated through differential analysis. The test parameters used for differential analysis are the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) [37].

Let $\mathcal{C}$ be an encrypted image obtained from a plain image $\mathcal{P}$ using a cryptosystem and key $k$. Now, if one pixel of $\mathcal{P}$ is changed to create $\mathcal{P}'$, and $\mathcal{P}'$ is encrypted with the same key $k$ to produce $\mathcal{C}'$, then for an image of width $w$, height $h$, and bit depth $d$ per pixel, the NPCR ($\mathcal{N}$) and UACI ($\mathcal{U}$) is calculated as follows:

$$\mathcal{D}(i,j) = \begin{cases} 0, & \mathcal{C}(i,j) = \mathcal{C}'(i,j) \\ 1, & \mathcal{C}(i,j) \neq \mathcal{C}'(i,j) \end{cases} \tag{9}$$

$$\mathcal{N}(\mathcal{C}, \mathcal{C}') = \frac{\sum_{x,y} \mathcal{D}(x,y)}{w \times h} \times 100\% \tag{10}$$

$$\mathcal{U}(\mathcal{C}, \mathcal{C}') = \frac{\sum_{x,y} |\mathcal{C}(x,y) - \mathcal{C}'(x,y)|}{(2^p - 1) \cdot (w \times h)} \tag{11}$$

The critical $\mathcal{N}$ and $\mathcal{U}$ values [37] for a $512 \times 512$ and 8-bit pixel depth image are given in Table VI. Further, Tables VII and VIII show the $\mathcal{N}$ and $\mathcal{U}$ values for different significant levels for the proposed method.

Table VI
CRITICAL VALUES OF $\mathcal{N}$ AND $\mathcal{U}$ RANDOMNESS TEST WITH SIGNIFICANCE LEVEL ($\alpha$) 0.05, 0.01, AND 0.001.

| Pixel depth | Significance level | Critical $\mathcal{N}$ | Critical $\mathcal{U}$ | |
|---|---|---|---|---|
| P | $\alpha$ | $\mathcal{N}^*_\alpha$ | $\mathcal{U}^{*+}_\alpha$ | $\mathcal{U}^{*-}_\alpha$ |
| 8 | 0.05 | 99.589335 | 33.372959 | 33.554124 |
| 8 | 0.01 | 99.581033 | 33.344496 | 33.582587 |
| 8 | 0.001 | 99.571726 | 33.311465 | 33.615618 |

Table VII
$\mathcal{N}$ TEST RESULTS FOR DIFFERENT SIGNIFICANCE LEVEL.

| Image | $\mathcal{N}$ | Critical $\mathcal{N}$ value | | |
|---|---|---|---|---|
| | | $\alpha$= 0.05 | $\alpha$ = 0.01 | $\alpha$ = 0.001 |
| Boat | 99.6051% | Pass | Pass | Pass |
| Pirate | 99.6117% | Pass | Pass | Pass |
| House | 99.5956% | Pass | Pass | Pass |

Table VIII
$\mathcal{U}$ TEST RESULTS FOR DIFFERENT SIGNIFICANCE LEVEL.

| Image | $\mathcal{U}$ | Critical $\mathcal{U}$ value | | |
|---|---|---|---|---|
| | | $\mathcal{U}^{*-}_{0.05}/\mathcal{U}^{*+}_{0.05}$ | $\mathcal{U}^{*-}_{0.01}/\mathcal{U}^{*+}_{0.01}$ | $\mathcal{U}^{*-}_{0.001}/\mathcal{U}^{*+}_{0.001}$ |
| Boat | 33.4175% | Pass | Pass | Pass |
| Pirate | 33.4322% | Pass | Pass | Pass |
| House | 33.5160% | Pass | Pass | Pass |

### B. Information entropy

The measurement of randomness for any information is denoted as information entropy [38], defined by as follows:

$$H(S) = \sum_{i=1}^{N} p_i \log_2 \frac{1}{p_i} \tag{12}$$

In Eq. 12, $x_i$ consists of $N$ bits, with $P(x_i)$ representing the probability and $N$ denoting the gray level. The entropy $H(x)$ is a crucial measure in image cryptography as it quantifies the unpredictability and disorder within an image, which is essential for assessing randomness. Higher entropy indicates greater uncertainty in gray values, thereby enhancing the security of cryptographic systems. In an ideal scenario with a random image featuring 256 grey levels, $H(x)$ reaches its maximum value of 8, reflecting high unpredictability and serving as a key metric for evaluating the robustness of cryptographic systems. Table IX presents the entropy values of the encrypted images using the proposed encryption algorithm.

Table IX
INFORMATION ENTROPY OF ENCRYPTED IMAGES.

| Image | Cipher Image | | |
|---|---|---|---|
| | R | G | B |
| House | 7.9974 | 7.9972 | 7.9970 |
| Peppers | 7.9993 | 7.9994 | 7.9994 |
| | Grayscale | | |
| Boat | 7.9992 | | |
| Cameraman | 7.9992 | | |

### C. Comparison

This section compares our proposed algorithm with existing image cryptosystems using statistical metrics as detailed in Refs [11], [12], [21]–[23]. Image encryption is typically vulnerable to CPA, where an adversary selects plaintexts and analyzes the resulting ciphertexts to find weaknesses. KPA occur when an attacker has access to known plaintext-ciphertext pairs, allowing them to detect patterns and compromise security. To counter both CPA and KPA attacks, Fig. 8 shows encryption and decryption results for $512 \times 512$ pixel Black and White images using the DNA-LFSR algorithm. Test results in Tables X and XI demonstrate strong NPCR, UACI, and Chi-square performance, aligning closely with theoretical expectations. The entropy and correlation values also match theoretical predictions, affirming the algorithm's security. The block-cyclic construction and DNA LFSR randomization effectively thwart cryptanalytic attacks, as our algorithm's high levels of confusion and diffusion make such attacks ineffective.

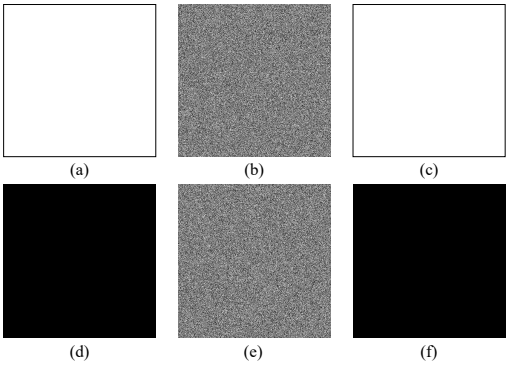



Figure 8. Encryption and decryption by DNA-LFSR, (a) Plain image white, (b) Cipher image, (c) Decrypted image, (d) Plain image black, (e) Cipher image, and (f) Decrypted image.

Table X
INFORMATION ENTROPY AND CORRELATION OF CIPHER IMAGES.

| Image | Entropy | H | V | D |
|---|---|---|---|---|
| Black | 7.9992 | -0.0094 | 0.0125 | 0.0076 |
| White | 7.9993 | -0.0022 | -0.0066 | -0.0209 |
| Average | 7.99925 | -0.0058 | 0.0029 | -0.0066 |

Table XI
$\chi^2$ VALUE, NPCR, UACI VALUES OF CIPHER IMAGE.

| Image | $\chi^2$ value | NPCR (%) | Result | UACI (%) | Result |
|---|---|---|---|---|---|
| Black | 274.8379 | 99.6052 | Pass | 33.4886 | Pass |
| White | 267.6250 | 99.6113 | Pass | 33.4802 | Pass |
| Average | 271.2315 | 99.60825 | Pass | 33.4844 | Pass |

Table XII
SECURITY COMPARISON WITH EXISTING SCHEME.

| Algorithm | Entropy | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| Proposed | 7.99925 | -0.0050 | -0.0051 | -0.0020 |
| Lai et al. [11] | 7.9978 | 0.0036 | -0.0034 | 0.0083 |
| Wang et al. [12] | 7.9993 | -0.0088 | 0.0047 | 0.0053 |
| Sun et al. [21] | 7.9988 | 0.0022 | -0.0105 | -0.0035 |
| Chen et al. [22] | 7.9914 | -0.0043 | -0.0067 | 0.0006 |
| Ali et al. [23] | 7.9984 | -0.0032 | -0.0017 | 0.0027 |

So, our proposed scheme ensures no information about the original images is revealed, confirming its robustness against potential attacks. Comparative assessments with proposed encryption methods referenced in [11], [12], [21]–[23] are summarized in Table XII. The proposed encryption algorithm is resilient against differential attacks, as the NPCR value is 99.61% and UACI is 33.46%, which is near the ideal value, respectively and outperforming all states of the arts ciphers. Overall, the proposed algorithm shows flexibility, efficiency, and high security, rendering it a practical option for image encryption requirements.

## V. CONCLUSION

In current storage systems, users do not have direct control over their stored images, which inevitably reveals their privacy to potential risks. This paper introduces confusion through

block-cyclic construction mapping. Subsequently, it offers to integrate a Deoxyribonucleic Acid (DNA)-based LFSR into the diffusion phase to increase the security level. Considerable performance evaluations and analyses were conducted, including comparisons with other cryptographic systems proposed in existing literature. These estimations demonstrated that the current cryptosystem exhibited favourable random characteristics and high-security levels. Comprehensive experimental studies and attack simulations have been conducted to validate the security of the proposed algorithm. These studies show that the algorithm possesses a sufficiently large key space and sensitivity. Additionally, the attributes of the ciphertext image, such as information entropy, correlation of adjacent pixels, NPCR, and UACI, closely align with theoretical values. The practicality and usefulness of the proposed scheme are validated through experimental findings, indicating its potential suitability for multimedia security applications.

## ACKNOWLEDGEMENT

The authors extend their appreciation to the Researchers Supporting Program at King Saud University. Researchers Supporting Project number (RSPD2024R867), King Saud University, Riyadh, Saudi Arabia.

## REFERENCES

[1] Y. Dou and M. Li, "Cryptanalysis of a new color image encryption using combination of the 1d chaotic map," *Applied Sciences*, vol. 10, no. 6, p. 2187, 2020.

[2] J. M. K. Mastan and R. Pandian, "Cryptanalysis of two similar chaos-based image encryption schemes," *Cryptologia*, vol. 45, no. 6, pp. 541–552, 2021.

[3] P. Dang and P. Chau, "Image encryption for secure internet multimedia applications," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 395–403, 2000.

[4] A. Arora and R. K. Sharma, "Known-plaintext attack (kpa) on an image encryption scheme using enhanced skew tent map (estm) and its improvement," *Optik*, vol. 244, p. 167526, 2021.

[5] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using gan-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3977–3984, 2024.

[6] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps," *Ieee Access*, vol. 6, pp. 18 759–18 770, 2018.

[7] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Processing*, vol. 118, pp. 203–210, 2016.

[8] Y. Zhang, C. Li, Q. Li, D. Zhang, and S. Shu, "Breaking a chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 69, pp. 1091–1096, 2012.

[9] Q. Wang, X. Zhang, and X. Zhao, "Color image encryption algorithm based on novel 2d hyper-chaotic system and dna crossover and mutation," *Nonlinear Dynamics*, pp. 1–27, 2023.

[10] J. Wu, J. Zhang, D. Liu, and X. Wang, "A multiple-medical-image encryption method based on sha-256 and dna encoding," *Entropy*, vol. 25, no. 6, p. 898, 2023.

[11] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multi-scroll memristive hopfield neural network with adjustable memductance and application to image encryption," *IEEE Transactions on Neural Networks and Learning Systems*, 2022.

[12] L. Wang, S. Jiang, M.-F. Ge, C. Hu, and J. Hu, "Finite-/fixed-time synchronization of memristor chaotic systems and image encryption application," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 12, pp. 4957–4969, 2021.

[13] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding," *Expert Systems with Applications*, vol. 237, p. 121514, 2024.

[14] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on dna encoding," *Optics & Laser Technology*, vol. 95, pp. 94–99, 2017.

[15] R. Soni, G. Prajapati, A. Khan, and D. Kulhare, "Triple stage dna cryptography using sequential machine," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 8, pp. 859–867, 2013.

[16] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new dna sequence operation," *Chaos, Solitons & Fractals*, vol. 162, p. 112456, 2022.

[17] Q. Zhang and X. Wei, "A novel couple images encryption algorithm based on dna subsequence operation and chaotic system," *Optik*, vol. 124, no. 23, pp. 6276–6281, 2013.

[18] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on dna operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558–2565, 2016.

[19] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic dna encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[20] X. Wang, Y. Su, L. Liu, H. Zhang, and S. Di, "Color image encryption algorithm based on fisher-yates scrambling and dna subsequence operation," *The Visual Computer*, pp. 1–16, 2021.

[21] Y. Sun, K. Yu, A. K. Bashir, and X. Liao, "Bl-iea: A bit-level image encryption algorithm for cognitive services in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[22] X. Wang and M. Zhao, "An image encryption algorithm based on hyperchaotic system and dna coding," *Optics & Laser Technology*, vol. 143, p. 107316, 2021.

[23] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and boolean operation," *Multimedia Tools and Applications*, vol. 79, no. 27-28, pp. 19 853–19 873, 2020.

[24] C. Zhang, J. Chen, D. Chen, W. Wang, Y. Zhang, and Y. Zhou, "Exploiting substitution box for cryptanalyzing image encryption schemes with dna coding and nonlinear dynamics," *IEEE Transactions on Multimedia*, vol. 26, pp. 1114–1128, 2024.

[25] F. Ahmed, M. U. Rehman, J. Ahmad, M. S. Khan, W. Boulila, G. Srivastava, J. C.-W. Lin, and W. J. Buchanan, "A dna based colour image encryption scheme using a convolutional autoencoder," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 3s, pp. 1–21, 2023.

[26] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color image cryptosystem based on sine chaotic map, 4d chen hyperchaotic map of fractional-order and hybrid dna coding," *IEEE Access*, vol. 11, pp. 54 928–54 956, 2023.

[27] P. K. Pal, D. Kumar, and V. Agarwal, "Efficient image encryption using the tinkerbell map in conjunction with linear feedback shift registers," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 44 903–44 932, 2024.

[28] S. Deb, B. Biswas, and B. Bhuyan, "Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field," *Multimedia Tools and Applications*, vol. 78, pp. 34 901–34 925, 2019.

[29] S. Deb and B. Bhuyan, "Chaos-based medical image encryption scheme using special nonlinear filtering function based lfsr," *Multimedia Tools and Applications*, vol. 80, pp. 19 803–19 826, 2021.

[30] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *science*, vol. 266, no. 5187, pp. 1021–1024, 1994.

[31] L. Wang, S. Jiang, M.-F. Ge, C. Hu, and J. Hu, "Finite-/fixed-time synchronization of memristor chaotic systems and image encryption application," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 12, pp. 4957–4969, 2021.

[32] G. Zeng, W. Han, and K. He, "High efficiency feedback shift register: $\sigma-$lfsr," Cryptology ePrint Archive, Paper 2007/114, 2007, https://eprint.iacr.org/2007/114. [Online]. Available: https://eprint.iacr.org/2007/114

[33] F. B. Demir, T. Tuncer, and A. F. Kocamaz, "A chaotic optimization method based on logistic-sine map for numerical function optimization," *Neural Computing and Applications*, vol. 32, pp. 14 227–14 239, 2020.

[34] Usc-sipi image database. [Online]. Available: https://sipi.usc.edu/database/database.php

[35] E. H. Rachmawanto, R. Zulfiningrum *et al.*, "Medical image cryptosystem using dynamic josephus sequence and chaotic-hash scrambling," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6818–6828, 2022.

[36] I. Cohen, Y. Huang, J. Chen, J. Benesty, J. Benesty, J. Chen, Y. Huang, and I. Cohen, "Pearson correlation coefficient," *Noise reduction in speech processing*, pp. 1–4, 2009.
[37] Y. Wu, J. P. Noonan, S. Agaian *et al.*, "Npcr and uaci randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.
[38] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.