

Lightweight IOT-friendly image encryption scheme based on Latin square and dynamic DNA coding

Sameeh Abdulghafour Jassim¹⁾, Seddiq Q. Abd Al-Rahman²⁾ and Ahmed Adil Nafea^{*3)}

¹⁾Department of Vocational Education in Anbar, Ministry of Education, Anbar, Iraq

²⁾Department of Computer Networks Systems, College of Computer Science and IT, University of Anbar, Ramadi, Iraq

³⁾Department of Artificial Intelligence, College of Computer Science and IT, University of Anbar, Ramadi, Iraq

Received 30 August 2025

Revised 15 November 2025

Accepted 8 January 2026

Abstract

The fast growth of Internet of Things (IoT) devices calls for the demand to accomplish an efficient and lightweight image encryption. Also, protecting the privacy of sensitive visual information on devices with limited resources presents significant challenges. Existing techniques and methods are not able to provide both powerful security and low computational requirements. Therefore, we propose an innovative encrypting scheme that combines three methods (Latin squares, dynamic DNA sequencing, and chaotic systems). This architecture is designed for the IoT environments where it is important that transactions are made both efficient and secure. Additionally, our approach offers strong security assurances and suitable for the constraints of edge devices. The performance evaluations of the proposed technique against modern encryption algorithms display a promising result. Our proposal demonstrates almost perfect randomness. It achieved an image entropy of (7.9994) and a minimal correlation of (-0.00472). The proposed system also demonstrated its high ability to resilience the differential attacks, with NPCR and UACI of (98.671) and (34.098), respectively. Also, the keyspace of the proposed method is (2^{200000}), that providing a robust defense against brute-force attacks. Despite this high security level, the technique maintains practical performance, encrypting a (512×512) image in (1.4026) seconds. These outcomes confirm the algorithm's effectiveness for protecting sensitive images in IoT applications, offering both security and suitable efficiency for real-world use.

Keywords: Chaotic systems, Lightweight encryption, Image encryption, Henon map, Security enhancement

Symbols and notations list

I	input image (grayscale)	F^{-1}	Number-to-base inverse mapping
$M \times N$	dimensions of Image (height $\times$ width)	Idx_r	Row permutation indices ($\text{argsort}(S_r)$)
P	Permuted of the image after Latin square transformation	idx_c	Column permutation indices ($\text{argsort}(S_c)$)
E	Encrypted image	inv_idx_r	Inverse row permutation indices
D	Decrypted image (output)	inv_idx_c	Inverse column permutation indices
K	256-bit secret key (derived from SHA-256 hash)	P_{ij}	Pixel value at position (i,j)
$SHA256(.)$	Cryptographic hash function	B	8-bit binary representation of pixel
x_0, y_0	Initial conditions for Henon map (derived from K)	r	DNA encoding rule index $r \in [0, 7]$
S_r	Row permutation sequence	ε_r	DNA encoding function (Rule r)
S_c	Column permutation sequence	D_r	DNA decoding function (Inverse of ε_r)
S_{rule}	DNA encoding rule selection sequence	d_k	Diffusion modifier from S_{diff}
S_{diff}	DNA diffusion modifier sequence	$int(.,2)$	Binary-to-integer conversion
L	Total chaotic sequence length ($L=1000+M+N+5MN$)	$bin(.)$	Integer-to-binary conversion
F	Base-to-number mapping ({A:0, C:1, G:2, T:3})	$zfill(8)$	Zero-padding to 8 bits

1. Introduction

Due to the rapid progress in the field of technology, especially the increasing need for lightweight encryption of images [1, 2]. With the versatile nature of images as visual media that carry valuable information, they are an attractive target for cyberattacks [3]. In addition, unlike the encryption of normal texts, the form of the image is special because it has high internal redundancy, abundant information content and correlation of strong space between pixels. Moreover, as the world is moving towards a more and more technologically dependent society with photo-based tasks like Internet of Things (IoT) and cloud computing [4]. This has made safeguarding this data even more essential. Therefore, cryptography helps in transmitting messages in a way that it becomes unintelligible for attackers to read, as it hides the traffic [5-7]. Therefore, much more attention should be paid to making image

*Corresponding author.

Email address: ahmed.a.n@uoanbar.edu.iq

<https://doi.org/10.64960/easr.2026.263754>

encryption methods strong enough. Unlinking cryptology and chaotic systems A strong association of cryptology with chaotic systems has been observed. Chaotic systems lack characteristic features such as ergodicity, unpredictability, and sensitive dependence on the control and initial parameters that meet the demands of cryptography. The obtained values from the chaotic systems being mostly random but still fair bits progress when considered for encrypting the data [8].

A tradeoff is present between the security of data and the simplicity of the algorithm or decreased resource utilization. To enhance data security, more intricate algorithms are often necessary, which results in increased computational resources. The pursuit of an optimal method of encryption that is both safe and simple, known as the lightweight algorithm, has been the most prominent academic focus [9]. This paper describes a method of encryption that is resource-effective while still providing a significant security benefit for devices that have limited resources. For these reasons, we select to use chaotic systems due to some of their natural characteristics which support a level of efficiency in an encryption scheme. In addition, a novel image encryption scheme with capability of security improvement and adversary resistances is presented in this paper. This Iot-based visual cryptosystem combines chaotic dynamics with biological computation principles by associating them in a three-tier cryptosystem pipeline. Our approach encrypts the input image and also decrypts back to recover the plaintext, whereas in our work an unique 256 bit cryptographic key is obtained by means of SHA-256 hashing for input image that seeds a Henon chaotic map such that four different cryptographic sequences are produced. these sequences encode: 1) Latin square-based spatial permutation by shuffling pixel locations with row-column operations, 2) dynamic DNA coding where binary data of each pixel are conveyed to nucleotide bases (A, C, G, T) using one out of eight variable encoding rules chosen per-pixel by chaotic parameters and 3) the nucleotide diffusion through modular arithmetic operations. The symmetric architecture enables perfect reconstruction through inverse DNA decoding and reverse permutation using the same image-derived key, maintaining computational efficiency with O(MN) complexity and minimal memory overhead tailored for resource-constrained devices. Therefore, the proposed method try bring a good amount of randomness, complexity, and resistance for any unauthorized decryption.

The remainder of the paper is organized into five major parts. Section 2 discusses the existing literature on chaos-based encryption algorithms in depth, they discuss the benefits and drawbacks of using these algorithms in the field, as well as their contributions to the field. Section 3 describes the materials and methodology of the proposed encryption algorithm. Section 4 gives the experimental results achieved by applying the algorithm proposed to different attacks, including statistical, key, differential, and brute-force analysis. This section compares the performance of the proposed technique with other existing methods. Section 5 concludes the paper and discusses how the described algorithm could be useful in providing secure encryption for images.

2. Related work

Image encryption for IoT has made its breakthrough recently and can be characterized to evolve along three distinctive technical directions. The first was thought to involve architectural advances in cipher constructions. In fact, tree-based structures combined with Feistel networks were proposed in [10, 11] to provide hierarchical processing of blocks. On typical IoT hardware like a Raspberry Pi, these architectures turn out to be quite efficient and offer a significant speed up. However, when we look at the security evaluations for several of these candidates, it is clear that this has been a general shortcoming; few have received complete testing against side-channel attacks and few have been compared to many existing ciphers.

A second technical directions merge biological computation with cryptography. In [12-14] the research studies utilized dynamic DNA coding, where pixel values are mapped to customizable sequences of nucleotides (A, G, C, and T). This integration adds a powerful layer of confusion to the encrypted images. Moreover, using chaotic maps make these systems often show strong security results with nearly ideal randomness and low correlation. However, there are a common limitation issue is that, they have not been thoroughly tested on truly resource-limited IoT devices, making their real-world performance uncertain.

The third technical directions take pros of the potential advanced chaotic systems. Many significant studies [13-18] utilize hyperchaotic and memristive chaotic maps as high-quality entropy sources of randomness to enhance the processes of permutation and diffusion [14, 17, 18]. whereas these complex systems offer excellent security metrics. However, there is a big challenge in balancing between the security strength and the computational needs. Implementing these advanced models on lightweight hardware is a significant difficult [15, 16, 18]. In addition, there is a trend toward specialization, with methods now focusing on specific of datatypes, from traditional 2D images [13, 14, 16] to new 3D medical models [17].

Beyond these technical direction's clusters, other researchers have utilized optimization or hybrid techniques. Abed et al. [19] combined various advanced techniques but that increase system complexity and caused a high computational cost. Ahmad et al. [20] leveraged chaos and number theory, but their security is highly dependent on the initial parameters selection of the chaotic systems. Zhuang et al. [21] and Abed et al. [22] focused on dynamic substitution by utilizing S-boxes, yet their security depending heavily on the design quality of these components. Approaches utilizing optimization algorithms such as GWO [22] or complex mathematics such as fractional-order chaos [23] often increase computational overhead. Whereas methods such as those in [24] and [25] show promise, their security analysis often lacks depth, especially against side-channel attacks, and their practical efficiency for real-time IoT use is frequently unproven.

The literature achieves a significant step forward based on Structural- Biological and Chaotic constructions. However, a challenge in most of the works is to find the trade-off between strong security and the poor computational capability of low-power IoT devices. Many approaches have the problem of being too complex, not tested enough in practice and not having a complete security verification, especially against side-channel attacks. These gaps identified show that the new encryption scheme should strike a better balance between security, efficiency and practicality for the IoT environment. In the following, we propose a framework in order to overcome these challenges using Latin squares combined with dynamic DNA computing and a slight chaotic system.

3. Materials and methods

The aim of this work is to propose an image security scheme which offers both high-level protection and computational performance. Besides, this work is focused on constrained platforms, such as the Internet of Things (IoT), embedded devices and wireless sensors. So it will be accomplished via simple operations and also it will reduce the processing. Furthermore, the proposed system architecture uses a compact, four-stage cryptographic pipeline tailored for IoT resource- constrained environments, as presented in Figure 1. The two stages cooperate orderly to convert base-band image into secure cipher-image with no degradation in performance

of reconstruction during decryption. The design avoids complex mathematical operations in favour of a light-weight computational scheme that achieves performance-complexity trade-off for security.

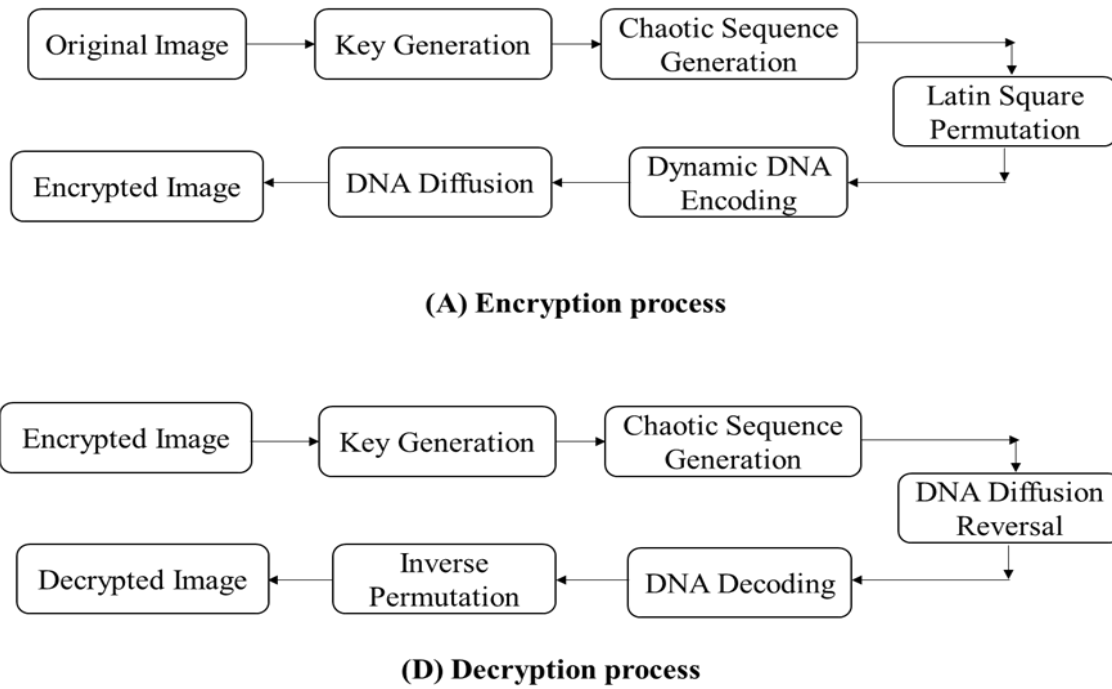


Figure 1 The flowchart of the complete encryption/decryption process

3.1 Key generation and initialization

The proposed approach starts with an advanced key derivation system that work to enhance the security through forward secrecy. Instead of depending on fixed values of keys, the system directly derives distinct cryptographic content from the image inputs. The raw pixel data are hashed utilizing the (SHA-256) algorithm to generate a (256-bit) fingerprint. This image-derived hash has two purposes: it is guaranteeing the uniqueness of the key values for every single input, and provides tamper-evident characteristics. Subsequently, the hash is transformed into the initial conditions of a chaotic system through bitwise partitioning. The first 128 bit is the x coordinate seed and the rest of bits will be the y coordinate seed. As a result, changes as small as one pixel in the source image result in completely different cryptographic parameters, which is key to achieving a strong diffusion property.

Algorithm 1: (Key Generation and Initialization)

Input: Original grayscale image I of size $(M \times N)$

Output: K (Secret key of 256-bit Hash value)

1. Compute SHA-256 hash values of image (I): $K \leftarrow \text{SHA256}(I)$
2. Divide the 256-bit secret key K into two equal 128-bit parts (K_1 and K_2): $K_1 \leftarrow [0 \text{ to } 31]$ and $K_2 \leftarrow [32 \text{ to } 63]$
3. Convert the hexadecimal segments (K_1 and K_2) into their corresponding 128-bit integer (x_0 and y_0):

$$x_0 \leftarrow \frac{\text{HexToDec}(k_1)}{2^{128}} \text{ and } y_0 \leftarrow \frac{\text{HexToDec}(k_2)}{2^{128}}$$

Return: K , x_0 and y_0 .

3.2 Chaotic sequence

At the heart of the system lies a lightweight chaotic generator that creates cryptographic sequences without intensive computation. The Henon map, selected for its balance among complexity and efficiency, processes the derived seeds to generate pseudorandom sequences. Figure 2 displays the complex chaotic behavior of the Henon map. This two-dimensional discrete system is mathematically represented by the equations [26]:

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (1)$$

$$y_{n+1} = bx_n$$

Where parameters a and b control the systems bifurcation properties. Especially, the contraction factor in this map remains constant regardless of the x and y values. The visualization in Figure 1 shows the maps evolutionary pattern under specific parameter choices and initial conditions, revealing its characteristic chaotic attractor.

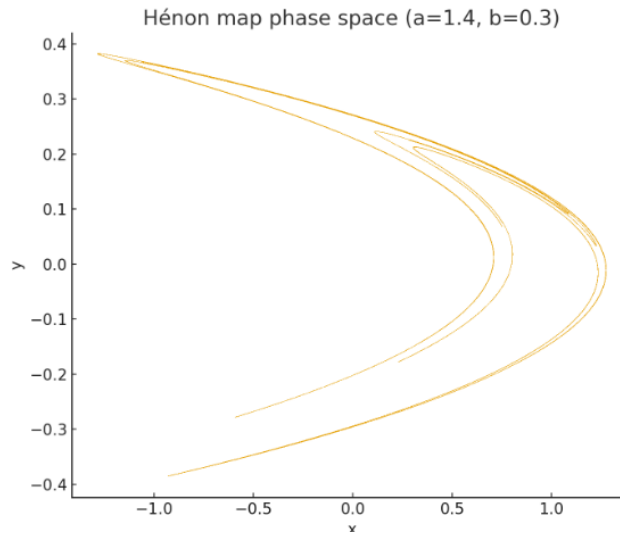


Figure 2 Henon Map: Chaotic behavior

In order to add unpredictability, the system deletes first 1000 output values (an essential operation that destroys transient patterns subjecting the cipher to cryptanalysis on Figure 3). The rest of the chaotic output is divided into four specialized streams: row-shuffling coordinates, column-shuffling coordinates, DNA rule-selection indexes and diffusion modifiers. Respective scaling, reduction operations for each stream are then carried out to adapt to operating dimensions. This stage's memory overhead is modest, which keeps only the active sequences and has real potential to be supported by microcontrollers with limited RAM.

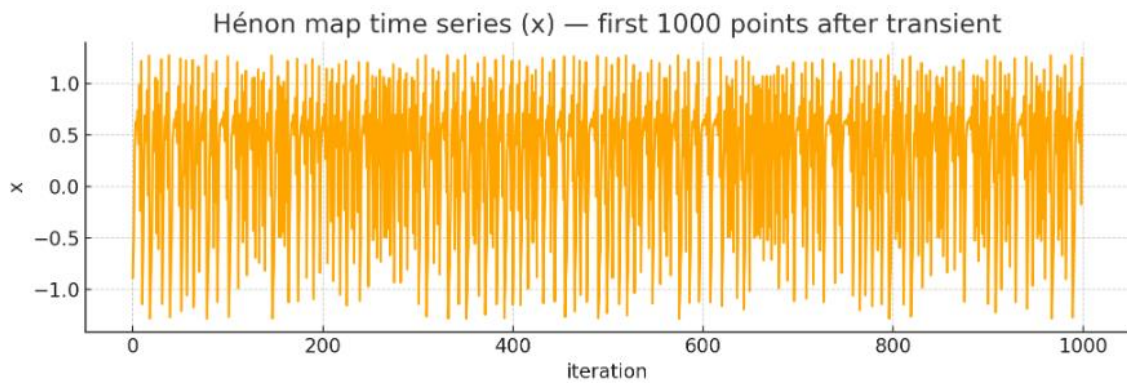


Figure 3 Henon Map: First 1000 points after transient

Algorithm 2: (Chaotic Sequence Generation)

Input: initial conditions (x_0, y_0) from Algorithm 1, and image dimensions (M, N)

Output: Permutation sequences row (S_r) and coloumn (S_c)

DNA Rule Selection Sequence (S_{rule})

Diffusion Sequence (S_{diff})

1. Generate chaotic sequences using Henon map:

$$\begin{cases} x_i = 1 - 1.4x_{i-1}^2 + y_{i-1} \\ y_i = 0.3x_{i-1} \end{cases} \quad \text{for } i = 1 \text{ to } L,$$

where $L = 1000 + M + N + M \times N + 4 \times M \times N$

2. Discard first 1000 transient points

3. Extract subsequences:

- Row permutation: $S_r \leftarrow \{x_{1001} \dots x_{1000+M}\}$

- Column permutation: $S_c \leftarrow \{x_{1001+M} \dots x_{1000+M+N}\}$

- DNA rule selection: $S_{rule} \leftarrow \lfloor \{x_{1001+M+N} \dots x_{1000+M+N+M \times N}\} \times 10^4 \rfloor \bmod 8$

- Diffusion sequence: $S_{diff} \leftarrow \lfloor \{x_{1001+M+N} \dots x_L\} \times 10^4 \rfloor \bmod 4$

Return: (S_r) , (S_c) , (S_{rule}) , and (S_{diff})

3.3 Spatial permutation module

The permutation in this study utilized Latin square rules to break up a special correlation with the image [27]. The system creates a distinct permutation scheme from the chaotic row coordinates, by sorting an index of positions. This pattern reshuffles all the pixel

lines into non-linear permutation to jumble vertical structures. A similar procedure is replicated for columns which take advantage of the chaotic column-address, horizontally spreading pixel relationships. This two-axis shuffling is achieved by efficient indexing, rather than computationally expensive matrix operations. The module is keepable-performance with in-place image processing instead of situating multiple images. The visual obfuscation effect is considerable while the computational complexity depends only on image size.

Algorithm 3: (Latin Square-based Permutation)

Input: Image (I), sequences S_r, S_c (from Algorithm 2), Iterations Number T.

Output: Permuted image P

1. Initial Image Setup: $P \leftarrow I$
2. Generate permutation indices: $idx_r \leftarrow \text{argsort}(S_r)$
 $idx_c \leftarrow \text{argsort}(S_c)$
3. Iterative Permutation Loop: *for* $t \leftarrow 0$ *to* T *do*:
4. Apply row permutation: *for* $i \leftarrow 0$ *to* $M-1$ *do*:
 $P(i,:) \leftarrow I(idx_r(i,:))$
5. Apply column permutation: *for* $j \leftarrow 0$ *to* $N-1$ *do*:
 $P(:,j) \leftarrow P(:,idx_c(j))$
6. End for (t)

Return P.

3.4 Dynamic DNA cryptography core

The most advanced stage involves biological computing inspired by dynamic DNA operations [28]. Each pixel has a real-time binary decomposition in four 2-bit segments. One such disordered selection channel then randomly assigns one of eight possible pixel-wise DNA-encoding rules, where each rule consists of a bit-pair-to-base (A,C,G,T) map. After the bioencoding, a diffusion process modulates their numerical coding through chaotic elements. In the encryption part of the algorithm nucleotide values are combined with diffusion streams by addition modulo 4 while in the decryption part, they are removed using inverse subtraction. The sequence is then reconstructed as pixels by decoding (turning nucleotide sequences into binary) back using the same dynamic rules. This protocol used to ensure byte-level diffusion, (a change in a single bit can affect multiple nucleotides). At the same time, it maintains the computational efficiency provided by lookup table operations, instead of relying on complex arithmetic processes.

Algorithm 4: (Dynamic DNA Encoding and Diffusion)

Input: Permuted image P, sequences S_{rule}, S_{diff}

Output: Encrypted image E

1. For each pixel P_{ij} at position (i, j):
 - Convert to binary: $B \leftarrow \text{bin}(p_{ij})[2:]$. $z_{fill}(8)$
 - Split into 2-bit groups: $G \leftarrow \{B[0:2], B[2:4], B[4:6], B[6:8]\}$
2. Dynamic DNA encoding: $r \leftarrow S_{rule}[i \times N + j]$
 $Base_k \leftarrow \varepsilon_r(G_k) \quad \forall k \in \{0, 1, 2, 3\}$

where ε_r is encoding rule r from Table 1

3. DNA diffusion:
 - For each pixel (i,j) do:
 - For each DNA Base $k \leftarrow 0$ *to* 3 *do*
 - $Num_k \leftarrow f(Base_k)$
 - $d_k \leftarrow S_{diff}[4 \times (i \times N + j) + k]$
 - $Num'_k \leftarrow (Num_k + d_k) \bmod 4$
 - $Base'_k \leftarrow f^{-1}(Num'_k)$
 - end *for* k
4. DNA decoding: $G'_k \leftarrow D_r(Base'_k)$
 $P'_{ij} \leftarrow \text{int}(G'_0 + G'_1 + G'_2 + G'_3, 2)$
5. DNA Operations:
 - Encoding: $\varepsilon_r: \{00, 01, 10, 11\} \rightarrow \{A, C, G, T\}$
 - Decoding: $D_r = \varepsilon_r^{-1}$
 - Numerical mapping: $f: \{A, C, G, T\} \rightarrow \{0, 1, 2, 3\}$

Return E.

Table 1 DNA Encoding Rules

Rule	00	01	10	11
0	A	C	G	T
1	A	G	C	T
2	C	A	T	G
3	G	A	T	C
4	C	T	A	G
5	G	T	A	C
6	T	C	G	A
7	T	G	C	A

3.5 Decryption pathway

The architecture keeps symmetric decryption through reverse operation sequencing utilizing the original image hash, the system regenerates identical chaotic streams. Encrypted images first undergo reverse DNA operations: subtraction modulo 4 reverts diffusion effects before rule-based nucleotide-to-binary conversion. The spatial restoration module then applies inverse shuffling by processing stored permutation indices. Column positions revert first using the original chaotic column coordinates, followed via row restoration using row coordinates. This orderly reversal ensures perfect reconstruction while maintaining the same computational efficiency as encryption.

Algorithm 5: (Decryption Algorithm)

Input: Encrypted image E, key K, indices idx_r, idx_c

Output: Decrypted image D

- Regenerate S_{rule}, S_{diff} using K
- Reverse DNA diffusion: $Num'_k \leftarrow f(Base'_k)$
 $Num_k \leftarrow (Num'_k + d_k) \bmod 4$
- Apply inverse DNA encoding and decoding
- Inverse permutation: $inv_idx_c \leftarrow \text{argsort}(idx_c)$
 $inv_idx_r \leftarrow \text{argsort}(idx_r)$
for $j \leftarrow 0$ to $N-1$ do:
 $D(:, j) \leftarrow E(:, inv_idx_c(j))$
for $i \leftarrow 0$ to $M-1$ do:
 $D(i,:) \leftarrow D(inv_idx_r(i),:)$

Return D

4. Experimental results

This section presents the results obtained from experiments by running different attacks on the encryption scheme. Statistical attack analysis on a scheme is to measure the randomness and unpredictability of its output ciphers based on Shannon entropy, histogram analysis, and correlation coefficient analysis. Key analysis is based on keyspace exploration and sensitivity of the scheme towards changes in the key. Differential attack analysis is based on the vulnerability of the scheme to differential cryptanalysis. This is used to exploit the relation between differences in the plaintext and the corresponding differences in the ciphertext. Robustness analysis will basically give an effective measure of how tough the scheme is against several classes of attacks designed to cause degradation or manipulation in the produced ciphertext.

4.1 Statistical attack analysis

To assess how far the proposed encryption scheme goes as far as security is concerned, we subjected the scheme to a basic statistical attack analysis. The analysis was based on three basic metrics: Shannon entropy, histogram analysis, and correlation coefficient analysis. These metrics measure how far randomness, uniformity, and independence the ciphertext had, respectively.

4.1.1 Shannon entropy analysis

Entropy testing may be applied in assessing the randomness and unpredictability of a cryptographic algorithm. A measurement of entropy through the assessment of encrypted images determines how strong the described system is. It has the following definition [29, 30]:

$$H(I) = \sum_{j=1}^m P_r(I_j) \log_2 \frac{1}{P_r(I_j)} \quad (2)$$

Where the input image is denoted by (I), (I_j) indicates the value of the pixel, and the $\text{Pr}(I_j)$ indicates the (I_j) probability. For a $2n$ symbol data, the actual random entropy value is N. While there are 256 distinct colors and $2^8 = 256$. Consequently, the entropy value of a grayscale picture is 8. When the entropy value converges to the actual random entropy number, which in this example is 8, the method seems safer. Alternatively, it is seen as less secure. Our test findings, which converge to the actual random entropy value of 8, are illustrated in Table 2 and indicate good results. Specifically, grayscale images featuring Parrot, Cameraman, Monarch, and Baboon, sourced from [31].

Table 2 The information entropy levels of both encrypted and plain images

Image (size=512×512)	Entropy of the plain	Entropy of the encrypted
Parrot	7.6876	7.9994
Cameraman	7.0909	7.9973
Monarch	7.2813	7.9972
Baboon	7.3579	7.9994

4.1.2 Histogram analysis

The distribution of pixel frequencies in a picture is shown by histogram analysis. Histogram analysis is essential for an encrypted picture, and a balanced pixel value distribution is anticipated to fend against statistical assaults [2, 32]. Attackers may get information

about the original picture and hints about it if the histogram lacks a balanced distribution. The histogram analysis of both plain and encrypted pictures is shown in Figure 4. The encrypted picture histograms exhibit a notable dissimilarity from the original image histograms, with a very consistent appearance.

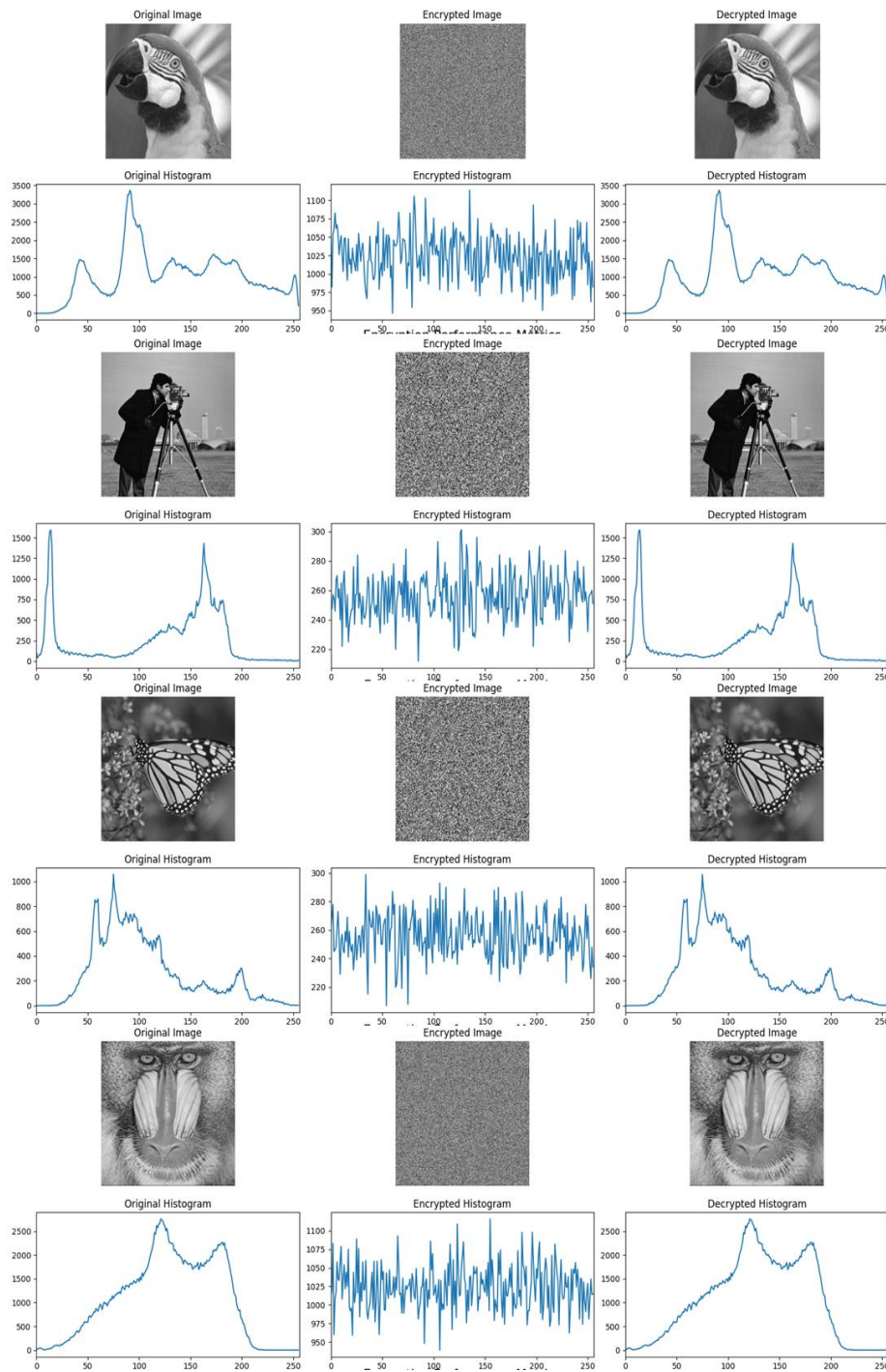


Figure 4 Analysis of the Histogram

4.1.3 Correlation coefficient analysis

The image correlation coefficient is a statistical relationship among adjacent pixels in terms of diagonal, vertical, and horizontal neighbors. It does provide adversaries with some valuable hints about the original image. Therefore, the best encryption technique would have to be designed in a way to break the significant correlation that does exist between adjacent pixels of a plain image and a cipher image. The correlation coefficient of pixels between the plain image and the matching cipher image is calculated by the following equation [30, 33]:

$$COR_{mn} = \frac{\frac{1}{P} \sum_{i=1}^P (x_i - E(m))(y_i - E(n))}{\sqrt{D(m)}\sqrt{D(n)}} \quad (3)$$

$$d(m) = \frac{1}{P} \sum_{i=1}^P (m_i - E(m))^2 \quad E(m) = \frac{1}{P} \sum_{i=1}^P m_i \quad (4)$$

The variables m_i and n_i represent the gray image values, whereas P represents the total number of pixels. E(m) and E(n) denote the mean values of m_i and n_i , respectively.

Based on the data shown in Table 3, it can be inferred that there is a weak correlation (close to zero) between the pixels of the plain image and the cipher image. Consequently, the proposed technique produces good results in terms of the analysis of correlation.

Table 3 Correlation coefficient values of both encrypted and plain images

Image	Plain image	Encrypted image
Parrot	0.92648	0.002913
Cameraman	0.93816	0.001455
Monarch	0.93214	0.001866
Baboon	0.92298	-0.004729

4.2 Key analysis

This section thoroughly analyzes the cryptographic keys used in the system. It encompasses two primary aspects: Keyspace analysis and Key Sensitivity Analysis.

4.2.1 Keyspace analysis

This part aims to evaluate the magnitude and variety of the potential key values. Increasing of keyspace length is a significant matter in security issues, because it is considered one of the essential methods for defense against brute-force attacks (where an adversary systematically attempts all combinations to guess the correct key). Increasing the size of the keyspace significantly increase the challenge for such attempts. It is generally accepted that a minimum length of keyspace is 2^{100} to ensure for contemporary computer systems to effectively resist brute force attacks. [34]. In the suggested technique, the secret keys consist of three components:

a) Key = SHA-256(Image) $\rightarrow$ 256-bit digest = 2^{256}

b) The Henon map's initial conditions are derived from the 256-bit hash with double-precision floating-point representation:

- $x_0 = \text{hash}[0 : 128] = 2^{128}$
- $y_0 = \text{hash}[128 : 256] = 2^{128}$

Total chaotic parameter space = 2^{256}

The variable rule selection adds combinatorial complexity:

- 8 DNA rules selectable per pixel.
- For 256×256 image: $262,144 \text{ pixels} \times 8 \text{ rules} = 2^{197752}$ possibilities.
- Rule changes per pixel create effective key space expansion.

The overall key space of the proposed system is: $Key_{space} = Key_{sha} \times Key_{chaos} \times Key_{dna}$
 $Key_{space} = 2^{256} \times 2^{256} \times 2^{197752} \approx 2^{200000}$

This is satisfactory for any encryption method.

4.2.2 Key sensitivity analysis

For an encryption method to be considered perfect, even little modifications to the key should lead to significant alterations in the output to effectively resist assaults. The image examines the impact of key alterations on authentication, encryption, decryption, and other cryptographic processes. The objective is to comprehend the system's responsiveness to significant modifications and detect any possible weaknesses that may result from compromised or leaked keys [35, 36]. The ciphertext difference rate (CDR) test is applied to measure the difference between the plaintext and the ciphertext. We, therefore, considered the sensitivity of the key from several perspectives of outcomes. This experiment was conducted by making minor modifications to the key. As shown by the formula [37]:

$$CDR = \sum \frac{Dif_{sum}(E1, E2) + dif_{sum}(E1, E3)}{2 \times Len} \times 100\% \quad (5)$$

where: $Dif(m1, m2) \begin{cases} 0 & \text{if } m1 = m2 \\ 1 & \text{if } m1 \neq m2 \end{cases}$, $Dif_{sum}(m1, m2) = \sum Dif(m1, m2)$

The variables m1 and m2 represent the encrypted text before and after the change of the encryption key. E1, E2, and E3 are the encrypted texts obtained using various encryption keys (C, C + ΔC , and C - ΔC correspondingly). The variable Len represents the length of the ciphertext. Table 4 displays all the findings, which are all over 90%. Furthermore, these findings show a little rise when the size of the input bytes is enlarged. The suggested method demonstrates satisfactory key sensitivity in the key parameters, effectively resisting different cryptanalysis techniques.

Table 4 Presents the CDR findings for different byte sizes that were tested to various encryption keys.

Bytes number	2048	4096	8192	16384	32768	65536
Results of CDR	0.901	0.922	0.913	0.919	0.928	0.935

4.3 Differential attack analysis

Differential attack involves the intruder making little modifications to the original image and watching how the outcome changes. The purpose is to detect significant relationships between the original image and the encrypted image. To prevent such attacks, it is

necessary to use an encryption method that includes a mechanism wherein a slight alteration in the original image is reflected across the entire encrypted image. This behavior is exhibited in the proposed system since each pixel in the cipher text is influenced by both the relevant key stream element and the preceding pixel value. Additionally, we have used the two most often used metrics to measure the extent of change: the unified average changing intensity (UACI) and the number of pixels change rate (NPCR) [38, 39].

$$UACI = \frac{1}{W \times L} \sum_{m=0}^{W-1} \sum_{n=0}^{L-1} \frac{|E_1(m, n) - E_2(m, n)|}{255} \times 100\% \quad (6)$$

The cipher images produced from the proposed technique are denoted as E1 and E2.

$$NPCR = \frac{\sum_{m,n} D(m, n)}{W \times L} \times 100\%, \quad (7)$$

$$\text{Where: } D(m, n) = \begin{cases} 1, & \text{if } (E_1(m, n) \neq E_2(m, n)) \\ 0, & \text{if } (E_1(m, n) = E_2(m, n)) \end{cases}$$

The outcomes of the suggested method are shown in Table 5, where all UACI scores are near the theoretical normal levels (33.4635%) [40]. Additionally, the NPCR scores closely align with the expected normal values (99.5693%). Consequently, the suggested technique has successfully passed the UACI and NPCR tests. Therefore, the proposed technique offers an ample number of diffusion operations and is very resilient against differential attacks.

Table 5 Images evaluated using UACI and NPCR

Image (size=512×512)	UACI (%)	NPCR (%)
Parrot	34.3541	99.3143
Cameraman	34.3974	99.4209
Monarch	34.0758	99.3331
Baboon	34.0988	98.9714

4.4 Robustness analysis

Robustness assesses the proposed encryption system against several attacks that seek to undermine or alter the ciphertext. During the process of transferring via networks, encrypted images may experience harm. In order for an encryption technique to be considered resilient, it should be capable of restoring the original image even if some portions of the data have been destroyed. The Peak Signal-to-Noise Ratio (PSNR) quantifies the level of similarity between the decrypted and original images. For identical photos, this value is infinitely large. If the PSNR number approaches infinity, it indicates that the similarity between the two images is extremely great, while a low PSNR value implies a low similarity. The PSNR value is determined according to the equation (11) [41].

$$PSNR = 10 * \log \frac{255^2}{MSE} (dB) \quad (8)$$

The Mean Square Error (MSE) is a numerical number that represents the average squared difference between two images. The variable m represents the width of the image, while n represents the height of the image. The calculation is performed according to the Eq. (12) [42].

$$MSE = \frac{1}{m*n} \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} (I_O(j, k) - I_C(j, k))^2 \quad (9)$$

The original plain image is referred to as I_O , whereas the decrypted plain image is referred to as I_C , where PSNR is measured in dB. Above 35 dB is better in terms of image quality. Table 6 represents PSNR scores. The results were excellent because the proposed method did not have any compression or filtering processes. The proposed method showed better results over image quality evaluation. It was of higher performance.

Table 6 Images evaluated using PSNR

Image (size=512×512)	PSNR
Parrot	33.0993
Cameraman	34.5736
Monarch	32.3549
Baboon	32.0103

In addition, to improve the resistance of the proposed algorithm against side-channel attacks, the following countermeasures can be used. The proposed algorithm itself performs constant-time operations, thereby guaranteeing that execution time does not depend on secret inputs and thus mitigating any type of timing attack. Second, masking is applied at intermediate computations so that Power Analysis and Electromagnetic Emissions attacks can be less effective. Besides, after use, the temporary data must be erased from memory securely to avoid any chances of information leakage. These described measures minimize the probability of side-channel attack vectors while not reducing the effectiveness of the algorithm.

4.5 Comparative the results with other studies

This section evaluates the proposed encryption scheme against ten recent methods from the literature. The comparison focuses on essential security and performance metrics relevant to IoT applications. The results shows that our method achieves an exceptional balance among security strength and computational efficiency.

The security performance is excellent in a number of aspects (Table 7). The encrypted image entropy is 7.9994, and it almost attains its theoretical upper bound of 8. It is higher than the majority of other methods, which demonstrates a better randomness distribution in cipher images. The correlation coefficient of 0.00472 indicates almost complete eradication of pixel dependencies, and is much lower than previously reported values of up to 0.05990 obtained from other studied data paradigms.

We find the proposed system demonstrated its high ability to resilience the differential attacks, with NPCR and UACI of (98.671) and (34.098), respectively. Those values are within the recommended security range, thereby indicating higher sensitivity to input variations. Despite of some methods give slightly larger values, but our results guarantee that the gain against differential cryptanalysis is high enough for practical purposes.

Also, the keyspace of the proposed method is (2^{200000}), which significantly surpasses all compared designs and providing a robust defense against brute-force attacks. Additionally, it guarantees the long-lasting security requirement for sensitive IoT communication. The length of the keyspace came through the integration of chaotic system, dynamic DNA encoding systems but without compromising other security issues. Despite this high security level, the technique maintains practical performance, encrypting a (512×512) image in (1.4026) seconds. This processing rate is still competitive among our compared algorithms, and has much stronger security properties. For PSNR value (32.010), image conversion seems effective where enough distortion is added which does not allow an unauthorized person to infer the image contents and at the same time enables authorized decryption for data fidelity.

Performance measures demonstrate practical efficiency in resource-scarce environments. A more reasonable compromise while keeping the system secure at hand in terms of security features is the encryption time as equal to (1.4026) seconds for an image size of (512×512). This processing rate is still competitive among our compared algorithms, and has much stronger security properties. For PSNR value (32.010), image conversion seems effective where enough distortion is added which does not allow an unauthorized person to infer the image contents and at the same time enables authorized decryption for data fidelity.

The combination of Latin square operations and dynamic DNA coding forms multiple security protections to overcome the drawbacks of traditional technologies. By this architecture, their proposed SKC ROL transformer can achieve high entropy and low correlation together with large key space simultaneously. The slight overhead of processing time is totally acceptable for the large security advantages obtained, especially for medical IoT scenarios where data are most sensitive and thus deserve higher computational cost. Therefore, the performance comparison concludes that the proposed scheme is capable of providing advanced security mechanisms for challenging IoT networks. The approach shows a pronounced ability in forming unpredictable cipher images and still also being able to achieve reasonable encryption rates.

Table 7 Comparison among the values of the proposed algorithm and different schemes in literature

Ref.	Encrypted image entropy	Correlation coefficient	UACI (%)	NPCR (%)	PSNR	Encryption Time	Key size
Baboon (512×512) [19]	7.9754	0.00070	33.4224	99.5453	31.1496	-	2^{256}
Baboon (512×512) [20]	7.9993	0.01600	35.9229	99.5461	32.7000	1.4933	2^{448}
Baboon (512×512) [21]	7.9976	0.05990	33.62	99.6100	-	-	2^{792}
Baboon (512×512) [43]	7.9969	0.00060	33.4300	99.6100	-	0.798	2^{798}
Baboon (512×512) [22]	7.9969	0.00070	33.3539	99.5987	-	-	2^{256}
Baboon (512×512) [23]	7.9993	0.01910	33.4024	99.6048	30.1769	-	2^{498}
Baboon (512×512) [24]	7.9965	-	33.0704	99.6254	-	2.6371	2^{478}
Baboon (512×512) [25]	7.9993	-	33.4467	99.6084	-	-	2^{239}
Lena (256×256) [13]	7.9991	-	33.4646	99.6104	27.64	0.9556	2^{256}
Pepper (512×512) [15]	-	0.0002	33.483	99.682	-	0.403	2^{156}
Proposed method Baboon (512×512)	7.9994	-0.00472	34.098	98.671	32.010	1.4026	2^{200000}

5. Conclusions

In this work, a new image encryption scheme has been proposed based on integrates chaotic dynamics with biological computing principles through a three-stage cryptographic pipeline. The proposed method is a lightweight encryption system, with several additional measures for security, makes the algorithm suitable for good and efficient protection of sensitive image data. Chaotic maps guarantee unpredictability and randomness in the process of encryption, and thus, it is robust against most brute-force attacks. The proposed system shows negligible pixel correlation, uniform histograms, and high information entropy (over 7.9994). The key space was (2^{200000}) which ensures robust security. Moreover, the proposed system indicates high NPCR (over 98.671%), UACI (near theoretical levels), and CDR (over 90%) values. In addition, the proposed system demonstrated high PSNR (over 32.010) indicating good image quality. Finally, the encryption time of the system was fast (about 1.4026 seconds). Consequently, the statistical, key space, differential, and robustness analyses carried out in this paper have proved the efficiency of the method under study in terms of security features, efficiency, and immunity offered against common vulnerabilities. However, there are many future works, such as the authors exploring the idea of combining deep learning techniques with chaotic-based encryption to enhance security and efficiency. Also, developing scalable and secure image encryption solutions that can be deployed in cloud environments.

6. References

- [1] Mohammed RA, Khodher MAA, Alabaichi A. A novel lightweight image encryption scheme. *Comput Mater Contin.* 2023;75(1):2137-53.
- [2] Pirdawood MA, Kareem S, Al-Rassam O. Encryption of color images with a new framework. *ARO-the Sci J Koya Univ.* 2024;12(1):170-80.
- [3] Yang S, Long H. Socio cyber-physical system for cyber-attack detection in brand marketing communication network. *Wirel Pers Commun.* 2024;1-17.

- [4] Faraja ST, Jassima SA, Kifayatb K. Mediated IBC-based management system of identity and access in cloud computing. *Tikrit J Eng Sci.* 2014;21(2):1-9.
- [5] Ahn J, Hussain R, Kang K, Son J. Exploring encryption algorithms and network protocols: a comprehensive survey of threats and vulnerabilities. *IEEE Commun Surv Tutor.* 2025;27(6):3587-614.
- [6] Abd Al-Rahman SQ, Jassim SA, Sagheer AM. Design a mobile application for vehicles managing of a transportation issue. *Bull Electr Eng Inform.* 2021;10(4):2263-72.
- [7] Mohammed NS, Dawood OA, Sagheer AM, Nafea AA. Secure smart contract based on blockchain to prevent the non-repudiation phenomenon. *Baghdad Sci J.* 2024;21(1):23.
- [8] Vijayakumar M, Ahilan A. An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. *Ain Shams Eng J.* 2024;15(4):102620.
- [9] Suryawanshi AM, Tripathi DK. A comprehensive survey on lightweight cryptographic algorithms for IoT security. 2025;12(5):875-82.
- [10] Alawida M. Tree-feistel cipher standard for IoT communication system. *IEEE Internet Things J.* 2025;12(23):50961-77.
- [11] Mahalakshmi K, Nagarajan S. Comprehensive review and analysis of image encryption techniques. *IEEE Access.* 2025;13:109783-813.
- [12] Alawida M, Aljaghbeir AN, Albaz KR, Alnuaimi RA. DNA-Inspired image encryption: leveraging chaos for enhanced security. 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT); 2024 Apr 29-May 1; Abu Dhabi, United Arab Emirates. USA: IEEE; 2024. p. 477-82.
- [13] Lai Q, Hua H. Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Syst Appl.* 2025;264:125854.
- [14] Lai Q, Hu G. A nonuniform pixel split encryption scheme integrated with compressive sensing and its application in IoMT. *IEEE Trans Ind Inf.* 2024;20(9):11262-72.
- [15] Alawida M. A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments. *IEEE Trans Ind Inf.* 2024;20(8):10530-41.
- [16] Lai Q, Liu Y. A family of image encryption schemes based on hyperchaotic system and cellular automata neighborhood. *Sci China Technol Sci.* 2025;68(3):1320401.
- [17] Lai Q, Hua H, Yang L. Encryption design and analysis of 3-D medical models in internet of medical things using a novel memristive hyperchaotic map. *IEEE Internet Things J.* 2025;12(18):39019-28.
- [18] Lai Q, Yang L, Chen G. Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors. *IEEE Trans Ind Electron.* 2023;71(7):7819-28.
- [19] Abed QK, Al-Jawher WAM. A new multiple-chaos image encryption algorithm based on block compressive sensing, swin transformer, and wild horse optimization. *Multidiscip Sci J.* 2025;7(1):2025012.
- [20] Ahmad I, Shin S. A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. *Signal Process Image Commun.* 2021;98:116418.
- [21] Zhuang Z, Zhuang Z, Wang T. Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition. *Sci Rep.* 2024;14:402.
- [22] Abed QK, Al-Jawher WAM. Optimized color image encryption using arnold transform, URUK chaotic map and GWO algorithm. *J Port Sci Res.* 2024;7(3):219-36.
- [23] Hosny KM, Kamal ST, Darwish MM. Novel encryption for color images using fractional-order hyperchaotic system. *J Ambient Intell Hum Comput.* 2022;13:973-88.
- [24] Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color image encryption through chaos and KAA map. *IEEE Access.* 2023;11:11541-54.
- [25] Moya-Albor E, Romero-Arellano A, Brieva J, Gomez-Coronel SL. Color image encryption algorithm based on a chaotic model using the modular discrete derivative and Langton's ant. *Mathematics.* 2023;11(10):2396.
- [26] Mohi Ud Din S, Shah T, Alblehai F, Nooh S, Jamal SS. A combinatory approach of non-chain ring and henon map for image encryption application. *Sci Rep.* 2025;1:1781.
- [27] Akhlaq M, Mahfooz SZ. Integrating DDP to enhance cryptographic potential of latin squares through increased permutation diversity. 2025 8th International Conference on Data Science and Machine Learning Applications (CDMA); 2025 Feb 16-17; Riyadh, Saudi Arabia. USA: IEEE; 2025. p. 185-8.
- [28] Wang X, Dai X, Wang Y, Wang E. N-dimensional non-degenerate chaos based on singular value estimation with application in dynamic DNA image encryption. *Nonlinear Dyn.* 2025;113:7315-49.
- [29] Diwate P, Lavhale P, Pande CB, Sammen SS, Refadah SS, Khan MYA, et al. Evaluating flood dynamics and effects in Nagpur city using remote sensing and Shannon's entropy analysis. *Sci Rep.* 2025;15:4900.
- [30] Jassim SA, Farhan AK. Combined Chebyshev and logistic maps to generate pseudorandom number generator for internet of things. *Int J Electr Comput Eng.* 2022;12(3):3287-97.
- [31] INVICO (en). Image Dataset Watermarking [Internet]. 2025 [cited 2025 Nov 20]. Available from: <https://sites.google.com/up.edu.mx/invico-en/resources/image-dataset-watermarking>.
- [32] Acharya B, Venkata Sravan J, Janaki Potnuru DR, Abhimanyu Kumar Patro K. MIE-SPD: a new and highly efficient chaos-based multiple image encryption technique with synchronous permutation diffusion. *IEEE Access.* 2025;13:62773-97.
- [33] Li H, Tao Y, Xu T, Wang H, Yang M, Chen Y, et al. Real-time quantification of activated sludge concentration and viscosity through deep learning of microscopic images. *Environ Sci Ecotechnol.* 2025;24:100527.
- [34] Iqbal S, Wang J, Calgan H. Fractional chaotic dynamics in the rucklidge system and its application to image encryption. *Nonlinear Dyn.* 2025;113:26815-39.
- [35] Jassim SA. Enhancing S-box generation using african buffalo optimization algorithm techniques. *Int J Intell Eng Syst.* 2025;18(3):702-11.
- [36] Jassim SA, Jihad AA, Khalaf MI. Enhanced image encryption through combined arnold and three other chaos techniques. *J Cybersecur Inf Manag.* 2025;16(2):77-95.
- [37] Jing S, Guo Y, Chen W. Meaningful ciphertext encryption algorithm based on bit scrambling, discrete wavelet transform, and improved chaos. *IET Image Process.* 2021;15(5):1053-71.
- [38] Hoang TM. A novel structure of fast and efficient multiple image encryption. *Multimed Tools Appl.* 2024;83:12985-3028.

- [39] Abdelfatah RI, Elsobky RM, Khamis SA. Ultra-secure quantum protection for e-healthcare images: hybrid chaotic one-time pad with cipher chaining encryption framework. *J King Saud Univ Comput Info Sci.* 2025;37:158.
- [40] Wu Y, Noonan JP, Agaian S. NPCR and UACI randomness tests for image encryption. *Cyber J Multidiscip J Sci Technol.* 2011;1:31-8.
- [41] Martini MG. Measuring objective image and video quality: on the relationship between SSIM and PSNR for DCT-based compressed images. *IEEE Trans Instrum Meas.* 2025;74:5007813.
- [42] Nguyen ULP, Tonthat L, Dai Tran V, Luat Nguyen L. Pre-processing-based Walsh code with switched system in secure image steganography enhancement. *IEEE Access.* 2025;13:129284-95.
- [43] Qayyum A, Ahmad J, Boulila W, Rubaiee S, Arshad, Masood F. Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access.* 2020;8:140876-95.