A Hybrid Multi-Layered Joint Compression Encryption Scheme for RGB Images

Original Scientific Paper

Suha Abdul Raheem Khoja*
University of Baghdad,
College of Engineering, Department of Electronics and Communication
Jadriyah, Baghdad, Iraq
s.khoja@coeng.uobaghdad.edu.iq

Zainab Noori Ghanim
University of Baghdad,
College of Engineering, Department of Electronics and Communication
Jadriyah, Baghdad, Iraq
zainab.noori@coeng.uobaghdad.edu.iq

*Corresponding author

Abstract *– Robust security and bandwidth conservation are essential for digital image transmission in the modern digital era. In this study, a hybrid multi-layer joint lossy encryption-compression scheme for securing RGB colored images is proposed. In this scheme, 3D SPIHT (Set Partitioning in Hierarchical Trees) is used to exploit channel similarities that conventional 2D schemes miss by treating the color channels as a unified 3D data cube. Two joint stages are embedded in the 3D SPIHT. In the first stage, the 3D LL4 subband, obtained after 4 levels of DWT (discrete wavelet transform) decomposition, is followed by dynamic range optimization using the rooting companding transform, and then simultaneous diffusion and compression using the Chinese Remainder Theorem (CRT). In the second stage, a diverse scrambling strategy is applied to the four subband outputs of the first-level DWT decomposition, which are scrambled using 2D Henon, Arnold, Chirikov, and Logistic chaos systems. The 3D SPIHT stream output is then scrambled using a combination of DNA encoding and the 3D Lorenz system. Experimental results show a balance between security robustness and compression efficiency. The compressed file size is approximately 40% of the original, and the PSNR of the retrieved images exceeds 30 dB. The keyspace is significantly higher than the ideal value of 2^{100}, providing protection against brute-force attacks, while multistage diffusion protects against differential and statistical attacks.*

Keywords: *Chaotic Systems, CRT, DNA Coding, Joint Compression-Encryption, SPIHT*

Received: January 1, 2026; Received in revised form: May 4, 2026; Accepted: June 1, 2026

1. INTRODUCTION

In the current digital era, efficient and secure image transmission and storage are necessary for applications such as telemedicine, military communications, and industrial surveillance. RGB images are superior to grayscale images because of their higher information density and strong inter-pixel dependencies. RGB images generally require larger data sizes and exhibit high pixel redundancy [1].

While protecting the privacy and integrity of image data is critical, these security measures must be carefully reconciled with the bandwidth and storage constraints of modern transmission channels. Historically, customary paradigms have treated image encryption and compression as entirely decoupled processes. Set Partitioning in Hierarchical Trees (SPIHT) has been widely regarded as one of the most efficient and powerful image compression algorithms, owing to its very low computational requirements and outstanding compression performance [2]. Standard methods involve applying compression before or after encryption; each has its own weakness. In the former, subsequent encryption may increase the final size due to pixel expansion, whereas in the latter, compression efficiency is significantly reduced due to the high randomness of the encrypted data. Furthermore, a longer time is required to implement encryption and compression as separate processes. Joint image compression and encryption are promising methods for overcoming the drawbacks of standard methods. These methods implement encryption and compression simultaneously,

offering higher security and effective image transfer and storage [3]. Many joint image encryption and compression schemes have been proposed recently [4, 5].

The wide range of image security schemes includes selective image encryption and joint compression-and-encryption systems. [1] introduced an overview of color image encryption schemes that draw attention to the susceptibility of full-image encryption systems to statistical attacks. Selective encryption balances security and efficiency by encrypting only the most important parts of the image. [6-8] Demonstrated that robust security can be achieved by encrypting only the most significant bit stream components of the SPIHT. Various joint image encryption and compression schemes based on number theory and chaos-based systems have been proposed. In [9], a lossless image encryption and compression scheme is implemented using the CRT and a hash table. [10] Introduced a joint image compression and encryption scheme using a dynamical 2D hyper-chaotic discrete nonlinear system and CRT. [11] Suggests a hybrid image encryption-compression model that combines CRT with number theory. A recent trend in image encryption is the use of deoxyribonucleic acid (DNA) sequences, which offer special features and high parallelism. To achieve high security, many image encryption schemes have proposed combining DNA encoding with chaotic models [12-14]. [15] Suggest a combination of the quantum chaotic map and the DNA complementary rule to scramble the plain image, and then the CRT was used for simultaneous compression and diffusion of the scrambled image.

To aligned with the current research trend, [16] proposed a privacy protection scheme based on DCT compression and nonlinear dynamics, [17] designed an image encryption scheme that combines a 4D Hénon memristor map with convolution-based diffusion, providing an efficient system that is secure against plaintext attacks by linking the key to the image via SHA-256; [18] suggested hyperchaotic 3D Xin-She Yang maps for multi-layer encryption; and [19] introduced 3D S-boxes with Fibonacci Q-matrices to enhance resistance to brute force attacks.

Existing frameworks frequently fail to exploit inter-channel spectral correlations, which results in inefficient optimization of RGB images. Conventional 2D SPIHT-based joint schemes typically treat color channels as separate components. This results in constrained compression performance, which in turn compromises overall security.

To address the aforementioned issues, this work employs the 3D SPIHT algorithm, widely used for video compression, to jointly compress and encrypt RGB images. To effectively consolidate processing across all channels, the color space is modeled as a unified three-dimensional data cube. The proposed scheme exploits spatial-spectral redundancies that are conventionally ignored. The primary contributions of this work are summarized as follows.

1. The 3D-SPIHT algorithm is used to process RGB channels as a single volumetric cube, allowing the system to exploit spatial and spectral redundancies simultaneously.
2. A CRT-based fusion step is embedded directly into the compression cycle. To prevent data expansion, 3D pixels are first decomposed to lower their intensity values. This allows the CRT to securely merge the RGB channels and perform non-linear substitution without increasing the overall data size.
3. A hybrid chaotic system based on five distinct maps is formulated to enhance pixel decorrelation and ensure high sensitivity to initial conditions.
4. The proposed scheme achieves a compression ratio near 40% with minimal visual loss, alongside a key space exceeding 2^{100} for protection against brute-force attacks.
5. The stream output of the 3D SPIHT coder is diffused using a combination of a fifth chaotic system and DNA encoding.

The rest of this paper is organized as follows. Section 2 introduces the background study. A detailed description of the proposed scheme is presented in Section 3. Experimental results and performance analyses are discussed in Section 4. Finally, Section 5 presents the study's conclusions.

2. BACKGROUND STUDY

Developing the proposed integrated scheme starts with a few technical requirements. Data reduction is primarily handled by 3D SPIHT and the Root Companding Transform, while the Chinese Remainder Theorem, which serves as a bridge between compression and security, provides the necessary diffusion. The final protection comes from the DNA encoding and five chaotic maps that complete the encryption process.

2.1. SPIHT COMPRESSION

SPIHT is a wavelet-based compression algorithm that was proposed by Said and Pearlman [20]. The wavelet transform simultaneously provides sufficiently good time and frequency resolution, making SPIHT an efficient and powerful image analysis and compression algorithm [21]. When applying SPIHT to an image, the DWT [22] is first used to decompose the image into four sub-bands: LL, LH, HL, and HH. The LL subband, also known as the approximate subband, contains the most recognizable image information and is often used to recursively decompose the original image into a multi-level hierarchy. The LH subband contains the horizontal edge details, the HL subband includes the vertical edge details, the HH subband contains the diagonal details, and the resulting coefficients are then grouped into sets known as spatial orientation trees (SOT) [23].

The 3D SPIHT, proposed by Kim *et al*. [24], is an extended version of the SPIHT algorithm. The difference

between the two algorithms is that each node in the SOT of the SPIHT algorithm has four offspring forming a group of 2×2 adjacent pixels, except for the leaf nodes, which have no offspring, whereas in the spatial orientation tree of the 3D SPIHT, each node has eight offspring forming a group of 2×2×2 adjacent pixels [25]. The SOT structure of the 3D SPIHT defines the following partitioning sets of coordinates:

$O(i, j, k)$: set stores the coordinates of every offspring of node (i, j, k).

$D(i, j, k)$: set stores the coordinates of every descendant of node (i, j, k).

$H(i, j, k)$: set stores the coordinates of every root-level node.

$L(i, j, k) = D(i, j, k) - O(i, j, k)$.

A significance test was used to check the significance of the nodes corresponding to the coordinates in these partitioning sets. The formula for the significance test for a partitioning subset T is shown in Equation 1.

$$S_n(T) = \begin{cases} 1, if max(i,j,k) \in T \left| C_{(i,j,k)} \right| \geq 2^n \\ 0 \; otherwise \end{cases} \quad (1)$$

where $C(i, j, k)$ represents the coefficient at (i, j, k), which implies that if $Sn(T)=1$, then the coefficient set T is significant at the threshold $2n$. $n=\lfloor log_2 (max(i, j, k) \{|C(i, j, k)|\}) \rfloor$. The coordinates in the partitioning sets are then stored in three lists according to the significance test as follows:

The list of significant pixels (LSP) contains the coordinates of the identified significant coefficients.

The list of insignificant pixels (LIP) contains the coordinates of coefficients that have been identified as insignificant in the previous sorting pass.

The list of insignificant sets (LIS) contains entries that represent either set $D(i, j, k)$ or set $L(i, j, k)$.

The 3D SPIHT coding process, identical to the SPIHT process, involves the following steps.

(1) Initialization: Initialize the three lists as follows: LSP initially empty, LIP with all the coordinates of the root nodes stored in H, and LIS with all descendants of H.

(2) Sorting pass: The test function mentioned in 1 tests the significance of the coefficient coordinates stored in the LIP and LIS. If the coefficient is significant, it is moved to the LSP set; otherwise, it is moved to the end of the LIP or LIS sets. The test results were output as a binary code stream.

(3) Refinement pass. Transmits the nth most significant bit of the coefficients stored in the LIP, except those added in the last sorting pass.

(4) Update threshold. Decrement n by one and iterate the sorting and refinement passes until the termination condition is reached [23]. The 3D SPIHT algorithm has two termination conditions. First, the process stops as soon as the file size reaches the target compression limit. Second, the system halts naturally after completing the final n=0 bit-plane.

2.2. CHINESE REMINDER THEOREM

Let $m1, m2, m3, \ldots, mk$ be a set of k pairwise co-prime positive integers. If M_i^{-1} is the modular multiplicative inverse of an integer M_i mod m_i, then the equation $M_i M_i^{-1} \equiv 1 (\text{mod } m_i)$ is satisfied, where $i = 1, 2, 3, \ldots, k$. For any k integers $b_1, b_2, b_3, \ldots, b_k$, the system of simultaneous congruence $x = b_1 \text{ mod } m_1$, $x = b_2 \text{ mod } m_2$, $\ldots$, $x = b_k \text{ mod } m_k$ has a unique solution modulo $m=m_1 m_2 m_3 \ldots m_k$ which is given by $x \equiv M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 + \ldots + M_k M_k^{-1} b_k (\text{mod } m)$ [26]. In decoding, the individual pixel value b can be recovered from x using congruence $b_i = x \text{ mod } m_i$, where $i = 1, 2, 3, \ldots, k$ [27]. The number of pixels k is regarded as the compression ratio of the CRT [26].

2.3. DNA SEQUENCE CODING RULES AND OPERATIONS

The molecular structure of Deoxyribonucleic Acid (DNA) comprises four nucleic acid bases: adenine, thymine, cytosine, and guanine, abbreviated as (A), (T), (C), and (G), respectively. There is a complementary relationship between these four DNA bases, where C and G complement each other, and A and T complement each other. DNA bases are usually represented by two binary digits since, in the binary system, 0 and 1 are complementary, and 00 and 11 are complementary. Likewise, 01 and 10, and therefore 00, 01, 10, and 11, can be set to the four DNA bases in any combination. Accordingly, there were 4! encoding rules. Table 1 shows the eight allowable rules, which are the standard mappings among these 24 encoding rules that follow the Watson-Crick complement rule.

The DNA encoding addition, subtraction, and XOR operations are identical to ordinary binary addition, subtraction, and XOR operations. Analogous to the eight DNA-encoding rules, each DNA-encoding operation has eight types. The DNA XOR operation based on rule 1 is listed in Table 2 [28-30].

Rule 1 is chosen in the proposed work because it is faster than the other seven rules. Also, a single fixed rule prevents heavy computation delays. This choice ensures very fast execution across the entire system.

Table 1. DNA encoding rules

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

Table 2. DNA XOR operation

⊕	A	T	G	C
A	A	T	G	C
T	T	A	C	G
G	G	C	A	T
C	C	G	T	A

2.4. ROOTING COMPANDING TRANSFORM (RCT)

Rooting Companding Transform is a nonlinear companding technique equivalent to the standard square-root technique. It is a distortion-reduction technique primarily used for speech signals that increases the average signal power by compressing large signal amplitudes while expanding small ones. The formula of the Rooting Companding Transform is shown in Equation 2.

$$f(x) = |x|^R * sgn(x) \quad (2)$$

where $sgn(x)$ stands for $sign(x)$, which is used to maintain the phases of the signal, R specifies the amount of companding and ranges from 0.1 to 0.9 [31, 32].

2.5. CHAOTIC SYSTEMS

Chaotic maps are nonlinear functions widely used for image ciphering because of their sensitivity to initial conditions and parameters; a small change in any parameter or initial value can produce significantly different random iterates [33, 34]. This study uses five different chaotic maps: the logistic map, the Henon map, the Chirikov standard map, the Arnold cat map, and the 3D Lorenz system.

2.5.1. Logistic Map

The mathematical formula for the Logistic map is given in Equation 3.

$$x_{n+1} = rx_n(1 - x_n) \quad (3)$$

where $x_n \in (0,1)$ denotes the state value after n iterations, x_{n+1} denotes the value of the next iteration of x_n, and when the control parameter $r \in [3.57,4]$ the logistic map exhibits chaotic behavior [33, 35].

2.5.2. Arnold Map

The two-dimensional Arnold cat map can be mathematically described by Equation 4.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod(N) \quad (4)$$

where N represents the side length of the image, and c and d are two positive integers [36, 37].

2.5.3. 2D Henon System

The Hénon map is a two-dimensional discrete-time dynamical system defined by Equation 5.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (5)$$

where, x and $y \in [0,1]$ represent the chaotic state over n iterations, where a and b are control parameters. The chaotic behavior increases when a=1.4 and b=0.3, as shown in standard empirical tests [38, 39].

2.5.4. Chirikov Standard Map

The Chirikov system is appropriate for two-dimensional image applications, where its values are regularly generated in the two-dimensional space $[0,2\pi] \times [0,2\pi]$, see Equation 6.

$$\begin{cases} (x_n, y_n) \leftrightarrow (x_{n+1}, y_{n+1}), \\ x_{n+1} = x_n + k.\sin y_n \; mod \; 2\pi \\ y_{n+1} = y_n + x_{n+1} \; mod \; 2\pi \end{cases} \quad (6)$$

where k indicates the control parameter and (x_n, y_n) is the iterated state vector. The Chirikov system attains a good distribution when k >5 and becomes increasingly regular at $[0,2\pi]^2$ [14, 40].

2.5.5. 3D Lorenz System

Lorenz is a dynamical system that is described by the following system of ordinary differential equations; see Equation 7.

$$\begin{cases} \dot{u} = \alpha(v - u) \\ \dot{v} = \beta u - \beta w - v \\ \dot{w} = uv - \gamma w \end{cases} \quad (7)$$

where u, v, and w are three real status variables, while, β, and γ are three real positive control parameters. When α =10, γ=8/3, and β=28, the Lorenz system exhibits chaotic behavior [41-43].

3. PROPOSED WORK

The proposed scheme, shown in Fig. 1 and illustrated in pseudo code 1, is explained in the following steps:

1. A colored image of size $M \times N \times 3$ is passed into the first step of 3D SPIHT compression, in which the original image, namely I, is transformed into a wavelet coefficient matrix, namely WI, by applying four-level Bior4.4 of 2D DWT. Fig. 1 only shows the LL4 subband of the four-level 2D DWT.
2. The root companding technique is applied on the WI to balance the signal amplitude, thus preventing data loss during compression where, the pixel intensity values are decreased, so the C matrix with small intensity values is obtained, then each 3D pixel intensity value in the 3D LL4 is converted to a 16-bit binary number A, and the pixel A is then divided into three pixels: P_1 (8 bits size), P_2 (4 bits size), and P_3 (4 bits size), which obtains three 3D matrices with the same size as LL4 namely PM_1, PM_2, and PM_3, where PM_1 is filled with P_1 type pixels (8 bits per pixel), PM_2 is filled with P_2 type pixels (4 bits per pixel), and PM_3 is filled with P_3 type pixels (4 bits per pixel). CRT is then implemented on the three matrices in a pixel-wise manner, where the first pixels of the red, green, and blue layers of PM_1 are the first three entries to CRT, the second pixels of the red, green, and blue layers of PM_1 are the second three entries to CRT, and so on. Because CRT is a compression technique, the red, green, and blue layers of PM_1, PM_2, and PM_3 matrices pixels yielded one pixel output of CRT, thus, three new 2D matrices, namely PMO_1, PMO_2, and PMO_3 with the same size as LL4 were obtained, and the three new 2D matrices replaced LL4 in the 3D transformed image, where PMO_1 replaced the red layer of LL4, PMO_2 replaced the green layer of LL4, and PMO_3 replace the blue layer of LL4, consequently, LL4 is encrypted using CRT.

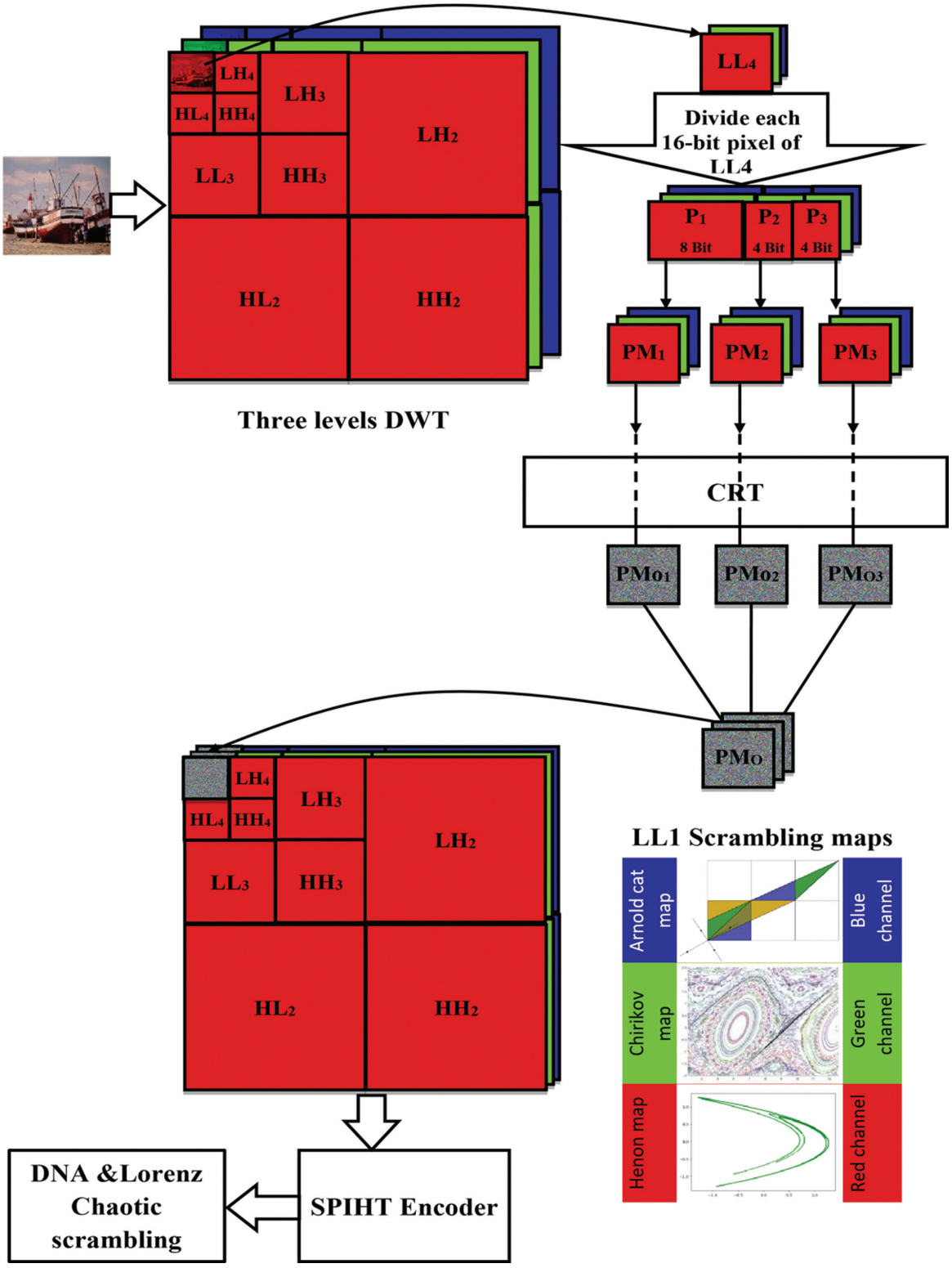


Fig. 1. The proposed multilayered scheme, depicting the integration of LL4 diffusion steps with CRT, the 3 chaotic maps scrambling of LL1, and DNA-Lorenz encryption.

3. Scrambling using chaotic systems is implemented in this step to the four subbands obtained from the first level decomposition of the 3D transformed image, as follows:

a. Row - and column-wise pixel scrambling using three different 2D chaotic maps is implemented on each color channel of the LL1 subband to break the inter-channel correlation more effectively than a single chaotic map, where the Henon chaotic map is applied to the red layer, the Chirikov standard map is applied to the green layer, and the Arnold cat map is applied to the blue layer. The three chaotic maps were arranged in ascending order, and their intensity values were used as an index to scramble the rows and columns of the LL1 subband.

b. Block scrambling shown in Fig. 2 is implemented on the other three subbands, where each of the 3D LH1, HL1, and HH1 is divided into blocks, namely B_{ijk} with size 8×8, where i and j specify the row and column numbers of each block, respectively, where i=1,…, M/ (2×8) and j=1,…, N/ (2×8), and k is the channel color number. Then, the B_{ijk} blocks of the red, green, and blue layers of each sub-band are converted to a sequence of consecutive blocks, namely B_b with length $M/(2\times8) \times N/(2\times8)\times3$, where b=1,.., n, here n is the number of blocks that equal to $i\times j\times k$, following a logistic map with varying constant values r, for the red, green, and blue layers is used to generate three 1D arrays L_r, L_b and L_g, the pseudo random numbers of the three arrays are used as an index to scramble the B_b blocks to obtain an array namely NewB with same length as B_b. Next, each of the three scrambled sequences in each sub-band is converted to a matrix in the form of B_{ijk} consequently, three 3D matrices were obtained; these matrices represent the NewC of the 3D scrambled LL1, LH1, HL1, and HH1, Fig. 2 shows block scrambling of 16 ×16 subband example.

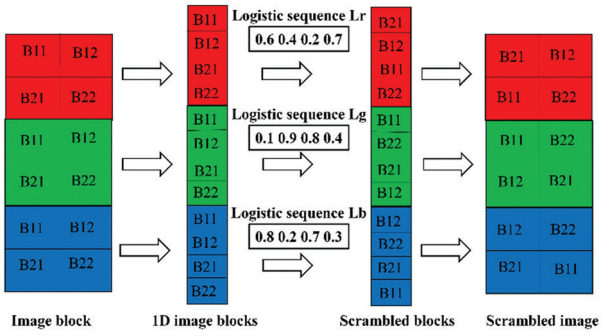


Fig. 2. First level 2D DWT LH1, HL1, and HH1 subbands block scrambling

4. An additional layer of security is implemented on NewC using a 3D Lorenz map and DNA encoding. After the 3D SPIHT sorting and refinement passes, the scrambled 3D-transformed image encoded bitstream output sequence BS is converted to a decimal sequence, namely PS, of length PL. On the other hand, iterate equation 7 for PL/3 times to obtain the PL size pseudo-number sequence. Equation 8 is used in each iteration to quantize the Lorenz system outputs u, v, and w.

$$\begin{cases} e = \lfloor(|u| - \lfloor|u|\rfloor) \times 10^7\rfloor \, mod \, 256 \\ f = \lfloor(|v| - \lfloor|v|\rfloor) \times 10^7\rfloor mod \, 256 \\ g = \lfloor(|w| - \lfloor|w|\rfloor) \times 10^7\rfloor \, mod \, 256 \end{cases} \quad (8)$$

where e, f, and g range from 0 to 255. After all iterations, the sequence:

$$[e_1, f_1, g_1, e_2, f_2, g_2, \cdots, e_n, f_n, g_n]$$

is obtained as KS output, where n represents the number of iterations. The KS is used as an index to scramble the PS sequence after converting each decimal value to binary, yielding the binary sequence SS. Next, the SS sequence is encoded according to rule 1 in Table 1 to obtain the DNA sequence DS. Rule 1 is also used to encode the KS sequence after it is converted to binary, yielding the DNA sequence DK. The resulting two DNA sequences are encrypted using the DNA XOR operation mentioned in Table 2 to obtain the encrypted DNA sequence DF. Finally, the DF sequence is transmitted to the receiver. The decoding process of the proposed scheme is the same as the encoding process, except that the operations are reversed.

The proposed scheme's efficiency stems from the 2D DWT and 3D SPIHT stages. These core components dominate the execution time. Both 2D DWT and 3D SPIHT have established complexities of $O(N)$ and $O(N\ log\ N)$, where N denotes the total number of pixels. The overall system complexity remains $O(N\ log\ N)$, making the performance comparable to the JPEG standard. Integrated encryption layers do not create a computational bottleneck. Specifically, choosing Rule 1 keeps the DNA step fast. Using all eight DNA rules just spends CPU time. This single rule prevents any heavy computation lags. Meanwhile, the 3D Lorenz map handles the core security work. For this reason, the whole system runs fast and supports high-speed communication.

Pseudo-code 1

Input: the original RGB image I (i, j, P), where i and j are row and column numbers, and P is the channel color.

Output: The DNA sequence DF

Step1: Implement 4 levels of 2D DWT on I

3D WI ← Implement 2D DWT on each layer of the RGB Image I

Step 2: Implement the Chinese Remainder Theorem

C ← Root Companding(WI)

A ← Convert each 3D decimal pixel of C(LL4(i, j, P)) to 16-bit binary

$P_1(i, j, P)$ ← A(1:8)

$P_2(i, j, P)$ ← A(9:12)

$P_3(i, j, P)$ ← A(13:16)

$PM_1(i, j, P)$ ← binary to decimal $P_1(i, j, P)$

$PM_2(i, j, P)$ ← binary to decimal $P_2(i, j, P)$ pixels

$PM_3(i, j, P)$ ← binary to decimal $P_3(i, j, P)$ pixels

$PMO_1(i, j)$ ← $CRT\,(PM_1(i, j, red), PM_1(i, j, green), PM_1(i, j, blue))$

$PMO_2(i,j)$ ← $CRT\,(PM_2(i, j, red), PM_2(i, j, green), PM_2(i, j, blue))$

$PMO_3(i,j)$ ← $CRT\,(PM_3(i, j, red), PM_3(i, j, green), PM_3(i, j, blue))$

$NewLL4\,(i, j, red) \leftarrow PMO_1(i, j)$

$NewLL4\,(i, j, green) \leftarrow PMO_2(i, j)$

$NewLL4\ (i, j, blue) \leftarrow PMO_3(i, j)$

$C(LL4) \leftarrow NewLL4$

Step 3: Implement Scrambling

a. $NewC\ (LL1, Red) \leftarrow$ Row Column Scrambling using Henon map ($C\ (LL1(i, j, Red))$)

b. $NewC\ (LL1, Green) \leftarrow$ Row Column Scrambling u-sing Chirikov map ($C\ (LL1(i, j, Green))$

$NewC\ (LL1, Blue) \leftarrow$ Row Column Scrambling using Arnold map ($C\ (LL1(i, j, Blue))$

c. **For** $P \leftarrow 1$ to 3

$B\ (1{:}8,1{:}8,1{:}n) \leftarrow C\ (LH1(i, j, P))$

$NewB\ (1{:}8,1{:}8,1{:}n/3) \leftarrow B(Lr)$.

$NewB\ (1{:}8,1{:}8,(n/3)+1{:}2n/3) \leftarrow B(Lg)$.

$NewB\ (1{:}8,1{:}8,(2n/3)+1{:}n) \leftarrow B(Lb)$.

$NewC\ (LH1(i, j, P)) \leftarrow NewB\ (1{:}8,1{:}8,1{:}n)$

End For

For $P \leftarrow 1$ to 3

$B\ (1{:}8,1{:}8,1{:}n) \leftarrow C\ (HL1(i, j, P))$

$NewB\ (1{:}8,1{:}8,1{:}n/3) \leftarrow B(Lr)$.

$NewB\ (1{:}8,1{:}8,(n/3)+1{:}2n/3) \leftarrow B(Lg)$.

$NewB\ (1{:}8,1{:}8,(2n/3)+1{:}n) \leftarrow B(Lb)$.

$NewC\ (HL1(i, j, P)) \leftarrow NewB\ (1{:}8,1{:}8,1{:}n)$

End For

For $P \leftarrow 1$ to 3

$B\ (1{:}8,1{:}8,1{:}n) \leftarrow C\ (HH1(i, j, P))$

$NewB\ (1{:}8,1{:}8,1{:}n/3) \leftarrow B(Lr)$.

$NewB\ (1{:}8,1{:}8,(n/3)+1{:}2n/3) \leftarrow B(Lg)$.

$NewB\ (1{:}8,1{:}8,(2n/3)+1{:}n) \leftarrow B(Lb)$.

$NewC\ (HH1(i, j, P)) \leftarrow NewB\ (1{:}8,1{:}8,1{:}n)$

End For

Step 4: Implement 3D SPIHT sorting and refinement passes on NewC

Step 5: Implement DNA encoding

$PS \leftarrow$ Binary to decimal (BS)

$SS \leftarrow$ Decimal to binary ($PS(KS)$)

$DS \leftarrow$ Apply rule 1 on SS

$DK \leftarrow$ Apply rule 1 on decimal to binary (KS)

$DF \leftarrow$ DNA-XOR (DS,DK)

4. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATIONS

The proposed scheme was evaluated on seven standard color images of 256 ×256 pixels. The images are entitled Lena, Peppers, House, Baboon, Airplane, Barbara, and Boats. The initial values X_0=0.3 and Y_0=0.3 are selected for the Henon, Chirikov, Arnold cat, and logistic maps; the Lorenz map initial values are X_0=0.12, Y_0=0.23, and Z_0=0.34. The parameters used in the proposed scheme are a=1.4 and b=0.3 in the Hénon map, and c=2 and d=3 in the Arnold cat map. α =10, γ =8/3, and β =28 in the Lorenz map, k is set to 8 in the Chirikov map. In the logistic map, selecting the different r values 4, 3.8, and 3.9 yields distinct, independent chaotic paths for each encryption layer. The three integers used in the CRT are 17, 18, and 19 because they are pairwise coprime, yielding highly efficient, small pixel intensity values while remaining appropriately scaled for the 4-bit, 4-bit, and 8-bit partitions of the 16-bit pixel.

4.1. STATISTICAL ATTACK ANALYSIS

A cipher is only as strong as the absence of its own footprints. If an encrypted image can retain its original RGB structure, the system essentially falls apart. This logic guides the upcoming tests, which use a histogram to evaluate pixel distribution and use correlation analysis to predict spatial patterns. Finally, it evaluates information entropy to ensure that no statistical ghost of the original data is sustained.

4.1.1. Histogram

A histogram is an important criterion for evaluating the security of an image encryption algorithm, as it shows the distribution of pixel intensities by depicting the number of pixels at each intensity level. The robust encryption algorithm should alter the distribution of the original image's pixels so that the ciphered image's histogram is significantly different from the original's. Fig. 3 shows the original image of boats with its red, green, and blue component histograms. Fig. 4 shows the ciphered image of boats with its red, green, and blue component histograms. As shown in the two figures, the histograms of the ciphered image are fairly flat and significantly different from those of the original image, indicating the impenetrability of the proposed scheme against statistical attacks.

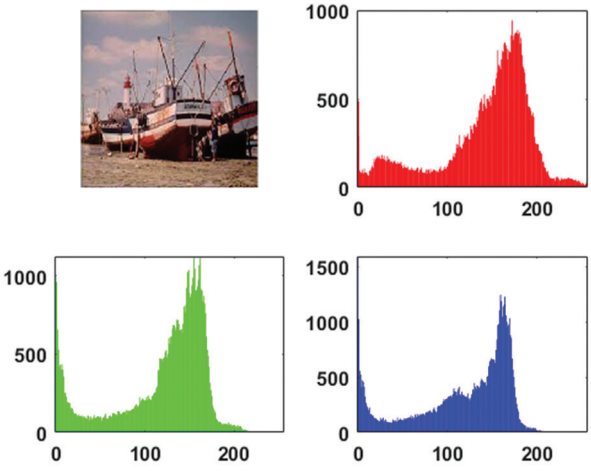


Fig. 3. The original image's red, green, and blue component histograms show the non-uniform distribution of the image

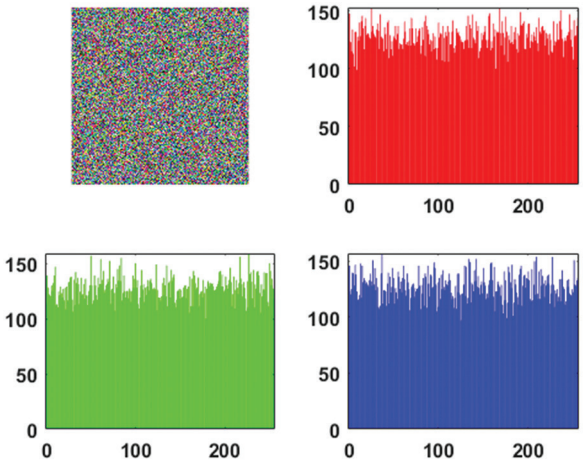


Fig. 4. The histograms of the ciphered image's red, green, and blue components show a fairly flat distribution

4.1.2. Correlation Analysis

Naturally, image pixels are highly correlated, which gives attackers a chance to recover the original image by analyzing pixel relationships in the encrypted image. Therefore, a strong cryptosystem should reduce the correlation between adjacent pixels in the image.

To measure the correlation between two adjacent image pixels in horizontal, vertical, and diagonal directions, pick 10000 random pairs of adjacent pixels, then measure the correlation between each pair using the formula of Equation 9.

$$C_{xy} = \sum_{xy} \frac{(x-\mu_x)(y-\mu_y)p(x,y)}{\sigma_x \sigma_y} \quad (9)$$

where $p(x, y)$ represents the pixel value at the position (x, y), μ and σ represent the mean and the standard deviation, respectively. The range of correlation coefficient values is from -1.0 to 1.0, where 1.0 indicates a positive correlation (both pixel values move in the same direction) and -1.0 indicates a negative correlation (the values move in opposite directions). In contrast, the ideal correlation must be close to or equal to zero. [44, 45]. The correlation coefficients of the red, green, and blue channels for the original and encrypted test images in vertical, horizontal, and diagonal directions are listed in Table 3, and the visual representation of the correlation distribution of boats image is shown in Figs. 5, 6 and 7, it is evident from the figures and table that the proposed scheme efficiently destroys the correlation between the adjacent pixels and approximately achieves the ideal zero. Table 4 shows that the correlation distribution of the proposed scheme is comparable to those in [46-51].

Table 3. The statistical evaluation of correlation coefficients for the original and encrypted test images demonstrates a shift from high pixel correlations to near-zero correlations in the encrypted images

Image		Vertical Corr.		Horizontal Corr.		Diagonal Corr.	
		Original Image	Encrypted Image ↓	Original Image	Encrypted Image ↓	Original Image	Encrypted Image ↓
peppers	R	0.9613	-0.0041	0.9406	-0.0106	0.9056	0.0014
	G	0.9825	-0.0038	0.9680	-0.0060	0.9442	-0.0031
	B	0.9523	-0.0073	0.9322	0.0026	0.8909	-0.0032
House	R	0.9024	0.0058	0.9583	-0.0193	0.9199	-0.0110
	G	0.8970	0.0035	0.9867	0.0042	0.8646	-0.0081
	B	0.9854	0.0019	0.9872	-0.0135	0.9761	0.0117
Baboon	R	0.9673	0.0119	0.9442	0.0084	0.9134	0.0006
	G	0.9642	-0.0029	0.9332	0.0057	0.8878	0.0090
	B	0.9760	-0.0148	0.9472	-0.0043	0.9248	0.0028
Airplane	R	0.9057	-0.0041	0.9479	0.0017	0.8344	-0.0111
	G	0.9300	0.0031	0.9248	0.0067	0.8782	0.0017
	B	0.9247	0.0112	0.9554	-0.0114	0.8973	0.0032
Barbara	R	0.9419	0.0067	0.9500	-0.0024	0.8938	0.0009
	G	0.9379	0.0023	0.9449	-0.0118	0.8790	-0.0219
	B	0.9502	-0.0064	0.9561	0.0088	0.8977	-0.0058
Boats	R	0.9522	-0.0016	0.8261	0.0020	0.7902	-0.0011
	G	0.9473	-0.0008	0.7726	-0.0050	0.7489	0.0057
	B	0.9517	-0.0037	0.7749	0.0026	0.7548	-0.0023

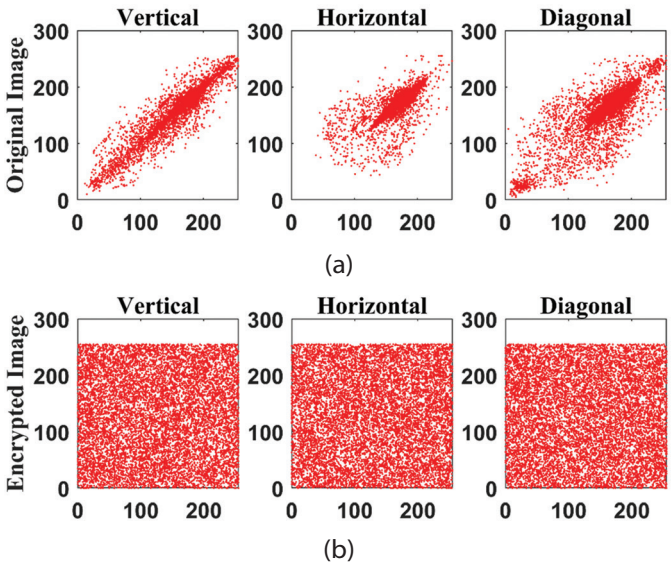


Fig. 5. The red channel pixel correlation distribution of boats image (**a**) original image and (**b**) encrypted image

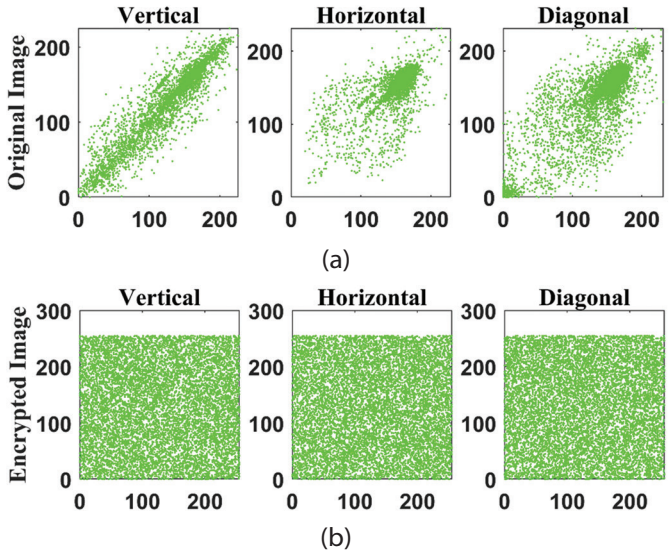


Fig. 6. The green channel pixel correlation distribution of boats image (**a**) original image and (**b**) encrypted image

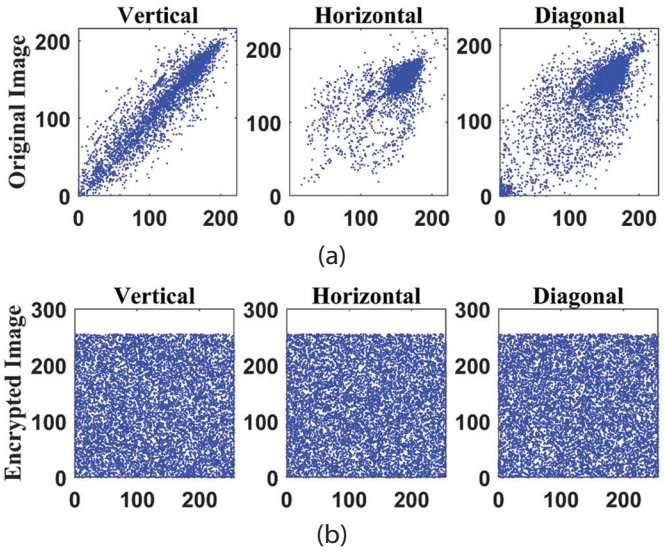


Fig. 7. The blue channel pixel correlation distribution of boats image(**a**) original image and (**b**) encrypted image

Table 4. Comparative evaluation of the proposed scheme correlation distribution results with the related schemes

Scheme	Image		Vertical Corr.		Horizontal Corr.		Diagonal Corr.	
			Original Image	Encrypted Image↓	Original Image	Encrypted Image↓	Original Image	Encrypted Image↓
Proposed	Lena	R	0.9550	0.0026	0.9482	0.0058	0.9083	-0.0019
		G	0.9377	0.0084	0.9550	0.0207	0.9276	-0.0073
		B	0.8851	-0.0176	0.9517	0.0126	0.9255	-0.0139
Ref [48]	Lena		0.9682	–0.0049	0.9852	–0.0062	0.9593	0.0029
Proposed	peppers	R	0.9613	-0.0041	0.9406	-0.0106	0.9056	0.0014
		G	0.9825	-0.0038	0.9680	-0.0060	0.9442	-0.0031
		B	0.9523	-0.0073	0.9322	0.0026	0.8909	-0.0032
Ref [47]	peppers		0.9667	0.0003	0.9594	-0.0032	0.9304	-0.0056
Ref [49]	peppers		0.0104	-0.0001	0.0109	0.0000	0.0151	0.0000
Ref [51]	peppers	R	0.9660	0.0006	0.9499	-0.0002	0.9008	0.0000
		G	0.9759	-0.0005	0.9585	0.0008	0.9467	0.0007
		B	0.9644	0.0003	0.9412	0.0006	0.9117	-0.0008
Proposed	Baboon	R	0.9673	0.0119	0.9442	0.0084	0.9134	0.0006
		G	0.9642	-0.0029	0.9332	0.0057	0.8878	0.0090
		B	0.9760	-0.0148	0.9472	-0.0043	0.9248	0.0028
Ref [46]	Baboon		0.8750	0.0131	0.8244	–0.0030	0.7873	0.0072
Ref [50]	Baboon		0.8248	0.0032	0..8776	0.0005	0.7725	0.0052

Table 5. The entropy values of the original and encrypted test images indicate a near-ideal random distribution

Image		Entropy of original image	Entropy of encrypted image↑
peppers	R	7.3876	7.9926
	G	7.6664	7.9931
	B	7.1978	7.9931
House	R	6.4311	7.9946
	G	6.5389	7.9933
	B	6.2320	7.9943
Baboon	R	6.2302	7.9936
	G	6.0732	7.9945
	B	6.3344	7.9927
Airplane	R	6.7254	7.9932
	G	6.8253	7.9937
	B	6.2078	7.9925
Barbara	R	7.5518	7.9925
	G	7.3756	7.9938
	B	7.4773	7.9927
Boats	R	7.4721	7.9941
	G	7.1429	7.9938
	B	7.1806	7.9928

Table 6. Compares the entropy values with related schemes, validating the randomness of the proposed scheme

Scheme	Image		Entropy of the original image	Entropy of the encrypted image↑
Proposed	Lena	R	7.5549	7.9938
		G	7.0167	7.9938
		B	6.7347	7.9939
Ref [48]	Lena		7.4456	7.9994
Proposed	peppers	R	7.3876	7.9926
		G	7.6664	7.9931
		B	7.1978	7.9931
Ref [47]	peppers		7.1903	7.9987
Ref [49]	peppers		4.7196	7.9984
Proposed	Baboon	R	6.2302	7.9936
		G	6.0732	7.9945
		B	6.3344	7.9927
Ref [46]	Baboon		7.0092	7.9973
Ref [50]	Baboon		7.2288	7.9976

4.1.3. Information Entropy

Shannon entropy is used to evaluate the unpredictability and randomness of the encrypted image, as given in Equation 10.

$$H(x) = \sum_{i=0}^{N} Q(x_i) log_2 \frac{1}{Q(x_i)} \quad (10)$$

where $Q(x_i)$ represents the probability of the occurrence of x_i, N represents the total number of x_i. The ideal entropy value for an image with 256 intensity levels is 8 [52]. The information entropy of the proposed scheme test images is listed in Table 5. It can be noted from the table that the red, green, and blue channel entropy values of all test images are very close to 8 and on par with those of references [46-50] as tabulated in Table 6. Therefore, the proposed scheme exhibits high randomness, making it immune to information entropy attacks.

4.2. DIFFERENTIAL ATTACK ANALYSIS

In differential attacks, the cryptanalyst usually seeks to identify the relationship between the original and encrypted images. This is done by slightly altering the original image and then encrypting it with the proposed algorithm. After that, they compare the encrypted image without alternation and the encrypted image with alternation. To assess the image encryption algorithm's resistance to differential attacks, the Number of Pixel Change Rate (NPCR) and the Unified Average Change in Intensity (UACI) are used; these two criteria are measured using Equations 11, 12, and 13.

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (11)$$

$$NPCR = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100\% \quad (12)$$

$$UACI = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255 \times M \times N} \times 100\% \quad (13)$$

where C_1 is the encrypted image, and C_2 is the encrypted image after changing one pixel in the original image. M and N represent the width and height of the image, respectively [53].

The $NPCR$ and $UACI$ values of the proposed scheme are tabulated in Tables 7 and 8, respectively. It can be seen from the two tables that the $NPCR$ and $UACI$ values of the proposed scheme are close to the ideal values as those of schemes in references [46-51], as shown in Tables 9 and 10, this indicates that the proposed scheme can resist differential attacks. The ablation study results presented in Table 11 clearly illustrate the individual contributions of the DNA encoding and CRT stages. It is evident from the data that, without DNA encoding, the UACI values drop sharply to nearly 0.1%, indicating that the DNA layer is the primary driver of diffusion and sensitivity in the proposed scheme. Furthermore, removing the CRT component reduces UACI by about 2%, indicating that CRT not only aids bit-level compression but also provides an additional security layer. These results confirm that every part of the proposed multi-layered architecture is vital for maintaining high resistance against differential attacks.

Table 7. The NPCR values of the test images demonstrate the proposed scheme's efficient, near-ideal diffusion against differential attacks

Image	NPCR↑		
	R	G	B
peppers	99.6795	99.5943	99.6470
House	99.6136	99.5965	99.6375
Baboon	99.6307	99.6033	99.6820
Airplane	99.6849	99.5308	99.5939
Barbara	99.6079	99.6417	99.6214
Boats	99.6032	99.5748	99.5642

Table 8. The UACI values of the test images illustrate the optimal intensity distribution of the proposed scheme

Image	UACI↑		
	R	G	B
peppers	33.5651	33.4159	33.5392
House	33.3434	33.4347	33.4148
Baboon	33.1944	33.3249	33.7031
Airplane	33.4011	33.5735	33.4489
Barbara	33.5597	33.4372	33.5087
Boats	33.7141	33.4472	33.4164

Table 9. Comparative evaluation of the NPCR values with related schemes, showing the high sensitivity of the proposed scheme to negligible plaintext variations

Scheme	image	NPCR↑		
		R	G	B
Proposed	Lena	99.5951	99.6016	99.6604
Ref [48]	Lena		99.5995	
Proposed	peppers	99.6795	99.5943	99.6470
Ref [47]	peppers		99.6068	
Ref [49]	peppers		99.6078	
Ref [51]	peppers	99.345	9.453	99.234
Proposed	Baboon	99.6307	99.6033	99.6820
Ref [46]	Baboon		99.6521	
Ref [50]	Baboon		99.6109	

Table 10. The comparison of UACI values with related schemes verifies the proposed scheme's outstanding intensity diffusion effectiveness

Scheme	Image	UACI↑		
		R	G	B
Proposed	Lena	33.6028	33.6848	33.1884
Ref [48]	Lena		33.45	
Proposed	peppers	33.5651	33.4159	33.5392
Ref [47]	peppers		32.0919	
Ref [49]	peppers		33.4774	
Ref [51]	peppers	33.453	33.345	33.321
Proposed	Baboon	33.1944	33.3249	33.7031
Ref [46]	Baboon		33.6032	
Ref [50]	Baboon		33.5337	

Table 11. Contribution analysis of CRT and DNA-Lorenz stages to UACI performance, validating the combined effect of the proposed multi-layered scheme in achieving optimal intensity diffusion limits

Image	Test type		UACI↑
Lena	Without DNA	R	0.1303
		G	0.1935
		B	0.1376
Lena	Without CRT	R	31.7454
		G	31.8377
		B	31.8841
Lena	With CRT and DNA	R	33.6028
		G	33.6848
		B	33.1884

4.3. KEYSPACE ANALYSIS

An efficient encryption system should have a large keyspace to resist violent attacks. The keyspace of the proposed scheme comprises the initial values and parameters are real numbers with significant digits reachs to 10^{-15}, Henon map initial values (X_0 and Y_0) and the parameters (a and b) are four real numbers, this yields the keyspace is $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{60}$, Chirikov map initial values (X_0 and Y_0), and the parameter k, now the keyspace is 10^{45}, Arnold cat map initial values (X_0 and Y_0) and the parameters (c and d), here the keyspace is 10^{60}, the keyspace obtained from applying Logistic map three times with the initial value X_0 and the parameter r is 10^{90}, the keyspace of CRT is 3×255 which is obtained from three prime numbers, 8 DNA rules together with the Lorenz map initial values (X_0, Y_0, and Z_0), and the parameters (α, β, and γ), this yields a keyspace 8×10^{90}, considering that the calculation precision is 10^{-15}, gets a total DNA and Lorenz keyspace 2^{302}. As a result, the key space of the proposed scheme exceeds 2^{100}, ensuring resistance to brute-force attacks.

4.4. KEY SENSITIVITY ANALYSIS

Key sensitivity indicates the degree of change in the decrypted image when the key is slightly changed. The key sensitivity of the proposed scheme consists of the initial values and parameters of the chaotic systems together with the DNA sequence rules, and CRT prime numbers, which are tested in two methods:

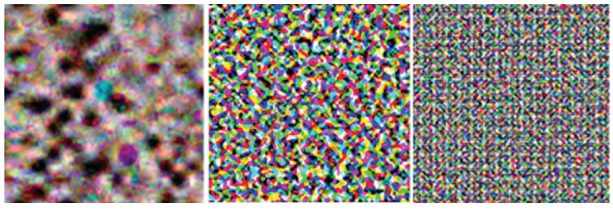
- First, the difference between two encrypted images is measured by re-encrypting the same image with a slightly different key, where the plain image is first encrypted with the correct keys to obtain an encrypted image, namely E_1. The same image is re-encrypted by changing the key, such as the chaotic system's initial value X_0, from 0.3 to $0.3 + 10^{15}$, yielding a new encrypted image, E_2. Finally, the intensity values of E_1 and E_2 are compared. The test image boats is used in Table 12 to measure the difference between E_1 and E_2 for each chaotic system control parameter, CRT prime numbers, and DNA rule.
- The second key sensitivity test is performed by encrypting the plain image using a wrong key, which is done by changing any keyspace parameter or initial value, that is, changing X_0 of any chaotic system to $0.3+10^{-15}$ instead of 0.3. The obtained encrypted image is then decrypted with the correct keys. The $PSNR$ values of the decrypted test image boats for each chaotic system control parameter, CRT prime numbers, and DNA rule are listed in Table 13. Fig. 8 (a), (b), and (c) depict the decrypted boats image, which is decrypted using the wrong Henon, Chirikov, and Arnold cat map parameters, the wrong Lorenz system initial value, and the wrong DNA rule, respectively. The figures show that no information about the original image can be obtained.

Table 12. A key sensitivity evaluation of the encrypted boats image with an incorrect key shows high sensitivity to a slight change in the key

Wrong parameter or initial value	Difference Rate↑
Wrong Logistic map initial value	99.5182%
Wrong Chirikov and Henon map parameters	99.4088%
Wrong CRT prime numbers	99.6208%
Wrong Lorenz system initial value	98.6169%
Different DNA rule	93.8615%

Table 13. PSNR values of the decrypted boats image using a wrong key show robustness against unauthorized access

Wrong parameter or initial value	Decrypted image PSNR↓
Wrong permutation parameters for Henon, Chirikov, and Arnold cat with precision 10-15	10.8508
Wrong encryption initial value for the Lorenz system with precision 10-15	5.2548
Using another DNA rule	5.2763
Wrong CRT prime no.	9.0258



(a) (b) (c)

Fig. 8. Decrypted boats image, which is encrypted with wrong (**a**) Henon, Chiricove, and Arnold cat map parameters, (**b**) Lorenz system initial value, (**c**) DNA rule, demonstrates that a slightly changed key produces an entirely masked image, preventing unauthorized recovery of the original image

4.5. COMPRESSION PERFORMANCE

The compression performance of the proposed scheme is evaluated using compression ratio (CR), Peak signal-to-noise ratio ($PSNR$), and Structural Similarity Index Measure ($SSIM$). The compression ratio of a compressed and encrypted image is measured in bits per pixel (bpp), the

number of bits required per pixel. The formula for measuring bpp is shown in Equation 14. A lower *bpp* value indicates greater compression when bpp is used to measure an image's compression ratio.

$$\text{bpp} = \frac{\text{Total compressed image bits}}{\text{Total number of image pixels}} \quad (14)$$

PSNR, defined in Equation 15, is the most widely used criterion for assessing image quality by measuring the difference between the original and decrypted images [21].

$$PSNR = 10\ log\ \frac{M \times N \times 255^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}[D(m,n)-E(m,n)]^2} \quad (15)$$

where $D(m, n)$ and $E(m, n)$ represent the pixel values of the original and decrypted images at position (m, n), respectively. [54] In lossy image compression, the ideal *PSNR* range for perfect image decryption is 30-50 dB. The ideal *PSNR* value must exceed 28 dB for good image encryption. *SSIM*, defined in Equation 16, is used to evaluate the difference between two similar images.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (16)$$

where x and y represent the plain image and the decrypted image, respectively, μ_x and μ_y are the average values of x and y, the covariance of x and y is symbolized by σ_{xy}, the variance of x and y is denoted by σ_x^2 and σ_y^2 respectively, $C1$ equals $(k_1L)^2$ and $C2$ equals $(k_2L)^2$, where L denotes the pixel intensity value, k_1 equals 0.01, and k_2 equals 0.03. To achieve ideal image encryption, the *SSIM* value must be very close to zero, indicating that the plain and encrypted images are dissimilar. For perfect image decryption, the *SSIM* value must be close to 1 [8]. The compression ratio in bits per pixel (*bpp*), peak signal-to-noise ratio (*PSNR*), and Structural Similarity Index (*SSIM*) values for the test images, decrypted using the proposed scheme, are listed in Table 14, which shows that the bpp values of the test images are small, the *PSNR* values are within the ideal range, and the values of *SSIM* are very close to 1.

Table 14. Objective accuracy evaluation of decrypted image, showing high reconstruction accuracy across *PSNR* and *SSIM* metrics relative to the achieved *bpp*

Image	*bpp* ↓	*PSNR*↑	*SSIM*↑
Lena	3.7723	36.2358	0.9909
peppers	3.0443	34.0806	0.9938
House	3.5957	31.0700	0.9737
Baboon	3.5698	31.5972	0.9710
Airplane	3.5033	32.3455	0.9723
Barbara	3.6351	33.7116	0.9806
Boats	3.4805	31.9815	0.9768

Table 15 compares the bpp, *PSNR*, and *SSIM* values of the proposed scheme with other joined image compression encryption schemes in [50, 55-57]. The table shows that the compression performance of the proposed scheme outperforms other schemes listed in the table, where the bpp value in the proposed scheme is less than that of other schemes, and at the same time, the *SSIM* value is closer to one than that of other schemes, and the *PSNR* value is more than 30.

The early stages of the proposed scheme modify the wavelet data before compression. This lowers the SPIHT efficiency slightly. The final encryption step only scrambles the bitstream, preserving the exact compression ratio. The system accepts this minor drop to guarantee high security.

Table 15. Quantitative performance comparison of the proposed scheme against related schemes, illustrating the enhanced reconstruction accuracy, PSNR, and SSIM achieved relative to the specific data reduction efficiency bpp

Scheme	Image	*bpp*↓	*PSNR*↑	*SSIM*↑
Proposed	Lena	3.7723	36.2358	0.9909
Ref [55]	Lena	4	33.2	0.78
Ref [57]	Lena	4	33.9387	0.9001
Proposed	House	3.5957	31.0700	0.9737
Ref [56]	House	4	34.0112	0.8618
Proposed	Baboon	3.5698	31.5972	0.9710
Ref [50]	Baboon	4	35.7943	0.9716

5. CONCLUSION

This work presented a hybrid lossy multi-layered framework that embeds encryption directly into the Three-dimensional coding of RGB data cubes. Instead of processing color channels separately, the proposed method treated them as a unified spatial-spectral datacube within an adapted 3D-SPIHT architecture. A two-level joint color image compression and encryption scheme that combines 3D SPIHT and CRT with multiple chaotic systems and DNA encoding is proposed in this work. At the first level, a single step of substitution and compression is applied to the LL4 subband using CRT, yielding a preliminary intensity decomposition that preserves the core image structure without increasing the data size. The second level of joint compression and encryption is implemented by combining four chaotic systems with 3D SPIHT compression. In conclusion, an initial intensity partitioning stage, this mapping preserves the global image structure while avoiding data expansion. An additional level of security, using the Lorenz system and a DNA XOR operation, is then implemented on the stream output of 3D SPIHT, which effectively uniformizes the statistical distribution.

Performance evaluations indicated that the proposed work compresses image data to approximately 40% of its original size without sacrificing cryptographic integrity. The keyspace is greater than 2^{100}, and the entropy is near-optimal, indicating that the proposed scheme is resistant to brute-force, statistical, and differential attacks. Finally, this approach shows that strict security requirements and high compression efficiency can be met simultaneously for secure image transmission, yet the standard DWT is inherently sensitive to geometric transformations.

To improve on the current framework, future work can explore employing an Integer Discrete Wavelet Transform to enable strictly lossless reconstruction. Implementing deep learning architectures for dynamic parameter selection is an attractive approach. Applying the proposed scheme to hyperspectral and medical images can help to evaluate its applicability in specialized, high-security domains.

DECLARATION OF THE USE OF AI TOOLS

The authors used Gemini 3 Flash and Grammarly Pro (v1.2.256.1883) for language editing and style refinement. All AI-assisted content was reviewed and edited by the authors, who take full responsibility for the integrity and accuracy of this work. No AI tool is listed as an author, and AI tools are not cited as primary sources.

REFERENCES

[1] H. M. Ghadirli, A. Nodehi, R. Enayatifar, "An overview of encryption algorithms in color images", Signal Processing, Vol. 164, 2019, pp. 163-185. doi: 10.1016/j.sigpro.2019.06.010

[2] M. Lahdir, H. Hamiche, S. Kassim, M. Tahanout, K. Kemih, S. A. Addouche, "A novel robust compression-encryption of images based on SPIHT coding and fractional-order discrete-time chaotic system", Optics & Laser Technology, Vol. 109, 2019, pp. 534-546. doi: 10.1016/j.optlastec.2018.08. 040

[3] X. J. Tong, P. Chen, M. Zhang, "A joint image lossless compression and encryption method based on chaotic map", Multimedia Tools and Applications, Vol. 76, 2017, pp. 13995-14020. doi: 10.1007/s11042-016-3775-6

[4] X. Liu, J Yang, "Joint JPEG compression and encryption with DC groups' random cross-permutation and ZRVs' inter-block permutation", IEEE Transactions on Multimedia, Vol. 28, 2025, pp. 373-387. doi: 10.1109/TMM.2025.3623554

[5] Y. Yang, J. Zheng, X. Zhang, Z. Zhang, "Design of image encryption and compression scheme compatible with JPEG XS based on spatial scrambling", Microelectronics Journal, Vol. 170, 2026, p. 107083. doi: 10.1016/j.mejo.2026.107083

[6] M. Hamdi, R. Rhouma, S. Belghith, "A selective compression-encryption of images based on SPIHT coding and Chirikov standard map", Signal Processing, Vol. 131, 2017, pp. 514-526. doi: 10.1016/j.sigpro. 2016.09.011

[7] T. Xiang, J. Qu, D. Xiao, "Joint SPIHT compression and selective encryption", Applied Soft Computing, Vol. 21, 2014, pp. 159-170. doi: 10.1016/j.asoc.2014.03.009

[8] I. Hraini, M. Farajallah, N. Arman, and W. Hamidouche, "Joint crypto-compression based on selective encryption for WMSNS", IEEE Access, Vol. 9, 2021, pp. 161269-161282. doi:10.1109/ACCESS.2021.3131566

[9] M. Brindha, N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem", Applied Soft Computing, Vol. 40, 2016, pp. 379-390. doi: 10.1016/j.asoc.2015.09.055

[10] H. Zhu, C. Zhao, X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem", Signal Processing: Image Communication, Vol. 28, No. 6, pp. 670-680, 2013. doi: 10.1016/j.image.2013.02.004

[11] I. Ahmad, S. Shin, "A novel hybrid image encryption-compression scheme by combining chaos theory and number theory", Signal Processing: Image Communication, Vol. 98, 2021, p. 116418. doi: 10.1016/j.image.2021.116418

[12] S. Li, Y. Yi, Z. Chen, S. Xie, "A hybrid color image encryption scheme integrating 3D hyperchaotic map, complex network, and compressed sensing", Journal of Information Security and Applications, Vol. 99, 2026, p. 104441. doi: 10.1016/j.jisa.2026.104441

[13] M. Tang, G. Du, Y. Y. Lin, "A novel multi-color image compression encryption algorithm based on the reconstruction coefficient matrix and DNA point mutation operation", Expert Systems with Applications, Vol. 270, 2025, p. 126620. doi: 10.1016/j.eswa.2025.126620

[14] A. Chowdhury, M. Uddin, M. R. Hassan, M. M. Billah, "Image encryption algorithm based on DNA sequence-driven key scrambling and secure hashing", Journal of Information Security and Applications, Vol. 93, 2025, p. 104140. doi: 10.1016/j.jisa.2025. 104140

[15] L. Guo, J. Chen, J. Li, "Chaos-based color image encryption and compression scheme using DNA complementary rule and Chinese remainder the-

orem", Proceedings of the 13th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 16-18 December 2016, pp. 208-212. doi: 10.1109/ICCWAMTIP.2016.8079839

[16] Y. Lin, Z. Xie, T. Chen, X. Cheng, H. Wen, "Image privacy protection scheme based on high-quality reconstruction DCT compression and non-linear dynamics", Expert Systems with Applications, Vol. 257, 2024, p. 124891. doi: 10.1016/j.eswa.2024. 124891

[17] Y. Lin, Y. Liao, Y. Wei, W. Zeng, U. Erkan, A. Toktas, Y. Zhang, D. Chen, "Lightweight image encryption via four-dimensional Hénon memristor map and fast block permutation", Nonlinear Science and Control Engineering, Vol. 1, No. 2, 2025. doi: 10.36922/NSCE025390012

[18] Y. Liao, Y. Lin, Z. Xing, Q. Li, G. Huang, D. Chen, "Using 3D-LMM-based encryption to secure digital images with 3D S-box and Fibonacci Q-matrix", IEEE Internet of Things Journal, Vol. 12, No. 24, 2025, pp. 55182-55195. doi: 10.1109/JIOT.2025.3624032

[19] U. Erkan, F. Toktas, A.Toktas, Q. Lai, S. Zhou, Y. Lin, S. Gao, "Multi-layer and multi-directional image encryption algorithm based on hyperchaotic 3D Xin-She Yang map", Expert Systems with Applications, Vol. 304, 2026, p. 130808. doi: 10.1016/j.eswa.2025.130808

[20] A. Said, W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, No. 3, 1996, pp. 243-250. doi: 10.1109/76.499834

[21] Nasrullah, J. Sang, M. A. Akbar, B. Cai, H. Xiang, H. Hu, "Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps", Applied Sciences, Vol. 8, No. 10, 2018, pp. 1-22. doi: 10.3390/app8101963

[22] Z. N. Ghanim, and S. A. Khoja, "A partial image encryption scheme based on DWT and texture segmentation", Cogent Engineering, Vol. 9, No. 1, 2022, p. 2026555. doi: 10.1080/23311916.2022.2026555

[23] T. Xiang, J. Qu, D. Xiao, "Joint SPIHT compression and selective encryption", Applied Soft Computing, Vol. 21, 2014, pp. 159-170. doi: 10.1016/j.asoc.2014.03.009

[24] B. J. Kim, W.A. Pearlman, "An embedded wavelet video coder using three-dimensional set partitioning in hierarchical trees (SPIHT)", Proceedings of the Data Compression Conference, Snowbird, UT, USA, 25-27 March 1997, pp. 251-260. doi: 10.1109/DCC.1997.582048

[25] B. J. Kim, Z. Xiong, W. A. Pearlman, "Low bit-rate scalable video coding with 3-D set partitioning in hierarchical trees (3-D SPIHT)", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 10, No. 8, 2000, pp. 1374-1387. doi: 10.1109/76.889025

[26] M. Brindha, N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem", Applied Soft Computing, Vol. 40, 2016, pp. 379-390. doi: 10.1016/j.asoc.2015.09.055

[27] I. Ahmad, S. Shin, "A novel hybrid image encryption-compression scheme by combining chaos theory and number theory", Signal Processing: Image Communication, Vol. 98, 2021, p. 116418, doi: 10.1016/j.image.2021.116418

[28] I. A. Taqi, S. M. Hameed, "A new beta chaotic map with DNA encoding for color image encryption", Iraqi Journal of Science, Vol. 61, No. 9, 2020, pp. 2371-2384. doi: 10.24996/ijs.2020.61.9.24

[29] S. M. Hameed, H. A. Sa'adoon, M. Al-Ani, "Image encryption using DNA encoding and RC4 algorithm", Iraqi Journal of Science, Vol. 59, No. 1B, 2018, pp. 434-446. doi: 10.24996/ijs.2018.59.1B.24

[30] X. Wang, Y. Wang, X. Zhu, C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level", Optics and Lasers in Engineering, Vol. 125, 2020, p. 105851. doi: 10.1016/j.optlaseng.2019.105851

[31] T. Sravanti, Y. Kamatham, C. S. Paidimarry, "Reduced complexity hybrid PAPR reduction schemes for future broadcasting systems", Proceedings of the Advances in Decision Sciences, Image Processing, Security and Computer Vision, Springer International Publishing, Vol. 2, pp. 69-76. doi: 10.1007/978-3-030-24318-0_9 (2019)

[32] Z. N. Ghanim, F. N. H. Al-Nuaimy, "Variable length error correcting code for image in OFDM and PAPR reduction", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 27, No. 2, 2022, pp. 859-866. doi: 10.11591/ijeecs.v27.i2.pp859-866

[33] S. Liansheng, D. Cong, Z. Xiao, T. Ailing, A. Anand, "Double-image encryption based on interference and logistic map under the framework of double random phase encoding", Optics and Lasers in Engineering, Vol. 122, 2019, pp. 113-122. doi: 10.1016/j.optlaseng.2019.06.005

[34] S. A. Jerjees, B. A. Esttaifan, T. Z. Ismaeel, "Hybrid ciphering method based on chaos logistic map and fingerprint information", Journal of Engineering Science and Technology, Vol. 15, No. 5, 2020, pp. 3013-3024.

[35] I. A. Taqi, S. M. Hameed, "A new Color image Encryption based on multi Chaotic Maps", Iraqi Journal of Science, Vol. 59, No. 4B, 2018, pp. 2117-2127. doi: 10.24996/ijs.2018.59.4B.17

[36] X. Wang, R. Si, "A new chaotic image encryption scheme based on dynamic L-shaped scrambling and combined map diffusion", Optik, Vol. 245, 2021, p. 167658. doi: 10.1016/j.ijleo.2021.167658

[37] A. Kumar, N. K. Nishchal, "Quick response code and interference-based optical asymmetric cryptosystem", Journal of Information Security and Applications, Vol. 45, 2019, pp. 35-43. doi: 10.1016/j.jisa.2019.01.004.

[38] M. Alawida, A. Samsudin, J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators", Information Sciences, Vol. 512, 2020, pp. 1155-1169. doi: 10.1016/j.ins.2019.10.055

[39] I. T. Almalkawi, R. Halloush, A. Alsarhan, A. Al-Dubai, J. N. Al-Karaki, "A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications", Journal of Information Security and Applications, Vol. 49, 2019, p. 102384. doi: 10.1016/j.jisa.2019.102384

[40] M. Hamdi, J. Miri, B. Moalla, "Hybrid encryption algorithm (HEA) based on chaotic system", Soft Computing, Vol. 25, No. 3, 2020, pp. 1847-1858. doi: 10.1007/s00500-020-05258-z

[41] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi, I. Hussain, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map", Mathematics and Computers in Simulation, Vol. 190, 2021, pp. 826-836. doi: 10.1016/j.matcom.2021.06.008

[42] D. Kumar, A. B. Joshi, S. Singh, "A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D lorenz-chaotic system", Results in Optics, Vol. 5, 2021, p. 100146. doi: 10.1016/j.rio.2021.100146

[43] A. A. Abdallah, A. K. Farhan, "A new image encryption algorithm based on multi chaotic system", Iraqi Journal of Science, Vol. 63, No. 1, 2022, pp. 324-337. doi: 10.24996/ijs.2022.63.1.31

[44] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, Y. Chen, "Colo image compression and encryption scheme based on compressive sensing and double random encryption strategy", Signal Processing, Vol. 176, p. 107684, 2020. doi: 10.1016/j.sigpro.2020.107684

[45] Y. Naseer, T. Shah, Attaullah, A. Javeed, "Advance image encryption technique utilizing compression, dynamical system and S-boxes", Mathematics and Computers in Simulation, Vol. 178, 2020, pp. 207-217. doi: 10.1016/j.matcom.2020.06.007

[46] L. Wang, W. Song, J. Di, X. Zhang, C. Zou, "Image encryption method based on three-dimensional chaotic systems and V-shaped scrambling", Entropy, Vol. 27, No.1, 2025, p. 84. doi: 10.3390/e27010084

[47] W. Alexan, N. H. El Shabasy, N. Ehab, E. A. Maher, "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations", Scientific Reports, Vol. 15, 2025, p. 31246. doi: 10.1038/s41598-025-15794-z

[48] C. Jiang, X. Zhang, X. Zhang, "A novel image encryption scheme based on two-dimensional chaotic map constructed from Ackley function and DNA operations", Entropy, Vol. 28, No. 3, 2026, p. 322. doi: 10.3390/e28030322

[49] A. Maity, Y. L. Chen, W. Alexan, P. Lip Yee, B. C. Dhara, "Image encryption with 6D hyperchaotic system and vision transformer autoencoder", Scientific Reports, Vol. 16, 2026, p. 4243. doi: 10.1038/s41598-025-34378-5

[50] Y. Liang, B. Peng, R. Liu, N. Kang, H. Zhou, "An image compression-encryption algorithm based on BP neural network optimized with fireworks algorithm", Scientific Reports, Vol. 16, No. 7967, 2026, pp. 1-24. doi: 10.1038/s41598-026-36772-z

[51] T. Qayyum, T. Shah, I. Khan, I. L. Popa, "A design of multiple color image encryption scheme based on finite algebraic structures", Scientific Reports, Vol. 15, No. 1, 2025, p. 42571. doi: 10.1038/s41598-025-21018-1

[52] L. Gong, K. Qiu, C. Deng, N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm", Optics and Lasers in Engineering, Vol. 121, 2019, pp. 169-180. doi:10.1016/j.optlaseng.2019.03.006

[53] M. Zhang, X. Tong, "Joint image encryption and compression scheme based on IWT and SPIHT", Optics and Lasers in Engineering, Vol. 90, 2017, pp. 254-274. doi: 10.1016/j.optlaseng.2016.10.025

[54] H. S. Ye, N. R. Zhou, L. H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion", Signal Processing, Vol. 175, 2020, p. 107652. doi: 10.1016/j.sigpro.2020. 107652

[55] C. Sun, E. Wang, B. Zhao, "Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyperchaotic system and plaintext-related scrambling", Entropy, Vol. 23, No. 3, 2021, p. 291. doi: 10.3390/e23030291

[56] Z. Dong, Z. Zhang, H. Zhou, X. Chen, "Color image compression and encryption algorithm based on 2D compressed sensing and hyperchaotic system", Computers, Materials & Continua, Vol. 78, No. 2, 2024, pp. 1977-1993. doi:10.32604/cmc.2024.047233

[57] J. Wang, X. Song, A. A. Abd El-Latif, "Efficient entropic security with joint compression and encryption approach based on compressed sensing with multiple chaotic systems", Entropy, Vol. 24, No. 7, 2022, p. 885. doi: 10.3390/e24070885