Received: August 21, 2023. Revised: October 11, 2023.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Selective Image Encryption Based on Wavelet Domain, 3D-Chaotic Map, and Discrete Fractional Random Transform

Haidar Raad Shakir[1]*

[1]*University of Thi-Qar, Thi-Qar, 64001, Iraq*
* Corresponding author's Email: haidar.raad@utq.edu.iq

Abstract: Minimizing the computational volume during cryptography while preserving optimal security has long been a goal of computer scientists. Selective encryption is a scalable trend in multimedia content protection. This study builds on the findings of previous studies. It suggests employing the integer Haar wavelet transform and 3D-chaotic with the discrete fractional random transform to encrypt color images. First, each primary color was wavelet-processed into four sub-bands. The approximation sub-band of the wavelet transformation was encrypted using discrete fractional random. Subsequently, to construct encrypted images, an updated approximation and detailed sub-bands, followed by pixel permutation, were utilized. A secure hash algorithm for a plain image was used to produce encryption keys. Finally, a numerical analysis and robustness evaluations were performed using an encrypted test image. The results demonstrated the high efficiency of the proposed method for image encryption. Additionally, it is secure against a wide range of attacks such as entropy and asymmetric attacks. The proposed solution outperformed the encryption approaches proposed by other researchers in terms of security and performance evaluation when using images. Therefore, it fills the gaps in the literature on state-of-the-art methods.

Keywords: Encryption, Image encryption, Chaotic maps, DWT, DFrRT, Selective encryption.

1 Introduction

With advanced communication methods, image transmission in social media accounts and financial reasons has become standard as opposed to traditional methods. Sharing a vital message can be achieved using visuals, such as images or graphics. However, data security becomes a concern when the deal is good. Generally, once an image is transmitted, it is viewed by the intended or authenticated person. There is a need for image encryption to enhance the security of the information from images [1]. The security problem can be approached using image encryption with different algorithms, such as the image2D-multiple parameters, 3D-chaotic map method, El-Gamal method, ANN, and the slant transform using the cosine method [2]. The intention was to use the chaotic form and 22 multiple parameters in this case. The elliptic process mainly protects the image from high insecurity and has proven to be the most reliable method for increased security. The reason behind using the chaotic method is the randomness, relation to the initial conditions of the image, and sensitivity.

In recent years, considerable research and development has focused on the creation of chaos-based image cryptosystems [3–8]. Recent developments in image encryption techniques can be broadly classified as either complete image encryption schemes [9] or selective (or partial) image encryption schemes [10]. Both the schemes have been used in recent years. Full-picture encryption techniques work with image data, which requires a significant investment of time and resources, and may not be suitable for use in systems that operate in real time. The use of algorithms that allow for selective image encryption results in considerable cost and time savings throughout the computational process. This is accomplished by encrypting a substantial portion of the original image [11].

The basic idea behind selective image encryption is to divide the information contained in an image into two distinct sections. The first portion is known as the public component, and all users can view and access it without being encrypted. The second section is what is known as the protected section; it is the section that is encrypted. The protected section will only be accessible to persons who have been given proper authorization. In selective encryption, one key aspect that is advised is to minimize the size of the protected portion as much as feasible [12, 13].

The major objective of selective encryption is to minimize the volume of data that must be encoded, which in turn helps to reduce the amount of processing time needed for real-time applications while still maintaining the necessary degree of security. The capacity of selective encryption to maintain the selected characteristics of the primary image, such as scalability, is one of the most essential advantages of this type of encryption.

The majority of an image's information is stored in the low-frequency coefficients of the frequency domain, while finer details are stored in the high-frequency coefficients [14]. In contrast to encrypting the entire frequency domain, only a subset of low-frequency coefficients is required, which reduces the redundancy. This makes it easy to determine which portion of the whole has to be encrypted and which portion may be left uncompressed [15].

To find a harmonious equilibrium between security and speed, several algorithms have been developed to selectively encrypt specific pixels or coefficients within an image [16, 17]. Many of these algorithms employ sophisticated techniques, including wavelet transform utilization. One of the benefits of wavelet transform is that it can be used to break the image into many layers [18].

Based on prior work, this study presents a new method of image encryption that utilizes a secure hash algorithm (SHA-256), discrete fractional random transform (DFrRT), and integer discrete wavelet transform (IDWT). Beginning with the LL component of the original image, one-level DWT was performed. Next, the LL bit streams were encrypted using the DFrRT technique. The final encrypted image is constructed by applying an inverse IDWT (IIDWT) and subsequently permuting the resulting image using a 3D-LCM chaotic map. When decrypting an image, the same process used during encryption is used; however, this time, it is used in reverse. The contributions of this study are as follows:

- Based on the image hash, the 3D-chaotic map, and DFrRT in the wavelet domain, a unique selective image encryption method was proposed. After applying the integer Haar wavelet transform to the plain image, the approximation portion is encrypted using the DFrRT. With only 25% of the image to be encrypted, the time required for approximating part-time encryption is drastically reduced. In addition, the security of the proposed algorithm is improved by introducing a random permutation of all image pixels subsequent to the application of the integer Haar inverse transform.
- The initial parameters of the 3D chaotic system were derived from the SHA-256 hash function applied to a plaintext image. Hash values and random sequences were generated differently for each plaintext image. Consequently, the proposed technique can withstand both known- and chosen-plaintext attacks.
- The proposed algorithm has superior security and is challenging to typical assaults, as shown by the secure data, simulation results, and comparison findings with the present algorithms.

The remainder of this paper is organized as follows.

- Section 2 introduces related work.
- Section 3 provides an outline of the fundamentals of image encryption and decryption.
- Section 4 outlines the proposed image-encryption scheme.
- Section 5 describes the simulations and tests to evaluate the performance of the algorithm.
- Section 6 presents a comparative analysis.
- Finally, Section 7 concludes the study.

2 Literature review

Researchers have used various methodologies and procedures in data security processes. This section examines many studies to determine the methodologies and procedures employed in data security and the protection of digital images.

Kumar et al. [19] introduced a strategy for image encoding and decoding that relies on the two-dimensional discrete wavelet transform (2D-DWT) and a three-dimensional lorenz-chaotic system (3D). In this approach, two levels of 2D-DWT are used to break down the collective representation of various images. Following this decomposition, substitution and permutation techniques were applied using a 3D Lorentz chaotic system. The encoding algorithm was then deployed on distinctive sub-bands at each decomposition level. Upon performing inverse DWT (IDWT), the entire image undergoes a bitwise (Exclusive-OR) XOR operation with a sequence generated by a 3D-Lorenz system, resulting in the final encrypted image. It is worth noting that implementing the proposed technique, whether in hardware or software, presents considerable challenges.

Several other schemes have been proposed, such as the image encryption technique suggested by Ding and Ding [20]. The encryption uses the 2D DWT, fractional-order Henon chaotic map, and 4D hyperchaotic system. A fractional-order Henon chaotic time series shuffles the transformed image after the primary image is changed to the time–frequency domain using a 2D DWT algorithm. The 4D hyperchaotic system then diffuses and encrypts the thoroughly shuffled image. The proposed algorithm is limited to gray scale images.

Tedmori and Al-Najdawi [21] presented a technique for the cryptographic protection of images. Using this technique, the authors proposed an encryption algorithm that utilizes the DWT to transition the initial image into the frequency domain. The objective of the algorithm is to invert the sign and randomly disperse all frequencies within the transformed domain. This encryption scheme has a relatively limited key space.

Somaya et al. [22] proposed a new algorithm unique from the others that uses the chaos-based algorithm for encryption and then compresses the remaining components using the wavelet transform algorithm. The DWT was applied to obtain the approximation coefficient (LL) as well as the detail coefficients. The LL part is encrypted using a 1D chaotic map, and the other coefficients are compressed using a wavelet transform.

Feng et al. [23] introduced the adaptive wavelet chaos-based encryption algorithm, which employed the convex optimization-particle swarm optimization approach to improve the adaptive capability of wavelet transform and scramble low-frequency coefficients. This approach is more resistant to assault; however, the decrypted image is slightly deformed.

Zhong and Li [24] proposed a 3D shuffling scrambling algorithm. This algorithm reconstructs the images into an image cube, and then applies wavelet transformation to each cube layer to encrypt the images. Subsequently, the low-frequency coefficient was scrambled using the 3D shuffling algorithm, and the cube was restructured using the high-frequency and scrambled low-frequency coefficient components. This algorithm is flexible and can encrypt images in color or gray scale of any size; however, it incurs a high computational cost.

Using the hash function SHA-3 and comprehensive sensing, an innovative asymmetric image encoding strategy is proposed in this study [25]. The preprocessed image yields calculated hash values, which are employed to derive the plaintext keys. Rivest–shamir–adleman (RSA) was employed to process the analogous ciphertext keys. The plaintext and ciphertext keys are subsequently recorded in a newly generated model, MTM, to establish the preliminary values for the slantlet transformation (SLT). Subsequently, the original image undergoes compression and distortion. Subsequently, the DWT was applied to the altered image, followed by an additional round of confusion applied to the low-frequency coefficients. However, it is important to emphasize that utilizing the Haar wavelet transform can result in a decline in the quality of decrypted images.

In the proposed method [26], the primary image is broken up into blocks, and then a mask is used to encrypt the wavelet domain coefficients. The encrypted coefficients are then given an Arnold scramble in the last step. The security of an image depends on the number of levels of the wavelet transform. The greater the number of levels it possesses, the higher the security of the image. Similarly, security depends on the number of arnold-scrambling operations.

In a recent method [27], a color-image cryptosystem was introduced, employing bit-plane decomposition, chaos theory, and DWT. The inclusion of bit-plane decomposition and DWT aims to optimize the overall computational efficiency. To achieve the desired outcome, only the low-frequency band is measured for encryption. Additionally, chaotic maps are harnessed to create random sequences and a key image, both of which contribute to diffusion within the plaintext image. The seed values for introducing randomness into the plaintext image were selected by examining the Gauss iterated map. It is worth noting that a drawback of this method is that encryption keys remain static and must be manually configured by the user prior to encryption.

Zhang et al. [28] suggested an image-encryption technique founded on a 3D zigzag transformation and view planes that utilized the traditional scrambling–diffusion paradigm. Chaotic sequences for the encryption procedure were produced using a pseudo-random number generator. The pixel coordinates were modified via a 3D zigzag transformation, while the pixel values were dispersed by the view planes. Color image encryption (CIE) technology has gradually acquired form as a result of the ongoing efforts of numerous scholars. The scrambling–diffusion framework can satisfy the majority of encryption requirements by combining the chaotic system and scrambling technique. The zigzag transform has significant limitations, even though it can be used to reorder the elements of a matrix. The matrix elements are scanned adjacently, which means that the correlation between adjacent elements cannot be lowered as required [29].

El-Shafai et al. [30] proposed an image encryption technique that relied on a 3D chaotic map by implementing a nonlinear ciphering method for the diffusion and permutation of pixel values. To provide a high level of security, the proposed cryptosystem performs five operations on medical images to be delivered. This includes 3D chaos generation, chaos histogram equalization, row and column rotation, and an XOR operator. The proposed method can only be applied to grayscale photos, and requires a significant amount of computation.

Based on the above investigation, we adopted selective encryption using a lightweight cipher as an alternative to the previously employed methods in prior publications. This choice considers the resource limitations of the potential devices and the demand for real-time functionality. Selective encryption, therefore, circumvents the full encryption overhead. Nevertheless, the traditional scheme for selective encryption tends to be relatively heavy, involving successive rounds of bit manipulation, even though it remains secure against brute-force attacks with today's computational capabilities. Hence, the adoption of a lightweight cipher reduced the computational burden. Furthermore, the key space is insufficient, which may make it unsecure under conditions that can be attached by hackers. Hence, a large key space is introduced. In a recent survey [31], it was demonstrated that a 1D chaotic map can be deciphered, and the analysis of a number of 2D chaotic map-based approaches was thoroughly compromised. Therefore, the selected 3D chaotic system has large Lyapunov exponents, which increase the randomness of the produced chaotic stream cipher and the structural complexity of the system. The integer Haar wavelet transform was utilized to maintain the superiority of the decrypted images.

3 Fundamental color-image encryption and decryption

3.1 Integer discrete wavelet transform (IDWT)

Xu et al. [32] employed a lifting scheme to create the integer Haar wavelet transform (IHWT), which represents the second generation of wavelet transforms, starting from the discrete Haar wavelet transform. During this process, a digital image undergoes wavelet transformation, breaking down the original image (with dimensions M × N) into four distinct sets of wavelet coefficients (LL, HL, LH, and HH), each of size M/2 × N/2, commonly referred to as sub-bands. Wavelet transformation was achieved by applying various combinations of low-pass and high-pass filters, both horizontally and vertically, to the digital image. The sub-bands are generated as follows: LL is derived from a low-pass filter applied in both the horizontal and vertical directions, HL results from a high-pass filter applied horizontally followed by a low-pass filter applied vertically, LH is produced from a low-pass filter applied vertically followed by a high-pass filter applied horizontally, and HH originates from high-pass filters employed in both the horizontal and vertical directions. These four decomposition processes in the IHWT are mathematically described by Eqs. (1)–(4).

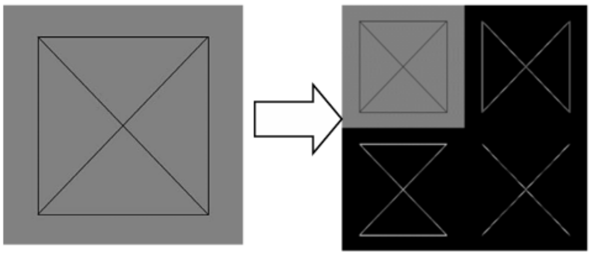


Figure. 1 Integer Haar wavelet transform (IHWT)

According to Fig. (1) The digital image was decomposed into four wavelet sub-bands: LL (top left), HL (top right), LH (bottom left), and HH (bottom right). The calculation for LL averages the values of the image; therefore, this sub-band has a significant coefficient value, high robustness, and good maintenance of the information contained within. In contrast, the HL and LH sub-bands are calculated from the edges of the image; therefore, the coefficient values are less significant. Specifically, HL excludes horizontal edges and preserves vertical and diagonal edges, whereas LH excludes vertical edges and preserves horizontal and diagonal edges. Finally, HH excluded both vertical and horizontal edges.

The IHWT decomposes a 2×2 nonoverlapping digital image into wavelet coefficients in accordance with Eqs. (1)–(4).

$$\begin{bmatrix} I_{m.n} & Im,n+1 \\ Im+1,n & I_{m+1,n+1} \end{bmatrix}$$

$$LL = \left[\frac{\left[\frac{I_{m,n}+I_{m,n+1}}{2}\right]+\left[\frac{I_{m+1,n}+I_{m+1,n+1}}{2}\right]}{2}\right] \tag{1}$$

$$HL = \left[\frac{I_{m,n}-I_{m,n+1}+I_{m+1,n}-I_{m+1,n+1}}{2}\right] \tag{2}$$

$$LH = \left[\frac{I_{m,n}+I_{m,n+1}}{2}\right] + \left[\frac{I_{m+1,n}+I_{m+1,n+1}}{2}\right] \quad (3)$$

$$HH = I_{m,n} - I_{m,n+1} + I_{m+1,n} - I_{m+1,n+1} \quad (4)$$

$I_{m,n}$ represents a single pixel in row m and column n.

To reconstruct the original image, Eqs. (5)–(8), we applied the wavelet coefficients calculated above, as follows:

$$I_{m.n} = LL + \left\lfloor\frac{LH+1}{2}\right\rfloor + \left\lfloor\frac{HL+\left\lfloor\frac{HH+1}{2}\right\rfloor+1}{2}\right\rfloor, \quad (5)$$

$$I_{m,n+1} = I_{m.n} - \left\{HL + \left\lfloor\frac{HH+1}{2}\right\rfloor\right\}, \quad (6)$$

$$I_{m+1,n} = LL + \left\lfloor\frac{LH+1}{2}\right\rfloor - LH + \left\lfloor\frac{HL+\left\lfloor\frac{HH+1}{2}\right\rfloor-HH+1}{2}\right\rfloor, \quad (7)$$

$$I_{m,n+1} = I_{m+1,n} - \left\{HL + \left\lfloor\frac{HH+1}{2}\right\rfloor - HH\right\}. \quad (8)$$

From Eqs. (5)–(8), it is evident that the IHWT preserves the information lost during truncation in Eqs. (1)–(4) by adding an integer value of 1 during reconstruction. With this lifting scheme, no errors occurred in the reconstruction of the initial image. The suggested algorithm scrambles only the LL part of the transform because it contains most of the image detail and presents twenty-five percent of the image. In addition, the IHWT maintained the quality of the reconstructed image after the decryption process. The wavelet transform is more resistant and steadier in the face of security attacks [33].

3.2 Discrete fractional random transform (DFrRT)

A 1-dimensional signal's discrete fractional random transform I is

$$R^{a} = R^{\alpha}S(R^{\alpha})^{T}, \quad (9)$$

where S is the target signal, *a* is the fractional order, R^a is the kernel transform of DFrRT, and $(R^a)^T$ denotes the transpose of R^a. Kernel transform R^{a} is defined as follows:

$$R^{\alpha} = \Lambda R_{R}^{a}\Lambda^{T}, \quad (10)$$

where $\Lambda\Lambda^{T} = 1$, and R_{R}^{a} is a diagonal matrix which can be defined as

$$D_{R}^{a} = diag\left\{1, \exp\left(-\frac{i2\pi a}{K}\right), exp\left(-\frac{i4\pi a}{K}\right), \dots, exp - \frac{i2(N-1)\pi a}{T}\right\}, \quad (11)$$

where *K* is the periodicity and Λ is the symmetric random matrix's eigenvector. The DFrRT inherits the mathematical properties of the fractional Fourier transform, including linearity, unitarity, index additivity, multiplicity, and Parseval energy conservation, among others [34].

3.3 3D-chaotic algorithm

Three chaotic maps are used to achieve this goal. These are vital for applying the backpropagation method. A logistic map is a function that defines the rules and dynamics of the system. The logistic map is important for defining a chaotic algorithm for image encoding and decoding [35]. Generally, a logistic map is represented using growth rate and time. It can be said to be the representation of growth rate against time. The 1D logistic map can be obtained as follows [36]:

$$x = rx(x-1), \quad (12)$$

where x is the initial value in the 1D logistic map for the $r\in[0, 4]$ ..., and the control parameter is *(u)*. The 3D-LCM is an advanced model of the 1D logistic map. The algorithm implies that the 3D-chaotic method is more secure than a 1D logistic map [37].

From the basic 1D-chaotic formulae represented using Eq. (12), the extended version of the chaotic map can be deduced to arrive at the 3D-LCM chaotic map [38]. The extended versions of the chaotic map are as follows :

$$x_{t+1} = r_1 x_t(1-x_t) + r_2 y_t^2 x_t + r_3 z_t^3, \quad (13)$$

$$y_{t+1} = r_1 y_t(1-y_t) + r_2 z_t^2 y_t + r_3 x_t^3, \quad (14)$$

$$z_{t+1} = r_1 z_t(1-z_t) + r_2 x_t^2 z_t + r_3 y_t^3. \quad (15)$$

Eqs. (13)–(15) above represented the chaotic behavior of the extended version deduced from the one-dimensional chaotic map. The control parameters for the 3D chaotic map were r_1, r_2, and r_3. The primary values are x_0, y_0, and z_0. The control parameters are represented as r_1, r_2, and r_3, and the obtained primary values are the keys applied in the proposed method for this study. Some of the essential factors that make the algorithm using the chaotic get more complicated include using a cubic function, as in Eqs. (13)–(15), the applied quadratic coupling, and the variables in the equation. Fig. 2 depicts the

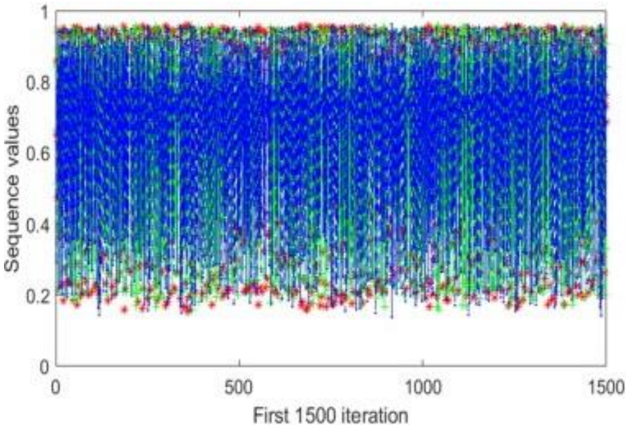


Figure. 2 Chaotic behavior of the first 1500 iterations of 3D-LCM chaotic map

chaotic map formed after 1500 iterations.

4 Proposed algorithm

The strategy proposed in this study may be divided into three basic steps. The designs involve both the encryption and decryption of the image, as well as the production of the key. The key generation stage is vital, as it decrypts the image once it has been encrypted. In general, the receivers of the image will be required to perform decryption, generate a key that will be shared with the authenticated persons, and use the key to decrypt the image to read the information and obtain the information in the image as it was from the sources. In addition, we consider that the receivers of the image are required to perform decryption.

4.1 Key generation

The secret key was produced using the SHA-265 hash algorithm. It was used to build a link between the encryption algorithm and the original image by constructing the primary and control parameters of the 3D-LCM chaotic map. A 256-bit binary sequence is the output of the SHA-256 hashing algorithm. To obtain the decimal values h1, h2, and h64, the 256-bit hash value of the original image was divided into 4-bit blocks and then multiplied by 64. The corresponding initial values, often known as secret keys, are determined by:

$$\begin{cases} x_0 = \frac{h_1 \otimes h_2 \otimes .. \otimes h_5}{256} \\ y_0 = \frac{h_6 \otimes h_7 \otimes .. \otimes h_{10}}{256} \times 4 \\ z_0 = floor\left(\frac{h_{11} \otimes h_{12} \otimes .. \otimes h_{15}}{256} \times 7\right) + 9 \end{cases} . \quad (16)$$

The three control parameters (r_1, r_2, and r_3) are generated according to:

```
Algorithm 1: Encryption procedure of plain image
Input: Plain color image I
a) Generate Secret Keys for 3D-LCM map by applying SHA-256 of the image;
b) Set Private Keys by user for DFrRT.
c) Converting the image into a frequency domain by applying integer Haar wavelet transform, to get approximation (LL) and detail coefficients (LH, HL, HH).
d) Scramble the approximation part using DFrRT as in Algorithm 2.
e) Apply inverse integer Haar wavelet transform (IDWT).
f) Shuffle IDWT resulting image using 3D-LCM system according to Algorithm 3.
g) Presenting the ultimate encrypted image E to the receiver
Output: Encrypted image E
```

$$\begin{cases} r_0 = \left(\frac{h_{16} \otimes h_{17} \otimes h_{18}}{256}\right) \times 3.89 + 0.01 \\ r_1 = \left(\frac{h_{19} \otimes h_{20} \otimes h_{21}}{256}\right) \times 2.34 + 0.01 \\ r_2 = \left(\frac{h_{22} \otimes h_{23} \otimes h_{24}}{256}\right) \times 1.46 + 0.01 \end{cases} . \quad (17)$$

The three DFrRT initial values (a_1, a_2, and a_3) are set as secret ranges.

4.2 Color-image encryption algorithm

Fig. 2 shows a diagram of the proposed method. The image passes through the proposed algorithm from the figure with the inputs as the private key and secret range. To effectively encrypt an image, it follows Algorithm 1.

The algorithm for the proposed approach employed both permutation and substitution techniques. All the steps of the encryption procedure are shown in Fig. 3.

In the first step, the necessary images for the algorithm's inputs are gathered. When dealing with H×W-formatted images, it is presumed that they are of the standard size.

In Step 2, an approximate matrix (LL) and three detail matrices are created using the DWT transformation.

Step 3 involves generating three chaotic sequences xi, yi, and zi using equations by validating the primary values x_0, y_0, and z_0 and iterating the 3D-LCM chaos system.

Step 4 involves transforming three random sequences (*xi*, *yi*, and *zi*) into integer sequences (t can be x, y, or z).

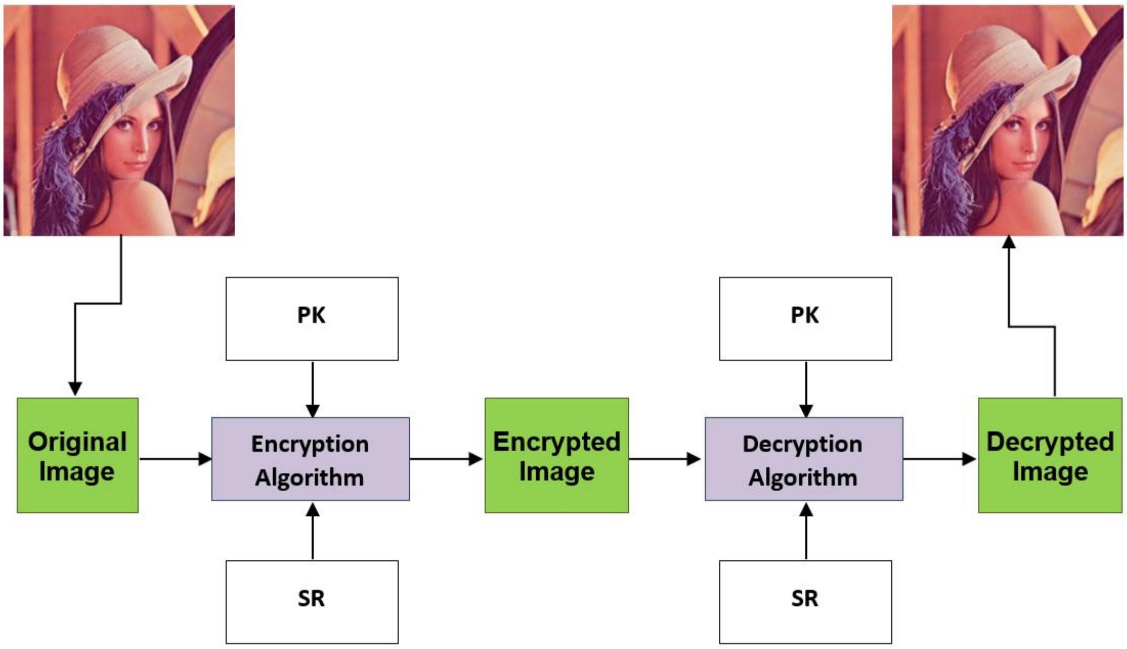


Figure. 2 Proposed method

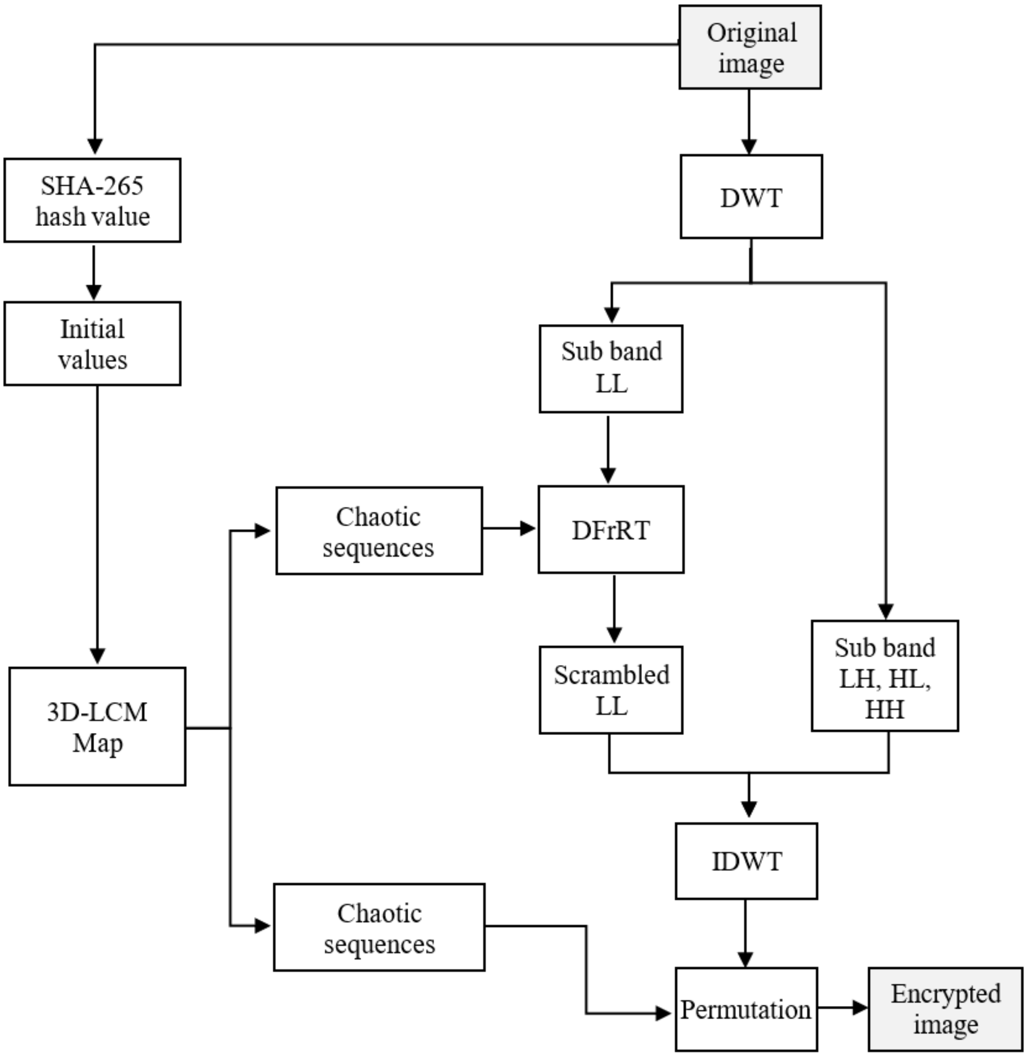


Figure. 3 Proposed color-image encryption block diagram

```
Algorithm 2: Scramble of approximation part of plain image
Input: Plain Color $LL_{m\times n\times q}$ part of the image
a) Initial x(i) y(1);
b) Obtain vector $x, y$ according to Eqs. (13-15);
c) Construct random matrix, according to Eq. (19) and Eqs. (20-21);
d) Obtain matrix $D_R^a$ . and $R^a$;
e) Tensor product $R_1$ , $R_2$, $R_3$.
Output: $LL'_{m\times n\times q}$
```

$$t_i^* = \left|\left\lfloor \left(t_i - \lfloor t_i \rfloor \right) \times 10^{14} \right\rfloor\right| \bmod 255, \quad (18)$$

where ⌊*x*⌋rounds x to the integer nearest to zero.

Step 5: The goal of Step 5 is to encipher the approximation section (LL) using the same matrices that were used to encode the xi and *yi* components of the chaotic map. Applying the DFrRT encrypts the (LL). This is how the cipher operates.

I. Obtain encrypted approximation part (LL') sequences by performing DFrRT on the LL. Random matrix obtained as

$$P = \frac{\eta Q_1 + (1-\eta) Q_2}{2}, \quad (19)$$

where $0 < \eta < 1$,random circular matrices Q_1 and Q_2 can be constructed by following expression

$$Q(i,1) = \lambda Q(i-1,N), \quad (20)$$

$$Q(i,2{:}N) = Q(i-1,1{:}N-1). \quad (21)$$

For the vector *Q(i; 1)*, we replace the first element with *(Q(i-1;N)*, where *2 I (M and > 1)*. The 3D-logistic chaotic locate (3D-LCM) in Eqs. (13–15) generates the first row of the vector Q, denoted by *Q(1;:)*.

Encryption LL sequences generated through following transform expression

$$LL'_{m\times n\times q} = \mathcal{F}_{m\times n\times q.} \quad (22)$$

The kernel matrices for each color channel are $R_1(m\ m)$, $R_2(n\ n)$, and $R_3(q\ q)$ (R, G, and B, respectively). In this case, tensor multiplication was performed using a separate kernel matrix, which is built from the starting values specified by the user in subsection 4.1. You may refer to it as "3D-DFrRT." For convenience, we set $R_1 = Ra_1$, $R_2 = (Ra_2)^T$, and $R_3 = -Ra_3$.

Algorithm 2 presents the pseudocode for the tensor-based encoding in conjunction with the 3D-LCM algorithm.

```
Algorithm 3: Pixel shuffling
Input: Scrambled IIDWT of the image
Set input image C, image width w, image height h, 3D-LCM chaos sequence matrix S
Initialize a 3D array P of dimension w × h × 3 with zeros;
for h = 1,2,...,6 do
    for d = 1,2,3 do
        Sort S[:,h] and get the vector of sorted position v;
            for i = 1,2,...,h do
                for j = 1,2,...,w do
                    p = v [(i - 1) × w + j];
                    k = ceil (p / w);
                    l = p - w×(k - 1);
                    P [i,j,d] = C [k,l,d];
                End
            End
    End
    E = P;
end
Output: Encrypted image E
```

In Step 6, we conduct an IIDWT using encrypted (LL) and detail matrices (LH, HL, and HH).

Step 7: To obtain the final encryption image, perform pixel permutation on the (IDWT) results. The {x_i},{y_i}, and {z_i} sequences are used to change the pixel positions. Algorithm 3 shows the shuffling pseudocode.

5 Experiment and result analysis

Here, we detail the simulated outcomes resulting from using the proposed method for image encryption. A 64-bit Windows 10 PC with 4 GB of RAM, Intel Core i5 CPU at 2.90 GHz, and MATLAB R2021a served as the coding platform. In this section, the security of the proposed method is discussed in detail. To assess the effectiveness of our approach, we performed experiments using the USC-SIPI image dataset [39].

5.1 Key space analysis

The key space for an image encryption system should be maximized to the greatest practical extent, with a minimum requirement of 2^{100} [40], to thwart brute-force assaults. In the suggested methodology, the 3D LCM chaotic system is defined by positive system parameters (r_1, r_2, r_3) and initial values (x_0, y_0, z_0), which serve as secret keys. In addition, DFrRT involves secret keys (a_1, a_2, a_3). When considering the positive system parameters and primary values of the 3D LCM

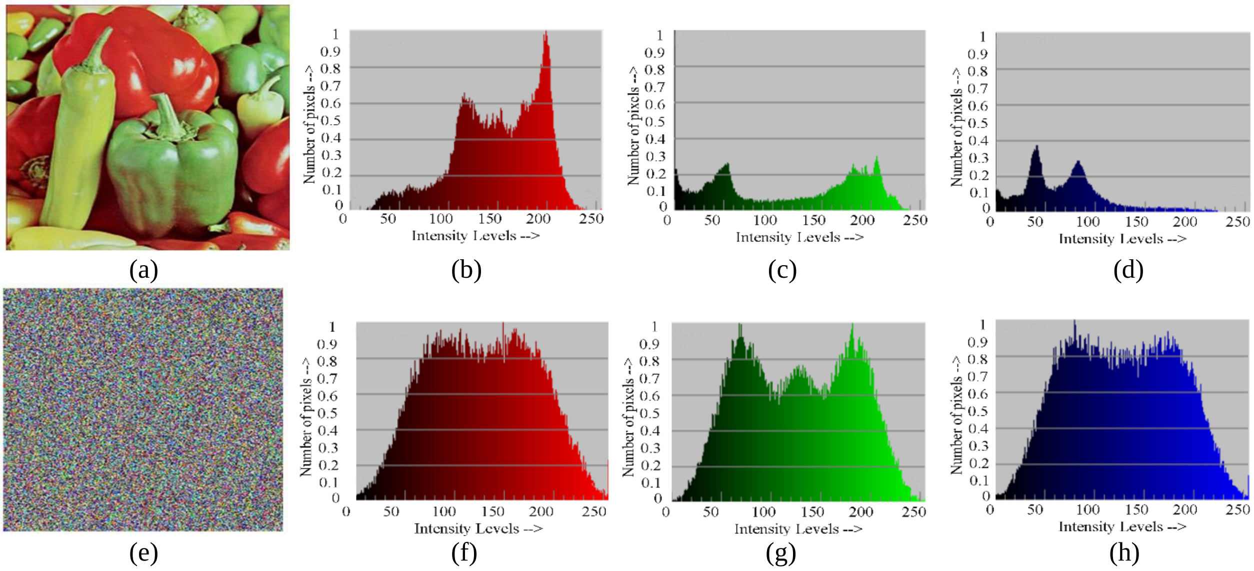


Figure. 4 Original simulation and cipher image histograms: (a) represent the original image, (b), (c), and (d) show the histograms of the R, G, and B channels of image (a), respectively, (e) Encrypted image, (f), (g), and (h) show the histograms of R, G, and B in image (e), respectively

chaotic system alongside a 256-bit hash key with a precision level of 10^{-15}, the key space expands to $(10^{-15})^{9} \times 2^{256}$, approximately equal to $2^{705} > 2^{100}$, which significantly surpasses the minimum required key space. Thus, our method effectively utilizes a key space that aligns with the security requirements, making it resilient against brute-force attacks.

5.2 Histogram analysis

The analysis represents the scattering of pixels for the primary and encrypted images. Histogram analysis was used in MATLAB for evaluation, which proved to be effective from the results collected. Original images produce a uniform distribution of histograms because there is a variance in the signals instead of the encrypted images, which is expected to produce a flab behavior.

Fig. 4 shows the original and cipher image histograms of the simulation. Through confusion and diffusion, the attack on the cipher is complex, as shown in Fig. 4. Determining the originality of an image using the substitution method on the cipher is complicated by comparing the behavior shown in Fig. 4. The histogram resulting from the encrypted image is close to being invariant in nature from the figure. This complicates the algorithm because a low correlation is observed between the two.

5.3 Mean square error (MSE) and peak signal-to-noise ratio (PSNR)

Table 1. Evaluation of test images using (MSE) and (PSNR)

Image	MSE	PSNR
Airplane	9734.82	8.2475
Baboon	6922.92	9.7279
Lena	6535.46	9.9780
Fruits	8768.87	8.7014
Peppers	7526.55	9.3648

The image encryption property comparison was performed using MSE and PSNR. When the MSE increases, it implies that the relative distortion of the image also increases; in that case, we expect the pixels to be slightly different for the high MSE and low MSE. The MSE formula is as follows:

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j)-y(i,j)]^{2}. \quad (23)$$

In this equation, x(i, j) represents the input image, y(i, j) represents the output image, and (i, j) represents the coordinates used to encrypt the image. The matrix used for encryption is represented by M×N.

The peak signal and point ratio formulae help to determine the relationship between the two. Image noise can be measured in decibels by using this method. When the PSNR is low, it implies a high degradation of the encrypted image, and vice versa. Encryption was more effective when the ratio was lower. When the ratio increases, the physical eye can create visualizations of the image and try to recognize its shape instead of when it is low. This equation can be expressed as follows:

Table 2. Correlation coefficient analysis for the test images

Image name	Correlation for original image			Correlation for encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Airplane	0.96519	0.96099	0.93251	0.0022	0.0099	0.0114
Baboon	0.92306	0.86595	0.85434	0.0294	0.0444	−0.0176
Lena	0.97977	0.98931	0.96969	−0.0019	−0.0039	0.0011
Fruits	0.9726	0.97282	0.95225	0.0267	−0.0051	0.0202
Peppers	0.9378	0.9515	0.9028	−0.0540	0.0570	−0.0427

$$PSNR = 10\log_{10}\left[\frac{(I_{\max})^2}{MSE}\right], \tag{24}$$

where peak intensity is symbolized by *I* max, and the intensity value can be changed from time to time to obtain the results from the simulation as the input.

When the noise increased, the ratio decreased. This implies that the encryption complexity increases; hence, the image becomes more secure when noise increases, as shown in Table 1.

5.4 Correlation analysis

The correlation analysis of two images being encrypted determines how they are related in terms of their properties on the pixels. The primary objective of encryption is to minimize pixel correlation as extensively as possible, thereby enhancing the security of the encrypted image. This reduces the chances of a substitution attack on an image. The correlation and covariance equations applied in the analysis are represented as follows:

$$r_{xy} = \frac{|cov(x,y)|}{\sqrt{D(x)} \times \sqrt{D(y)}}, \tag{25}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{26}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{27}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{28}$$

In this context, the covariance between the two encrypted images is denoted as cov(x,y). After randomly selecting both the primary and encrypted images, we computed the association between 3,000 pairs of neighboring pixel spots over the horizontal, vertical, and diagonal axes of the images. We determined the mean correlation value by calculating a total of thousand times for each image. The results are shown in Table 2. This is illustrated in Fig. 4. Compared to the primary image, the correlation between the encrypted image pixels are much lower, suggesting that the method effectively counters statistical attacks.

As illustrated in Fig. 5, the pixels in the primary image exhibit a concentration across the diagonal line and in the areas flanking it in all three directions, indicating a strong correlation. In contrast, the pixels in the encrypted image were evenly dispersed within the coordinate space, indicating a substantial reduction in the correlation. Hence, both quantitative and qualitative analyses affirm that the algorithm effectively diminishes the correlation within encrypted images, bolstering their resistance to statistical attacks.

5.5 Entropy information

The encrypted image represents the level of certainty. This primarily represents the image aggregation function of the study. The equation used to represent entropy is as follows:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log_2 \frac{1}{p(m_i)}. \tag{29}$$

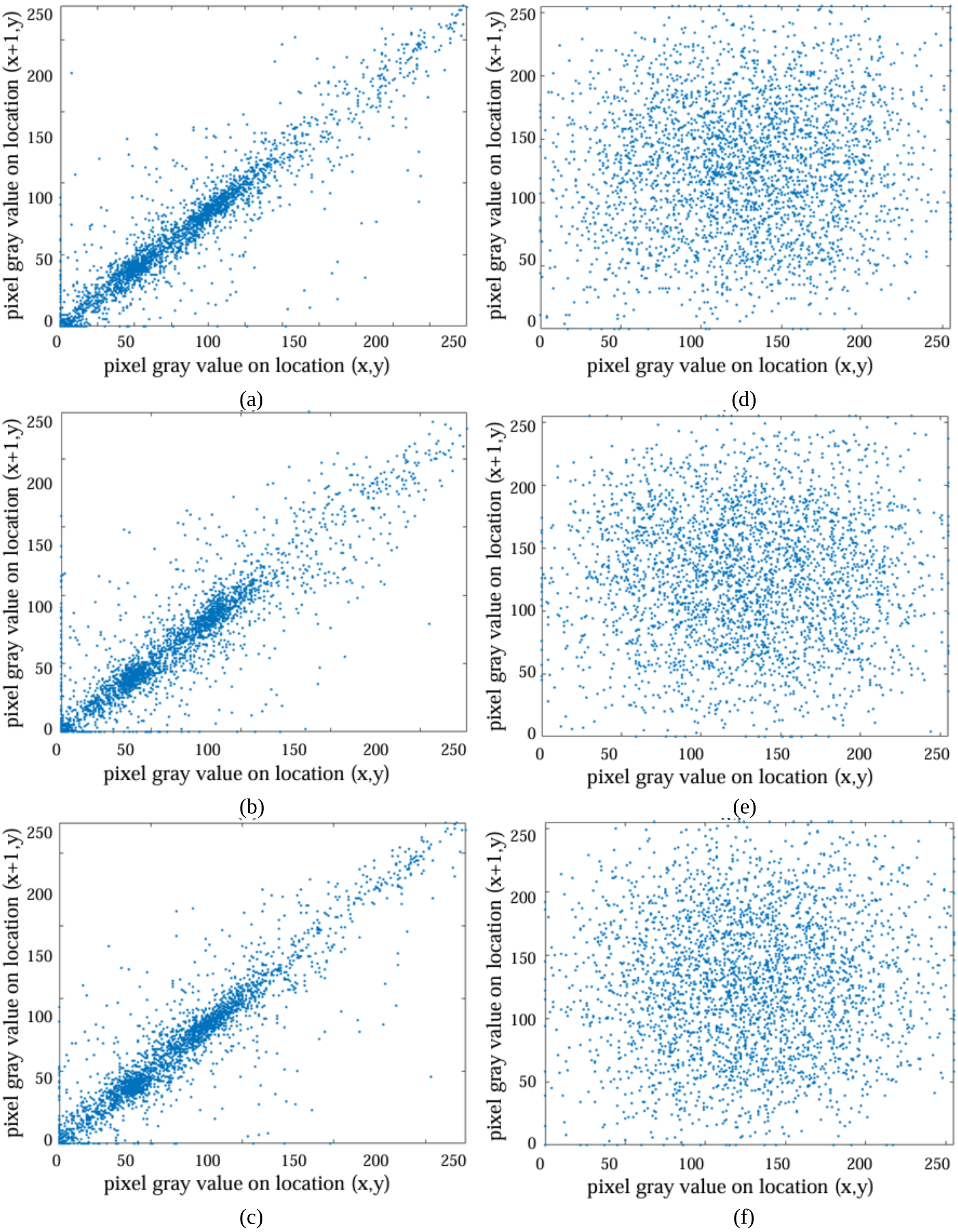
H(m) is the entropy of an image and p(m) is the probability of m or the frequency of m. When the entropy increases, the distribution of pixels becomes even greater.

The plaintext and ciphertext, which are the outcomes of the procedure, are shown in Table 3, along with their respective information entropies. When the ciphertext values are approximately 8, as they should be, it indicates that the encryption produces a complicated output that is close to a random signal value and is thus difficult to break.

5.6 Differential attack

In this type of attack, the attacker modifies the encrypted image by adding a small input to the active primary-image signal. Consequently, the attacker has access to the system, which can affect the desired changes. The following equations were used to assess the differential attack technique.

Received: August 21, 2023. Revised: October 11, 2023.



(a) (d)

(b) (e)

(c) (f)

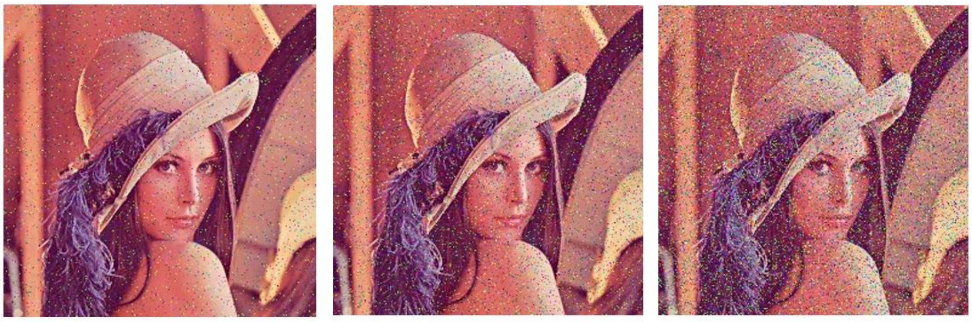
Figure. 5 The correlations between two neighboring pixels, with: (a), (b), and (c) representing the correlations in the vertical, horizontal, and diagonal directions in the plain image, and (d), (e), and (f) representing the correlations in the cipher image

$$NPCR\ (C_1, C_2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{D(i,j)}{L} \times 100\%, \quad (30)$$

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{cases}, \quad (31)$$

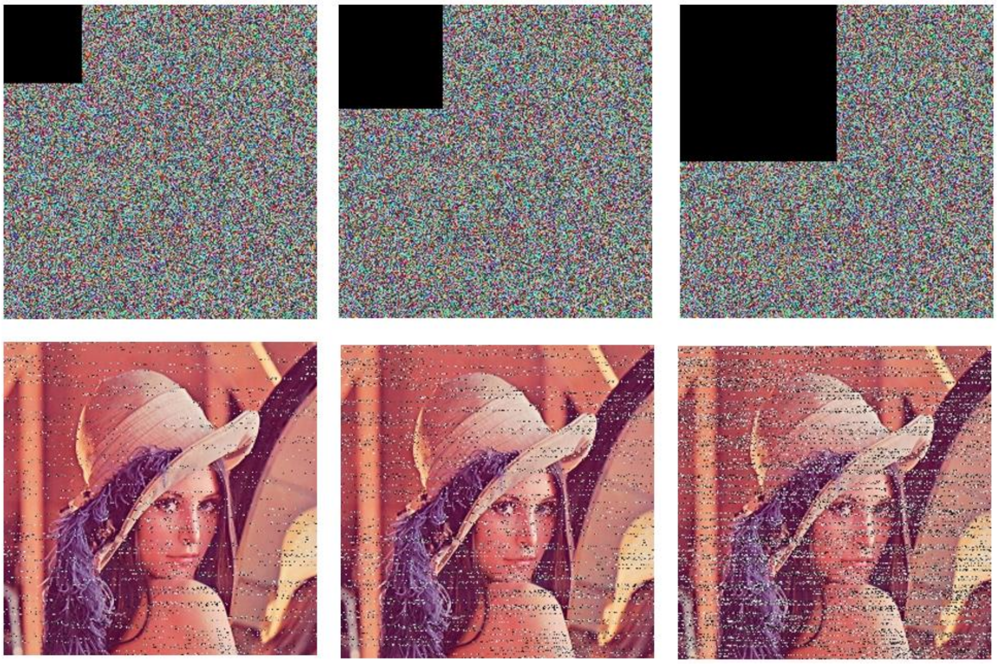
$$UACI\ (C_1, C_2) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{T \times L} \times 100\%, \quad (32)$$

where M and N represent the width and height of the encrypted image, respectively. L is the pixel



(a) (b) (c)

Figure. 6 Image restoration for Lena: (a) 0.001, (b) 0.01, and (c) 0.05 salt and paper noise



(a) (b) (c)

Figure. 7 Examining the attack decrypted version of the ciphertext image with a 5% loss in data loss of 15% in the ciphertext image and the outcome of decryption: (c) an example of ciphertext with a 25% loss of information and the outcome of decryption

Table 3. Entropy analysis for five images

Image	Entropy		
	Red	Green	Blue
Airplane	7.9992	7.9991	7.9996
Baboon	7.9990	7.9990	7.9993
Lena	7.9993	7.9996	7.9996
Fruits	7.9998	7.9995	7.9991
Peppers	7.9995	7.9998	7.9998

number because T is the largest value of L that the image can accept. C_1 and C_2 represent the cipher images as image1 and image2, respectively.

The NPCR and UCI values are listed in Table 4. The fact that the ciphertext has an NPCR of 99.7 percent and a UACI of 33.4 percent demonstrates the efficacy of the algorithm as a highly secure method of encryption.

Table 4. NPCR and UACI results

Image	**NPCR**			**UACI**		
	Red	Green	Blue	Red	Green	Blue
Airplane	99.48%	99.44%	99.59%	33.31%	33.25%	33.34%
Baboon	99.47%	99.45%	99.35%	33.35%	33.40%	33.33%
Lena	99.59%	99.60%	99.60%	33.43%	33.46%	33.45%
Fruits	99.58%	99.60%	99.52%	33.38%	33.26%	33.46%
Peppers	99.44%	99.57%	99.60%	33.36%	33.30%	33.31%

5.7 Analysis of noise and data-loss attack

Most data channels are noisy, which increases the risk of data corruption or loss during transmission [41]. Therefore, it is crucial that a cryptosystem can provide a solid line of protection against such attacks if it is well designed. We detail the effects of noise and data-loss attacks on test images encrypted using the proposed approach to gauge its efficacy. We considered a salt-and-pepper noise attack with varying amounts of added pepper noise. The data obtained in this study are presented in Fig. 6. Similarly, we examine black cut-outs of varying sizes (ranging from 4.5 percent to twenty-five percent of the image's content) to illustrate a data-loss attack (as shown in Fig. 6), all of which are meant to throw doubt on the dependability of the cryptosystem (for the Lena image). Figs. 6 and 7 display the outcomes, showing that the basic Lena image can be restored despite assaults of noise and data loss. Our proposed encryption system can withstand assaults such as noise, and data loss is evidence of its strength.

5.8 Time complexity test

The effectiveness of an encryption method is typically used as the criterion for quality. An efficient encryption technique requires a rapid computation time. However, it is not possible to perform an accurate comparison of run times if the run environments are significantly different. In this study, we chose to test the Lena image with pixel dimensions of 256×256 and 512×512. We compared the time taken to encrypt a file to those found in the literature [20, 22, 23, 28], and the findings are tabulated in Table 5. Our study’s encryption time for a 256×256 Lena image is 0.325 s, which is faster than the times reported in [20, 22, 23, 28], but slower than the time reported in [28] for 512×512 images. This study increases the size of the key space and shuffles the pixels in the confusion processes to satisfy stricter security standards. simultaneously enhances both temporal complexity and vulnerability to assaults. With only a modest increase in the time required, it maintains a reasonable rate of progress. Therefore, the proposed encryption technique can largely accommodate user requirements owing to its comparatively optimal encryption time and guaranteed encryption effect.

6 Comparison with previous works

Most researchers have attempted to incorporate improved techniques from previous studies to overcome existing shortcomings. Here, we analyze and compare the proposed cryptosystem with recent works. The assessment relies on evaluation metrics, such as entropy, correlation, NPCR, UACI, and key space. These metrics were assessed using digital Lena images and encryption algorithms detailed earlier. The outcomes of these tests are presented in Tables 6-9. Examining these tables reveals that the proposed scheme exhibits superior security performance compared with the encryption methods listed. Notably, the analysis of the correlation coefficient values in all three directions outperformed the corresponding values found in some of the existing encryption schemes outlined in Table 6. This observation indicates that the proposed image encryption technique has a considerable capacity to disrupt the association between nearby pixels in the original color image along different directions. Consequently, the proposed scheme demonstrated a superior level of resistance to common statistical attacks. From Table 7, it is evident that the entropy of the proposed image encryption algorithm closely approximates the ideal value of 8. Consequently, the level of information leakage within the proposed scheme remains minimal, thereby fortifying its resistance against entropy-based attacks.

Table 5. Lena's image encryption time comparison

Encryption algorithm	**Encryption time**	
	256×256	512×512
Reference [20]	0.54	1.02
Reference [22]	0.5	—
Reference [23]	—	3.27
Reference [28]	0.256	0.94
Proposed algorithm	0.325	1.081

Furthermore, compared with the latest available cryptosystems in [22, 25, 27], the proposed encryption scheme is more suitable for security applications because it is equipped with powerful chaotic mapping in terms of complex dynamic behavior. Additionally, based on the analysis in Table 8, it can also be observed that the diffusion properties of the proposed method in the NPCR and UACI safety analysis are significantly better than those proposed in [20, 25, 27, 28].

Finally, Table 9 summarizes the key space assessment between the proposed image encryption method and the existing image encryption methods. The proposed encryption method provides a larger key space than the most popular image-encryption schemes used in previous studies [20, 25, 27, 28, 30].

7 Conclusion

This work suggests employing the IHWT and 3D-chaotic with DFrRT in color-image encryption. To obtain the LL part, a DWT with one level is first performed. The generated LL pixels were then encrypted using a DFrRT. Once an inverse Fourier

Received: August 21, 2023. Revised: October 11, 2023.

Table 6. Correlation coefficient comparison for encrypted Lena image

Correlation coefficient	Proposed scheme	Ref. [20]	Ref. [24]	Ref. [25]	Ref. [27]	Ref. [28]
Horizontal	−0.0019	−0.0082	−0.0016	0.0004	−0.0306	0.6393
Vertical	−0.0039	−0.0059	0.0052	0.0043	0.0097	−0.0452
Diagonal	0.0011	0.0007	0.0049	−0.0003	0.00406	−0.0473

Table 7. Average entropy analysis for proposed method and other reference methods

Proposed scheme	Ref. [20]	Ref. [25]	Ref. [27]	Ref. [28]
7.9994	7.9886	7.9977	7.9971	7.9993

Table 8. Comparison of NPCR and UACI between different schemes for encrypted Lena image

Scheme	**NPCR**	**UACI**
Ref. [20]	99.55%	33.25%
Ref. [24]	99.62%	—
Ref. [25]	99.60%	33.46%
Ref. [27]	99.59%	33.57%
Ref. [28]	99.61%	33.45%
Proposed	99.60%	33.45%

Table 9. Comparison of key space between different schemes proposed encryption method

Scheme	**Key space**
Ref. [19]	2^{299}
Ref. [20]	2^{589}
Ref. [25]	2^{265}
Ref. [27]	2^{270}
Ref. [28]	2^{372}
Ref. [30]	2^{412}
Proposed	2^{705}

transform is applied, a scrambled image is created (IDWT). Next, the image pixels were shuffled using a 3D-LCM chaotic map to create the ultimate encrypted image. Experimental findings show that the proposed approach is more efficient for image encryption. Furthermore, they are resistant to a wide range of threats, including entropy and asymmetric attacks. As a result, a very high level of security is achieved. The proposed solution outperformed the encryption approaches disclosed by other authors in terms of both security and performance evaluations using images.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, "Traditional and Hybrid Encryption Techniques: A Survey", *Networking Communication and Data Knowledge Engineering*, pp. 239–248, Springer, 2018.

[2] X. M. Wang, M. Lind, and G. P. Bingham, "A Stratified Process for the Perception of Objects: From Optical Transformations to 3D Relief Structure to 3D Similarity Structure to Slant or Aspect Ratio", *Vision Research*, Vol. 173, pp. 77–89, 2020.

[3] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A New Chaotic Algorithm for Video Encryption", *IEEE Transactions on Consumer Electronics*, Vol. 48, No. 4, pp. 838–844, 2002.

[4] Z. Chen, H. Li, E. Dong, and Y. Du, "A Hyper-Chaos Based Image Encryption Algorithm", In: *Proc. of 2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics*, pp. 188–191, IEEE, 2010.

[5] C. Li, G. Luo, K. Qin, and C. Li, "An Image Encryption Scheme Based on Chaotic Tent Map", *Nonlinear Dynamics*, Vol. 87, No. 1, pp. 127–133, 2017.

[6] Y. Zhang, "The Image Encryption Algorithm Based on Chaos and DNA Computing", *Multimedia Tools and Applications*, Vol. 77, No. 16, pp. 21589–21615, 2018.

[7] Z. Y. Peng, L. Wei, C. S. Ping, Z. Z. Jun, N. Xuan, and D. W. Di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES", In: *Proc. of 2009 IEEE International Conference on Systems, Man and Cybernetics*, pp. 474–479, IEEE, 2009.

[8] S. Wang, C. Wang, and C. Xu, "An Image Encryption Algorithm Based on a Hidden Attractor Chaos System and the Knuth–Durstenfeld Algorithm", *Optics and Lasers in Engineering*, Vol. 128, p. 105995, 2020.

[9] T. Gao and Z. Chen, "Image Encryption Based on a New Total Shuffling Algorithm", *Chaos, Solitons & Fractals*, Vol. 38, No. 1, pp. 213–220, 2008.

[10] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "A Novel Selective Image Encryption Method Based on Saliency Detection", In: *Proc. of 2016 Visual Communications and Image Processing (VCIP)*, pp. 1–4, IEEE, 2016.

[11] L. Li, Y. Yao, and X. Chang, "Plaintext-Dependent Selective Image Encryption Scheme Based on Chaotic Maps and DNA Coding", In: *Proc. of 2017 International Conference on Dependable Systems and Their Applications (DSA)*, pp. 57–65, IEEE, 2017.

[12] A. Ramesh and A. Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security", In: *Proc. of 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, pp. 840–844, IEEE, 2013.

[13] A. Massoudi, F. Lefebvre, C. D. Vleeschouwer, B. Macq, and J. J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives", *Eurasip Journal on information security*, Vol. 2008, No. 1, p. 179290, 2008.

[14] G. A. Spanos and T. B. Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video", In: *Proc. of International Conference on Computer Communications and Networks*, pp. 2–10, 1995.

[15] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video", *IEEE Transactions on Multimedia*, Vol. 5, No. 1, pp. 118–129, 2003.

[16] S. Sasidharan and R. Jithin, "Selective Image Encryption Using DCT with Stream Cipher", *International Journal of Computer Science and Information Security*, Vol. 8, No. 4, pp. 268–274, 2010.

[17] X. Liu and A. M. Eskicioglu, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions", *IASTED Communications, Internet & Information Technology (CIIT), USA*, p. 2003.

[18] S. G. Mallat, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 11, No. 7, pp. 674–693, 1989.

[19] D. Kumar, A. B. Joshi, and 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, p. 100146, 2021.

[20] L. Ding and Q. Ding, "A Novel Image Encryption Scheme Based on 2D Fractional Chaotic Map, DWT and 4D Hyper-Chaos", *Electronics*, Vol. 9, No. 8, p. 1280, 2020.

[21] S. Tedmori and N. A. Najdawi, "Image Cryptographic Algorithm Based on the Haar Wavelet Transform", *Information Sciences*, Vol. 269, pp. 21–34, 2014.

[22] S. A. Maadeed, A. A. Ali, and T. Abdalla, "A New Chaos-Based Image-Encryption and Compression Algorithm", *Journal of Electrical and Computer Engineering*, Vol. 2012, p. 179693, 2012.

[23] F. P. An and J. Liu, "Image Encryption Algorithm Based on Adaptive Wavelet Chaos", *Journal of Sensors*, Vol. 2019, p. 2768121, 2019.

[24] H. Zhong and G. Li, "Multi-Image Encryption Algorithm Based on Wavelet Transform and 3D Shuffling Scrambling", *Multimedia Tools and Applications*, pp. 1–20, 2022.

[25] Z. Chen and G. Ye, "An Asymmetric Image Encryption Scheme Based on Hash SHA-3, RSA and Compressive Sensing", *Optik*, Vol. 267, p. 169676, 2022.

[26] R. M. Saffari and S. Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Discrete Wavelet Transform Using Two Dimensional Logistic Map", In: *Proc. of 2016 24th Iranian Conference on Electrical Engineering (ICEE)*, pp. 1785–1790, 2016.

[27] A. Shafique, "A Noise-Tolerant Cryptosystem Based on the Decomposition of Bit-Planes and the Analysis of Chaotic Gauss Iterated Map", *Neural Computing and Applications*, Vol. 34, No. 19, pp. 16805–16828, 2022.

[28] X. Zhang and Z. Gong, "Color Image Encryption Algorithm Based on 3D Zigzag Transformation and View Planes", *Multimedia Tools and Applications*, Vol. 81, No. 22, pp. 31753–31785, 2022.

[29] M. Demirtas, "A Color Image Scrambling Method Based on Zigzag Transform and Cross-Channel Permutation", *Avrupa Bilim Ve Teknoloji Dergisi*, No. 36, pp. 91–95, 2022.

[30] W. E. Shafai, F. Khallaf, E. S. M. E. Rabaie, and F. E. A. E. Samie, "Proposed 3D Chaos-Based Medical Image Cryptosystem for Secure Cloud-IoMT EHealth Communication Services", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–28, 2022.

[31] U. Zia, M. McCartney, B. Scotney, et al., "Survey on Image Encryption Techniques Using Chaotic Maps in Spatial, Transform and Spatiotemporal Domains", *International Journal of Information Security*, Vol. 21, No. 4, pp. 917–935, 2022.

[32] J. Xu, A. H. Sung, P. Shi, and Q. Liu, "JPEG Compression Immune Steganography Using

Wavelet Transform", In: *Proc. of International Conference on Information Technology: Coding and Computing, 2004*, Vol. 2, pp. 704–708, IEEE, 2004.

[33] K. N. Singh and A. K. Singh, "Towards Integrating Image Encryption with Compression: A Survey", *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, Vol. 18, No. 3, pp. 1–21, 2022.

[34] H. Li and Y. Wang, "Double-Image Encryption Based on Discrete Fractional Random Transform and Chaotic Maps", *Optics and Lasers in Engineering*, Vol. 49, No. 7, pp. 753–757, 2011.

[35] R. Li, Q. Liu, and L. Liu, "Novel Image Encryption Algorithm Based on Improved Logistic Map", *IET Image Processing*, Vol. 13, No. 1, pp. 125–134, 2019.

[36] J. Oravec, L. Ovsenik, and J. Papaj, "An Image Encryption Algorithm Using Logistic Map with Plaintext-Related Parameter Values", *Entropy*, Vol. 23, No. 11, p. 1373, 2021.

[37] J. Gayathri and S. Subashini, "An Efficient Spatiotemporal Chaotic Image Cipher with an Improved Scrambling Algorithm Driven by Dynamic Diffusion Phase", *Information Sciences*, Vol. 489, pp. 227–254, 2019.

[38] P. N. Khade and M. Narnaware, "3D Chaotic Functions for Image Encryption", *International Journal of Computer Science Issues (IJCSI)*, Vol. 9, No. 3, p. 323, 2012.

[39] A. G. Weber, "The USC-SIPI Image Database: Version 5", *http://sipi. usc. edu/database/*, p. 2006.

[40] Y. Zhang, C. Li, Q. Li, D. Zhang, and S. Shu, "Breaking a Chaotic Image Encryption Algorithm Based on Perceptron Model", *Nonlinear Dynamics*, Vol. 69, No. 3, pp. 1091–1096, 2012.

[41] K. C. Jithin and S. Sankar, "Colour Image Encryption Algorithm Combining Arnold Map, DNA Sequence Operation, and a Mandelbrot Set", *Journal of Information Security and Applications*, Vol. 50, p. 102428, 2020.