International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 5 (2024) 67–84

Paper Type: Original Article

Fast Image Encryption Method using S-Box and Hyperchaotic System

Hala I. Mohamed [1,*], Khaled M. Hosny [1] and Osama Elkomy [1]

[1] Department of Information Technology, Faculty of Computer and Informatics, Zagazig University, Zagazig 44519, Egypt.
Emails: hala.i024@fci.zu.edu.eg; k_hosny@zu.edu.eg; omelkomy@zu.edu.eg.

Received: 01 Sep 2024 **Revised**: 02 Nov 2024 **Accepted**: 25 Nov 2024 **Published**: 30 Nov 2024

Abstract

Modern technology necessitates the transmission of millions of images between users daily. Securing these images is critical. Digital image encryption is a popular method for safeguarding image content. Chaos theory is a popular choice for image encryption due to its unpredictable and random nature. This paper proposes a cryptosystem based on the combination of 6D hyperchaotic and Chen for a more secure image encryption system; firstly, we get randomly generated variables produced by the six-dimension hyperchaotic system to confuse the original image. Secondly, bit XOR is used for more scrambling, and finally, the S-box is used for diffusion. It is dynamically generated by the Chen system with variable conditions. A novel chaotic S-box-based image encryption strategy has been developed to enhance the security and efficiency of image encryption systems ultimately. The security study and simulation results confirm the suggested scheme's effectiveness. Because of the new scheme's clear efficiency advantages and attacks, real-time image encryption may be used more effectively.

Keywords: Image Encryption; S-box; Hyper Chaotic; 6D; Compound Chaotic System; Chen's Chaotic System.

1 | Introduction

Digital Images are routinely distributed across various networks; thousands of digital images are transmitted every minute. Users of social networks seek to prevent others from accessing their images. Medical images are sensitive in healthcare networks, and their improper utilization could result in incorrect diagnosis and treatment choices. Digital images are widely used for information transmission and storage in several industries, such as medicine, education, and environmental observation. Transferring sensitive information across an insecure connection might lead to attacks. Image security during transmission has become a significant research focus [1]. The researchers suggested a variety of cipher algorithms to secure multimedia information. Using Chaos theory for image cryptography is an excellent method among these technologies. Chaotic maps are characterized by sensitivity to control parameters and beginning values, as well as ergodicity and non-convergence [2]. A good cryptography method addresses two key concepts: confusion and diffusion [3, 4]. The confusion approach involves randomly scrambling adjacent pixels, while the diffusion concept involves dispersing a minor modification in the original image's pixels over the encrypted image [5]. This review examines the literature on picture cryptography algorithms using 6D chaotic systems. N. N. Jasem and S. A. Mehdi [6] developed a new cipher algorithm that uses a hypersix-dimensional chaotic system. The algorithm uses switching, randomization, XOR operations, and diffusion in multiple phases to ensure strong

Corresponding Author: hala.i024@fci.zu.edu.eg

Licensee International Journal of Computers and Informatics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

cryptography.Zhang and Han [7] present a color image encryption scheme using a 6D hyperchaotic system, dynamic DNA coding, and image hashing. The hash series is mined using an image hashing method and serves as the chaos system's control parameter and initial value. The image's RGB values are synthesized into a two-dimensional array,then pixel replacement using an upgraded two-dimensional chaos map. Finally, the 6D hyperchaotic system generates random sequences for DNA coding and arithmetic computations. Rashid and Hussein [8] provide an efficient approach for encrypting grey and color images using a logistic 6D chaotic system and image density. The method uses an exclusive OR procedure to generate keys and encrypt images. Sun [9] proposed image encryption using random signal insertion and a 6D hyperchoice system with randomized indications and repeatedly introducing variables into the chaotic system. The totality value of all original pixels is used to generate the chaos system's starting values. Then, a pixel is separated into two equal parts. and process a larger array. Cycle shift confusion and diffusion are applied to the new array. Mehdi and Ali [10] present an image encryption and decryption system using a novel Six-dimensional hyperchaotic system. The algorithm consists of four phases: A chaotic sequence Production, Latin square, confusion, and dissemination (X). Wu et al. [11] developed a new image cryptography approach using two-dimensional DWT and a six-dimensional hyperchaotic system in spatial and frequency domains. The key sequence is based on the chaotic system and plain image. H. Mondel et al. [12] developed a sparse representation approach and 6D chaos system to identify non-zero sparse components in greyscale images using a well-trained thesaurus and RC6. Yassir and Shakir [13] proposed a combination of elliptic-curve cryptography with a 6D hyperchaos system, starting with an SHA-256 hash algorithm key. S. Sun [14] developed a method for encrypting images utilizing a 6D hyperchaotic system and inserting random signals into the system's values during repetition. The chaotic system's preliminary variables are derived from the sum of all initial pixels. Yu et al. [15] investigated a novel Hopfield neural network with 6D fractional order. Naim and Pacha [16] developed a new image cryptography that combines a 6D hyper chaos system with an upgraded Hill cipher. Modulo 257 is used to replace whole zero pixels with 256-valued pixels. John and Kumar [17] This article also reviews research on picture encryption techniques using the Fibonacci matrix. Dişkaya et al. [18] present a new cryptography system using Fibonacci polynomial matrices. Compared to the original Chen system, the Chen hyperchaotic system [19] has higher-dimensional chaotic dynamics because it is a higher-dimensional extension of the Chen system with more nonlinear components and variables. The Chen hyperchaotic system exhibits chaotic and hyperchaotic patterns with multiple unstable equilibrium points and intricate attractor systems. used a hyperchaotic system as a cipher key with 6 dimensions and range values to encrypt medical photos and 3D-printed models.

The hyper-chaotic mechanism generates key sequences with a large key space. Exploiting hyper-chaotic systems improves security performance. Color images provide more information than grey images. Encrypting color images in a timely and efficient manner is a significant problem. The authors used a six-dimensional hyperchaotic system to encrypt color images to address the limitations of tiny key spaces. The first phase involves employing a 6D hyperchaotic system to jumble the pixel coordinates in the original image. we build a fast color image encryption strategy using a unique S-Box and a complex, chaotic system. We apply real random number seeds from the surrounding noise to act as the complicated Chen system's initial values and parameters. The complex Chen system is employed to generate different parameters that are used to diffuse three color components by the bitwise exclusive operation, and one sequence is applied to create three S-Boxes to substitute each pixel's components, further adhering to another switching sequence.

S-box is the only nonlinear component among the block cryptosystem, and it has the mixing ability and good cryptographic properties of some traditional cryptosystems, such as DES, IDEA, and AES. Therefore, S-box is usually employed to design robust cryptosystems. Each block uses the same or different key stream in the block encryption system. Wang et al. [23-25] designed some novel block encryption schemes. In Ref.[23], a block encryption scheme is designed based on the high-dimension Lorenz system and perceptron model within a neural network. In ref. [24], block encryption for images using a combination of confusion and diffusion is proposed; several one-dimension chaotic maps are dynamically selected to encrypt blocks of image, in the order of the pseudo-random sequence generated by Baker map, for mutual diffusion of pixels,

the confusion is working by the pseudo-random order of route, the combination is deep-seated. In Ref. [25], a block cryptographic scheme based on the coupled chaotic map lattice is designed, and a pseudo-random number generator is constructed with the coupled spatiotemporal chaotic map lattice, which depends on the plaintext and can be easily implemented in parallel by hardware. The S-box plays an important role in the block encryption algorithm.

In recent years, some methodologies based on S-box have been designed to encrypt images. Wang et al. [26] proposed a block encryption scheme based on S-box. The S-box is generated by iterating the Tent map, the plaintext is divided into blocks and encrypted by different S-boxes, and the cipher blocks are obtained by 32 rounds of substitution and left cyclic shift. Özkaynak and Özer [27] chose the continuous-time Lorenz system to design a strong S-box. Their methodology is analyzed and tested for the following criteria: Bijective property, nonlinearity, strict avalanche criterion, output bits independence criterion, and equiprobable input/output XOR distribution. Hussain et al. have designed novel image encryption schemes based on S-box [28–31]. In Ref. [28], they designed an image encryption scheme based on the NCA chaotic system and cryptographically secure S8 AES substitution boxes. They analyzed S-box in image encryption using the root mean square error method [29], designed an image encryption algorithm based on a total shuffling scheme and chaotic S-box transformation [30], and an image encryption algorithm based on PGL (2, GF (28)) S-boxes and TD-ERCS chaotic sequence [31]. Wang et al. [32] transformed the problem of constructing an S-box into a Traveling Salesman Problem and a method based on chaos and genetic algorithm. The method fully uses the traits of the chaotic map and evolution process to obtain the stronger S-box. As a general requirement for image encryption schemes, the encrypted image should greatly differ from its original form. Two criteria can measure such differences: the number of pixel change rates (NPCR) and the unified average changing intensity (UACI) [33]. For two images with only a one-pixel difference between them, to get the ideal NPCR and UACI, two measures can be taken: one measure is to generate the keys dependent on the plain image [32], and the other is to use the avalanche effect to confuse the image ,In the 19th century, mathematician Poincaré discovered chaos in particular systems and introduced essential concepts linked to chaos. Lorentz, a meteorologist, created the Lorentz chaotic system after studying atmospheric chaos. This resulted in the rapid development of chaos theory in nonlinear dynamics [35]. Chaos theory has a strong theoretical foundation and is widely used in physics, chemistry, electronics, biology, engineering, and economics. Scholars have discovered that fractional-order chaotic systems can cause chaos. Some argue that fractional calculus, which contains fractional orders, better reflects the real world than integer orders [34], Research on fractional chaotic systems has grown significantly ,Chaotic systems exhibit unique traits such as sensitivity to initial values and unpredictability. They are ideal for Image Encryption (IE) due to their low sensitivity to beginning values and unpredictable nature [36]. This has led to the creation of many IE methods utilizing chaotic systems. One method for image encryption involves combining two chaotic systems. One system compresses images, while the other produces unpredictable sequences.

The dual-system approach to imageencryption improves security by increasing unpredictability and complexity [31]. Matthews invented the first Logistic map-based stream cipher in 1989. Chaotic systems have become increasingly popular in cryptography since then. In 1998, Fridrich used a two-dimensional Baker's map to develop a framework that conceals the link between an original and encrypted image. Simple chaotic maps are not often used in image encryption due to restrictions such as limited key space, low linear complexity, and brief repeating patterns. However, the concept of hyper-chaos can aid in overcoming these limits. Hyperchaotic systems have more than two positive Lyapunov exponents, resulting in complex patterns, increased unpredictability, and stronger randomness. Using more than four starting values leads to a larger key space for encryption systems , Integrating symmetric and asymmetric encryption techniques, a hybrid encryption solution improves data security. Fast and secure symmetric encryption and the defensive strength of asymmetric encryption are combined in hybrid encryption. Although symmetric encryption is fast, key exchange issues may arise. These problems are resolved by asymmetric encryption. However, it may be slower. Both advantages are balanced by hybrid encryption. It has drawbacks, including secure key exchange, performance, and compatibility with current systems, and its efficacy is contingent upon the particular

requirements of the system. The experimental findings demonstrate the scheme's effectiveness; the contribution of this effort is summarized as follows:

- Create image cryptosystem security via a 6D hyperchaotic system.
- Implementing numerous confusion-diffusion structures to ensure strong security.
- The 6D hyperchaotic system's huge key space is resilient to brute force attacks.
- BitXOR for more confusion, and Optimize image cryptosystem performance by combining a Chen chaotic system for generating SBOX for the diffusion step.
- Applying rationalized processes to increase complexity for the ideal encryption algorithm.

The subsequent sections are organized as follows: Section 2 covers the mathematical basics of the 6D hyperchaotic system, Chen and S-box. The cryptography algorithm is available in Section 3. In Section 4, experiments and findings are discussed. Section 5 introduces the comparison of performance. Section 6 outlines the conclusion

2 | Preliminaries

2.1 | Six-Dimensional Hyperchaotic System

Mathematical studies often illustrate that chaotic functions are nonlinear with dynamic behavior, and their responses are unpredictable. Research from the past indicates that the dynamic behavior of hyperchaotic functions is considerably more intricate than that of the correlating low-dimension chaotic functions; there should be at least four dimensions in a hyperchaotic system. Furthermore, hyperchaotic systems have at least two positive Lyapunov exponents, whereas low-dimension chaotic functions only have one. The 6D hyperchaotic system was defined by Wang and Yu [32] in Eq. (1):

$$
\begin{aligned}
&X_1 = a(X_2 - X_1) + X_4 - X_5 - X_6.\\
&X_2 = cX_1 - X_2 - X_1X_3.\\
&X_3 = -bX_3 + X_1X_2.\\
&X_4 = dX_4 - X_2X_3.\\
&X_5 = eX_6 + X_3X_2.\\
&X_6 = rX_1.
\end{aligned}
\tag{1}
$$

Where a, b, c, d, e, and rare constants; $X_1, X_2, X_3, X_4, X_5, X_6$ and X_6 refer to the state variable ر.In this paper, the constant values selected are a=10, b= $\frac{8}{3}$, c=28, d=1, e=8, and r=3.

2.2 | Chen Hyperchaotic System of Fractional-Order

Chen system was first presented by Professor Chen in 1999 [15], which can be described as follows in Eq. (2) because of its vast key space, quick pixel data scrambling, high sensitivity to initial conditions, and pseudo-randomness from deterministic chaos, the hyperchaotic Chen system is used in this work. Because of these characteristics, it is an ideal chaotic system for real-world picture encryption applications. The advantages of the hyperchaotic Chen system over other chaotic encryption systems usually result in a more reliable and safe encryption method based on this hyperchaotic system. The following is a mathematical expression for the hyperchaotic D Chen system of fractional order:

$$
\begin{aligned}
&x = a(y - x)\\
&y = (c - a)x - xz + cy\\
&z = xy - bz
\end{aligned}
\tag{2}
$$

where a, b, and c are parameters. The system is chaotic if a = 35, b = 3, and c ∈ [20, 28.4]. The dynamical property of the Chen system is more complicated than the Lorenz system, and this feature has been applied in secure communication. The initial values of $x_0, y_0\ z_0$and parameter c0 are served as keys. We use the keys to generate the initial values to enhance the randomness. Especially for the control parameter c, we make it dynamically change in the interval of [20, 28.4].

2.3 |S-Box Construction

We can employ the chaotic system with dynamical initial values and parameters for each layer to produce a unique 16 × 16 S-box. The plain image's red, green, and blue components will be encrypted. The Chen system can generate the corresponding S-box SR(i) ∈ S; the initial values and parameters are defined in Eq. (3). Similarly, for the green and blue components, the new initial values and parameters can be derived by Eqs. (4) and (5).

$$X_0'=X_0+ i* 0.001 - 0.0002 - n * 0.00002$$

$$y_0'=y_0 + i * 0.001$$

$$z_0'=z_0 + i * 0.001$$

$$c_0'=c_0+i * (28.4 - 20) * .001 - 0.0002 - n * 0.00002 \quad (3)$$

Similarly, Eqs. (4) and (5) can derive the new initial values and parameters for the green and blue components.

$$X_0'=X_0+ i * 0.001$$

$$y_0'=y_0+ i * 0.001 - 2 * 0.0002 - n * 00002$$

$$z_0'=z_0+ i * 0.001$$

$$c_0'=c_0+i * (28.4 - 20) * .001 - 0.0002 - n * 0.00002 \quad (4)$$

$$X_0'=X_0+ i * 0.001$$

$$y_0'=y_0+ i * 0.001 - 2 * 0.0002 - n * 00002$$

$$z_0'=z_0+ i * 0.001 - 3 * 0.0002 - n * 0.00002$$

$$c_0'=c_0+ i * (28.4 - 20) * .005 - 3 * 0.0002 - n * 0.00006 \quad (5)$$

The steps of generating S-box, as shown in follows.

3 |Proposed Method

We designed a chaos-based color image encryption scheme using a bijective function. First, diffuse the plain image using a 6D hyperchaotic system sequence for random rounds, then use the bit XOR operation for more diffusion. After that, it is decomposed into three components: red, green, and blue, separating each element into blocks of the same size. Generate each layer corresponding to 16 × 16 S-box by the Chen system with variable conditions, i.e., to build a bijection between the layer and the S-box set S. After substituting each layer with the paired S-box, we can get the ciphered image. Numerical simulation and security analysis demonstrate that the scheme is suitable for image encryption. Figure 1 depicts a flowchart for the proposed encryption; decryption is the inverse step of encryption.

Step 1. For each layer, generate the new initial values x'_0, y'_0, z'_0 and parameter c'_0 by Eq. (3).
Step 2. Set the initial value S(j) = j, j = 0, 1, 2, ..., 255.
Step 3. After iterating the Chen system for 300 times to eliminate the transient process, then continue to iterate it to get sequence $X = \{x_1, x_2, \ldots x_m\}$, the value of m is an indeterminate integer number, The sequence S'R(i) ∈[0,255]can be generated by the following pseudo-code.

```
j = 256; k = 0
while j ≥ 2
  k = k + 1;
   tmp = |xk | × 10 ^14;
  if int(tmp)mod j >  0
          S'R(i) (j) ↔ S'
           R(i) (int(tmp)modj);
            j = j − 1;
  end if
end
```

Step 4. Transform the sequence S'R(i) into an 16× 16 S-box SR(i) .

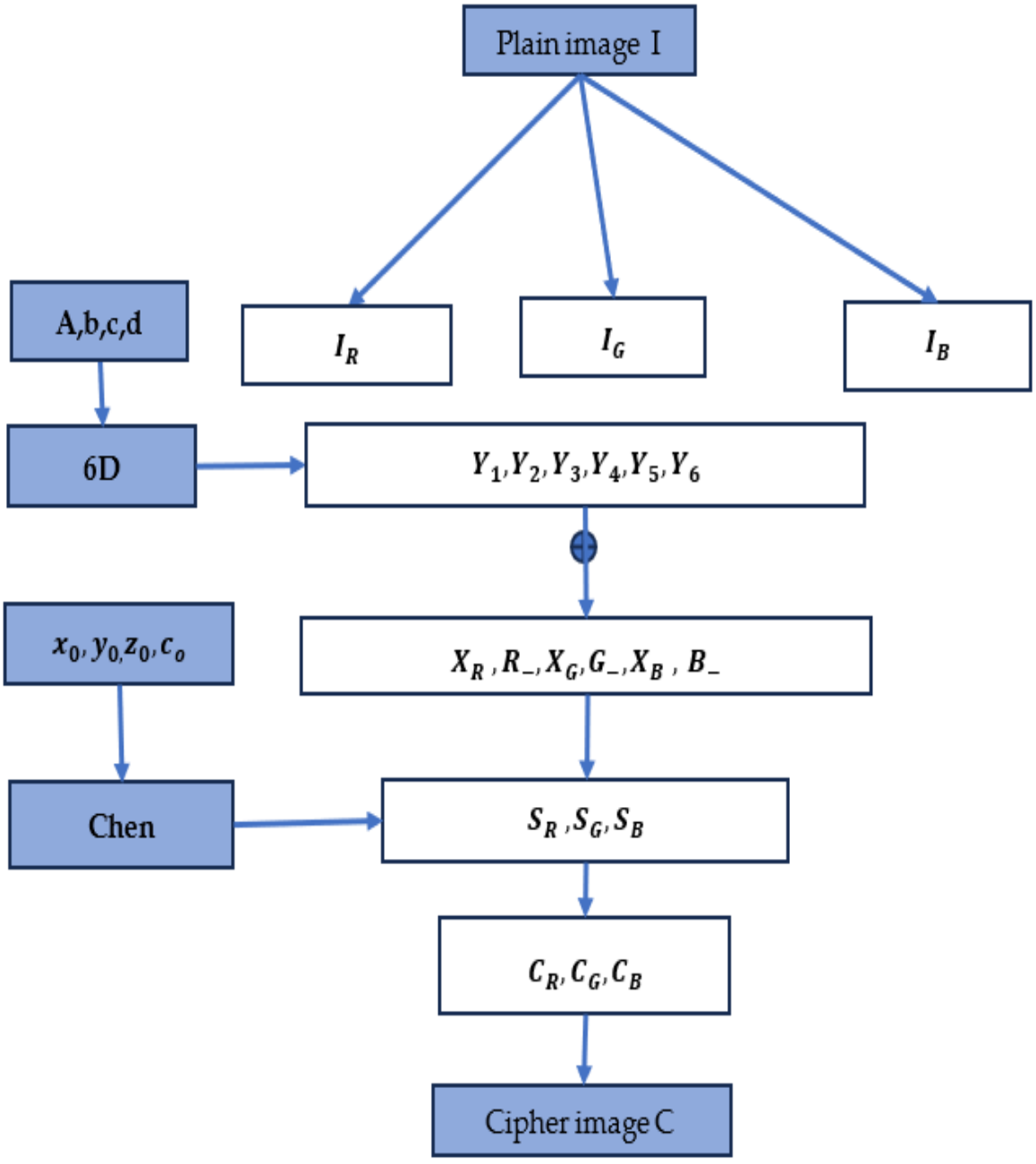


Figure 1. Flowchart Of encryption process.

3.1 | Illustrative Example of the Encryption process

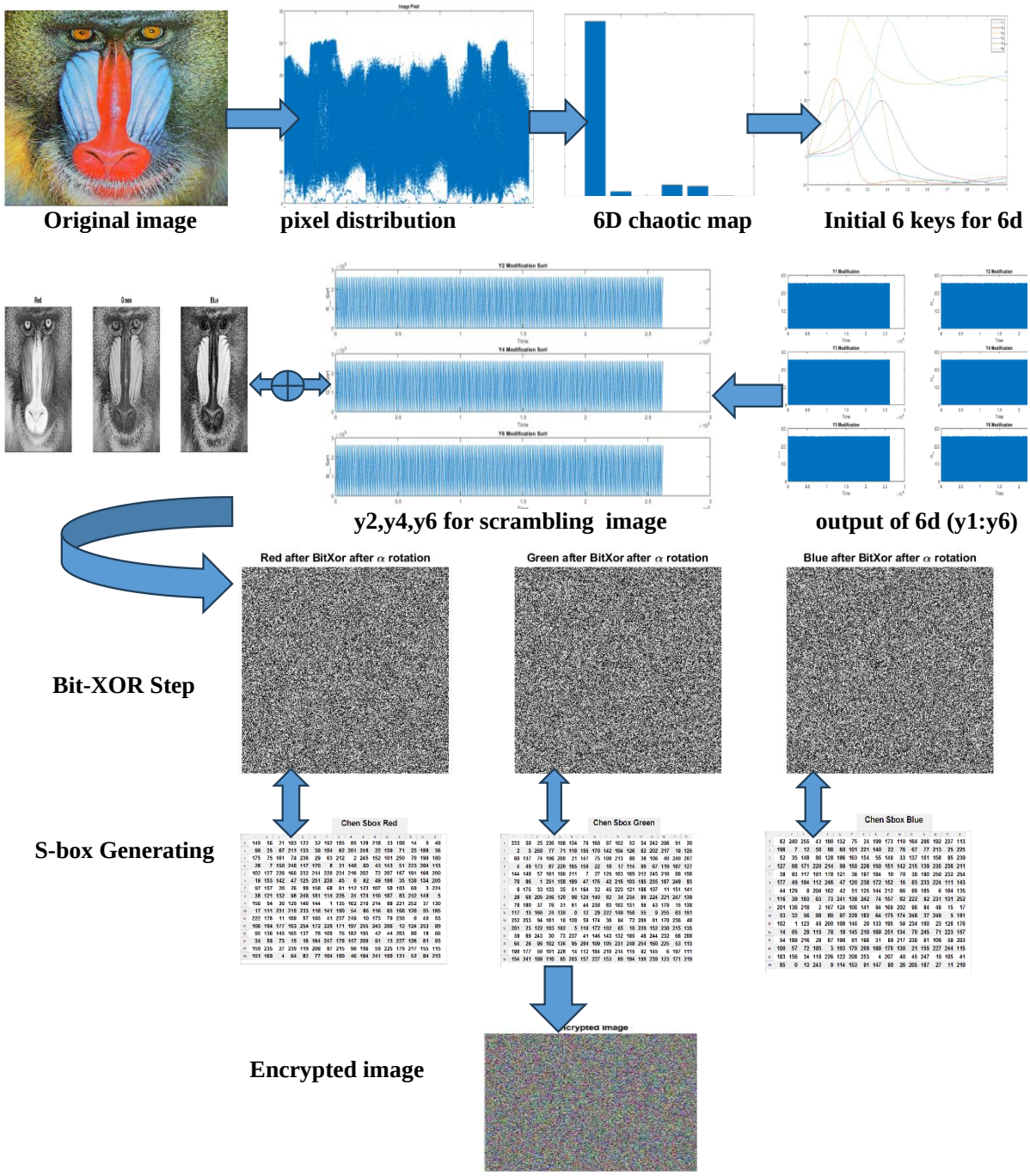


Figure 2. Illustrative example of encryption process.

3.2 | Pseudocode of Encryption Method

Input: I (I: image)

Output: C, keys (C: cipher image, keys)

3.3 | Algorithm

1. $I(MxnX3)$
2. $If\ Size(I,3)==1$ //Grayscale Image
3. $I=Set(3,I,I,I)$ //Convert I To Color Image
4. $End\ if$
5. $Transform\ the\ image\ array\ to\ a\ vector\ \mathcal{P}, \mathcal{P}=i(:)$
6. $x_1 = \frac{sum\ P(i)+(M*N)}{(M*N)+2^{23}}$
7. $FOR\ I=2:6$
8. $X_i = mod(X_{i-1} * 10^6, 1)$
9. $End\ for$
10. $Keys=[x_{1\to 6}, n_{0=(100:300)}, \alpha = random(2:8)]$
11. $Solving\ 6D\text{-}ODE$
12. $X_R = y_1$
13. $X_G = y_2$
14. $X_B = y_3$
15. $R\_ = y_4$
16. $G\_ = y_5$
17. $B\_ = y_6$
18. $\mathcal{R}=I_1, \mathcal{G}=I_2, B = I_3$
19. $FOR\ i=1:\ \alpha$
20. $\mathcal{R}=\mathcal{R}+R\_ + X_R \quad \mathcal{G}=\mathcal{G}+G\_ + X_G \quad \mathcal{B}=\mathcal{B}+B\_ + X_B$
21. $\vec{\mathcal{R}}\ reorder\ as\ R\_$
22. $\vec{\mathcal{G}}\ reorder\ as\ G\_$
23. $\vec{\mathcal{B}}\ reorder\ as\ B\_$
24. $End\ for$
25. $S_R, S_G, S_B = Chenbox(XR_{end}, XG_{end}, XB_{end}), n)$
26. $CR=SBOX(\mathcal{R}, S_R))$
27. $C\mathcal{G}=SBOX(\mathcal{G}, S_G))$
28. $C\mathcal{B}=SBOX(\mathcal{B}, S_B)$
29. $C=[C\mathcal{R}, C\mathcal{G}, C\mathcal{B}]$
30. $Outputs:\ C, Keys$

Figure 3. Pseudo-code of the encryption process.

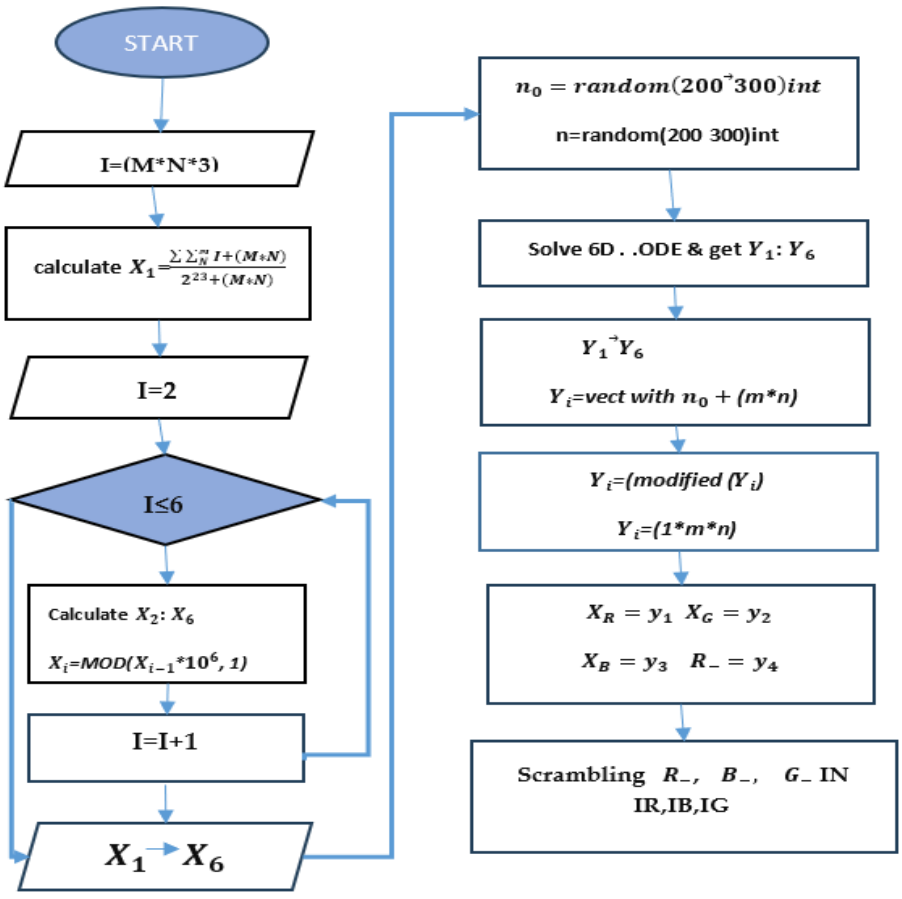


Figure 4. flowchart of the key generation process.

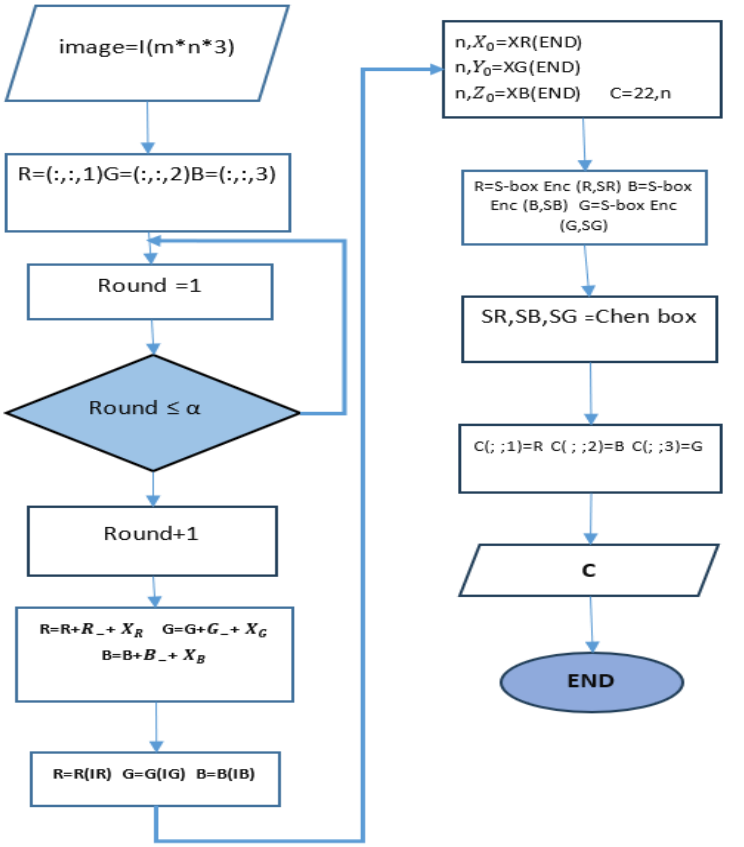
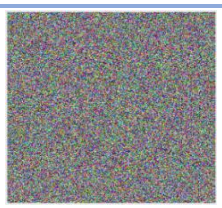
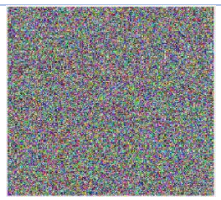
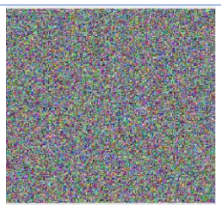


Figure 4. Flowchart of the key generation process.

Table 1. Encrypted and decrypted images.

Original image	Encrypted image	Decrypted image
		
		
		
		

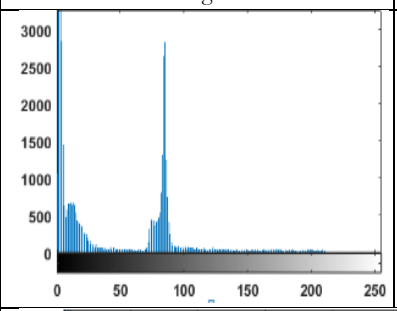
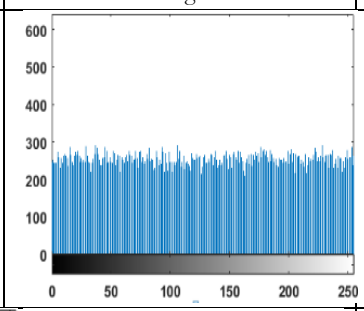
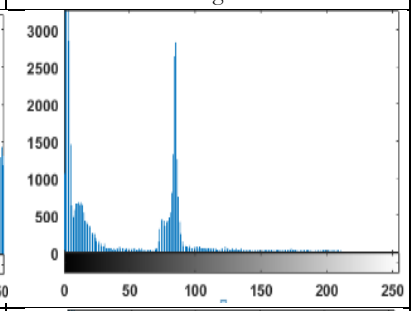
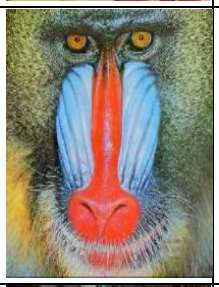
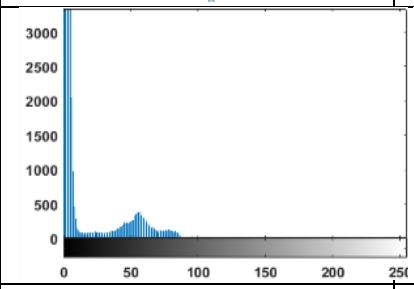
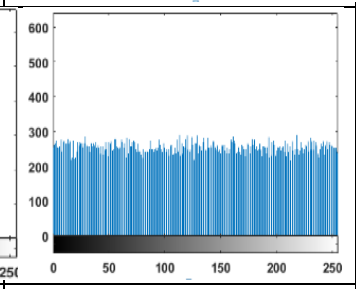
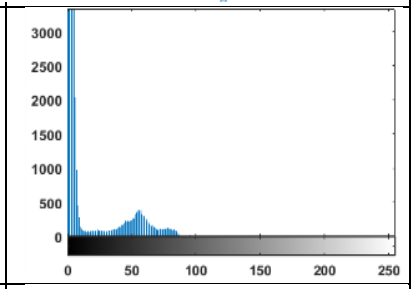
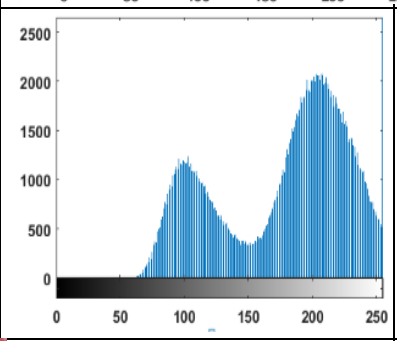
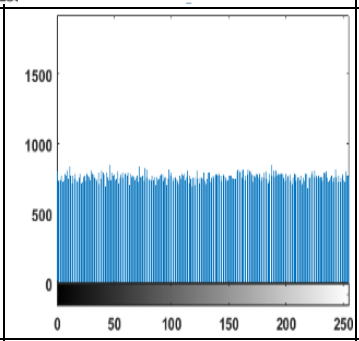
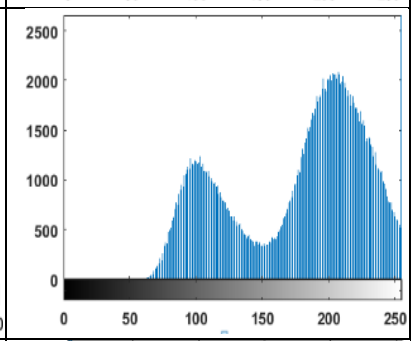
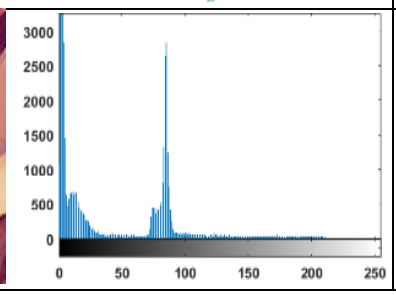
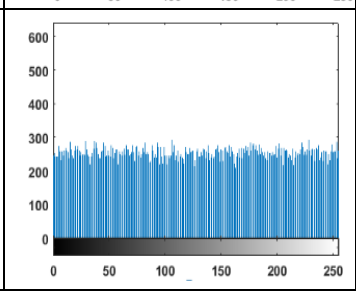
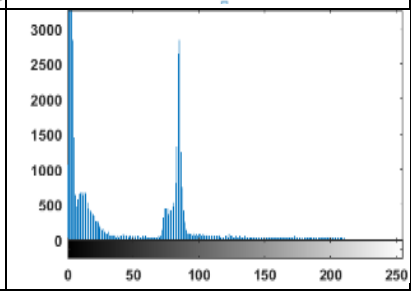
The test color images (as displayed in Table 1), test results, plain image, image after encryption, and Correspondence were decrypted.

4 | Experimental Results

4.1 | Histogram Analysis

A graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. A viewer can judge the tonal distribution by looking at the histogram for a specific image. Table 2 show Histogram analysis for image. component before encryption, component after encryption, component after decryption.

Table 2. Histogram analysis.

Original Image	Original Image Histogram	Encrypted Image Histogram	Decrypted Image Histogram
			
			
			
			

4.2 | Correlation Analysis

Correlation analysis is a statistical method used to discover if there is a relationship between two variables and how strong that relationship is. It reveals the degree of similarity between pixels in the original and encoded images. According to cryptographic techniques, neighboring pixels in the cipher image should be more connected. Table 3 displays the correlation coefficients of our structure, which were calculated in Eq. (6) using 4000 pairs of neighboring pixels selected randomly from the encrypted and plain images.

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i \ , \ D(X) = \frac{1}{N}\frac{1}{N}\sum_{i=1}^{N}(X_i - E(X)^2 \ R_{XY} = \frac{COV(X,Y)}{\sqrt{D(X)}\ \sqrt{D(Y)}} \ ,$$

$$COV(X,Y) = \frac{1}{N}\sum_{i=1}^{N}(X_i - E(X))(X_i - E(Y)) \quad (6)$$

Table 3. Correlation analysis.

Image Name	Colors	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Lena	R	-0.0111549	0.0331693	-0.0421698
	G	-0.0843582	-0.0304518	0.0352286
	B	-0.0701606	0.0261852	0.0005396
pepper	R	-0.0296002	0.0300728	0.0239084
	G	0.002747	0.0341719	-0.0332402
	B	-0.0241718	0.0468803	-0.0441189
baboon	R	0.031172	0.0155458	0.00557623
	G	0.025667	-0.0323875	0.00067505
	B	0.015855	0.02468973	0.02156940
couples	R	0.038053	-0.0285643	-0.01221959
	G	0.028516	-0.0341566	0.038880164
	B	0.068037	0.05038351	0.000342514

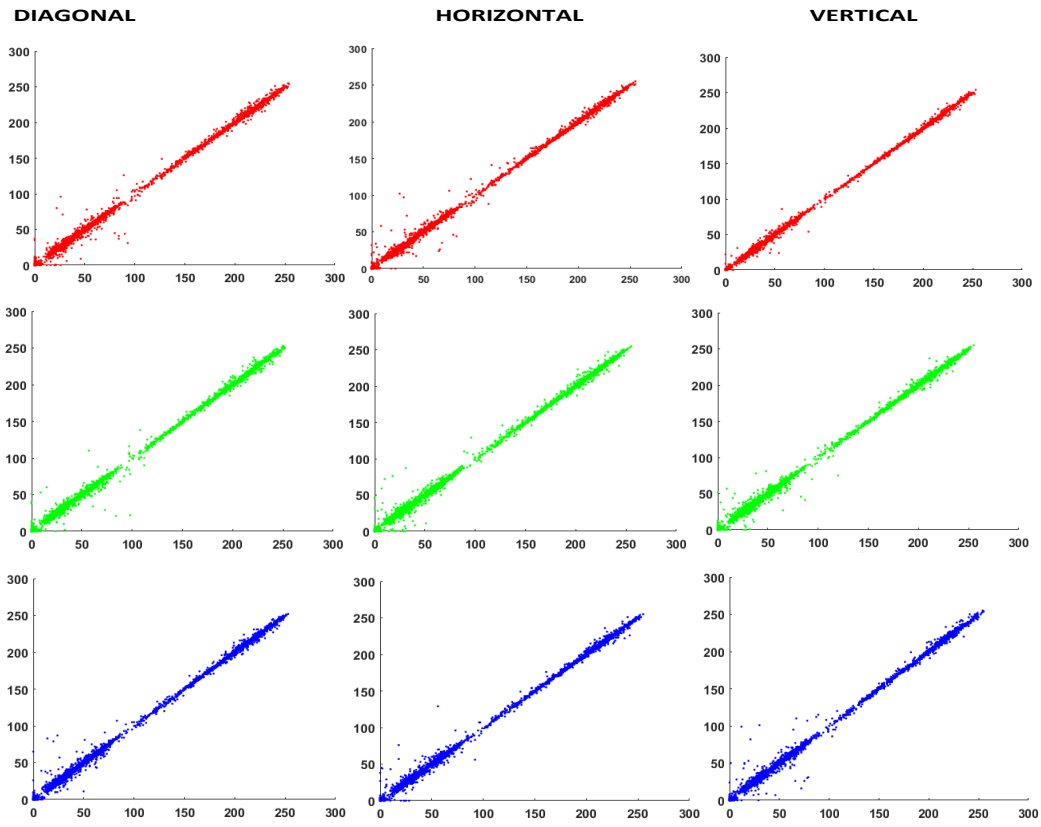


Figure 5. Correlation Analysis in the directions for Lena before encryption.

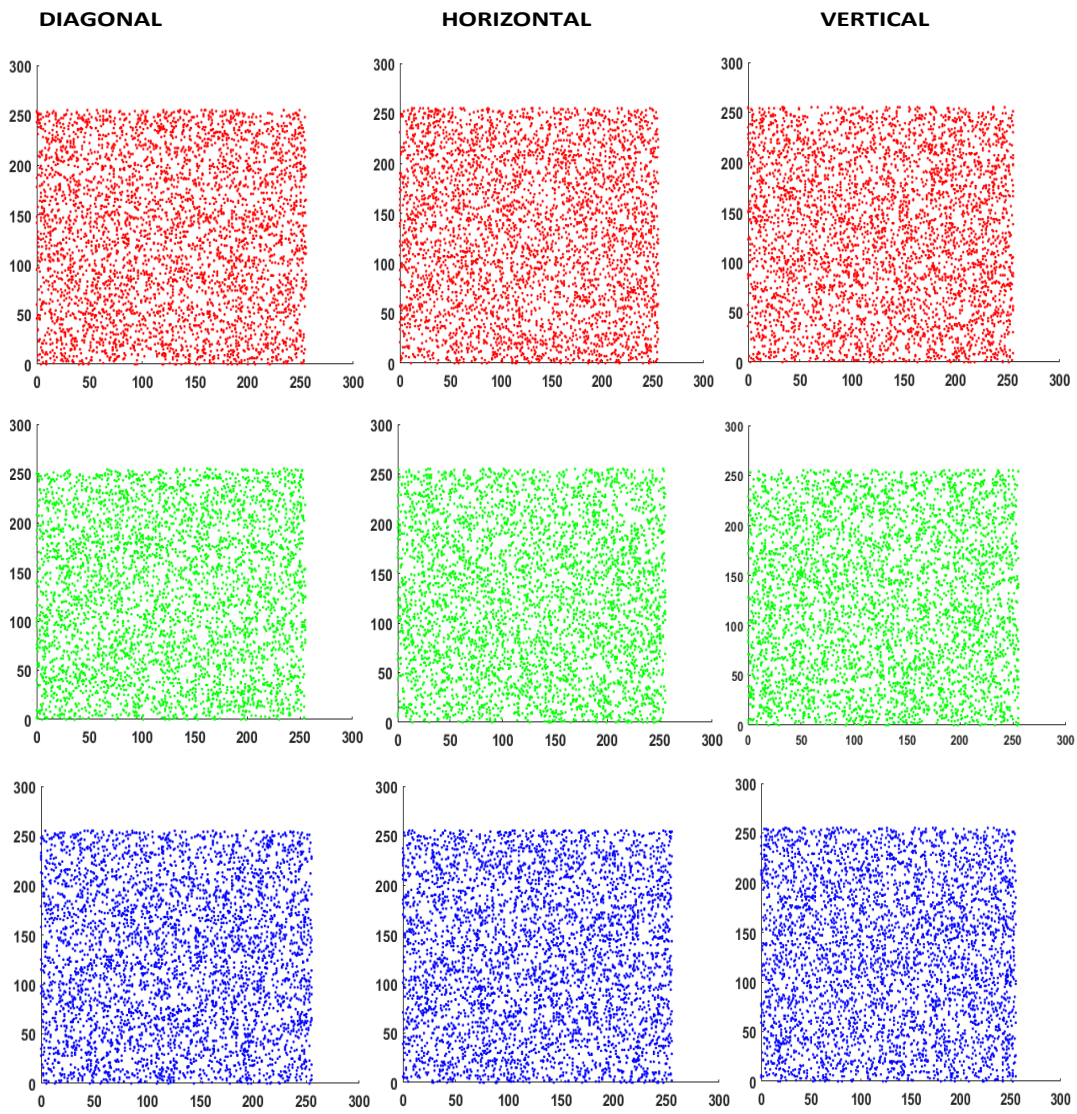


Figure 6. Correlation Analysis in the directions for Lena after encryption.

4.3 | Information Entropy

The information's entropy impacts how unpredictable things appear in the image. Information entropy should have a maximum value of 8, as shown in Eq. (7). Where r and P (ri) represent the information source and the probability of the ri sign, Table 2 shows the entropy results.

$$H(m) = \sum_{i=0}^{2^N-1} p(ri)\log_2 \frac{1}{p(mi)} \quad (7)$$

When determining the true unpredictability of an image, the global entropy may not always be reliable. Likely, the global entropy approach's assessment of extremely high entropy levels around the maximum does not adequately capture the underlying randomness of the two images. To address the global entropy problem, recognizable and random images can have the same global entropy. Wu et al. (2013) proposed using the local Shannon entropy, which is determined by averaging a random sample of non-overlapping image blocks' local entropy. As represented mathematically, it is as follows in Eq. (8).

$$H_{m.I_g}(S) = \sum_{i=1}^{n} \frac{H(S_i)}{n} \quad (8)$$

Table 4. Entropy analysis.

Image	Local	Entropy
Lena	7.102593218	7.99932092
Baboon	7.095249575	7.999328863
Pepper	7.108024409	7.999328863
Couple	7.116643678	7.999328444

4.4 | Differential Attack Analysis

The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are used to measure the sensitivity of the encryption system to minor changes, which are important indicators to test differential attacks, specifically speaking, the differential attack to make a small change to a pixel of the plain image and detect its impact on the ciphertext image. The mathematical expressions of NPCR and UACI are the arbitrary pixel values of the color image that are randomly selected, and the NPCR and UACI values are calculated and repeated 200 times to obtain an average value finally. Table 5, the NPCR measures the number of pixels that are different between two images. It is mathematically expressed as:

$$\text{NPCR} = \frac{\sum_{i,j} D_{i,j}}{M \times N} \times 100 \tag{9}$$

$$D_{i,j} = \begin{cases} 0, C_{1(i,j)} = C_{2(i,j)} \\ 1, C_{1(i,j)} \neq C_{2(i,j)} \end{cases} \tag{10}$$

The Unified Average Change Intensity (UACI);

The UACI measures the difference in the average intensity between the encrypted and plain images. It is mathematically expressed.

$$\text{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255} \tag{11}$$

Where M &N are the length and width of the image, C_1 &C_2 are encrypted and modified images.

Table 5. NPCR and UACI attacks analysis.

	Lena	Baboon	Peeper	Couples
UPCR	99.6167501	99.597168	99.6054331	99.6054331
UACI	30.4521069	33.8478693	32.2936917	33.2936917

4.5 | Attack Analysis

4.5.1 | Noise Attack

Noise interferes with the encrypted image when broadcast over a noisy channel. The scheme's efficiency is defined by its noise resistance and the trustworthy receiver's ability to recognize the image after decoding. The proposed method is validated by introducing salt and pepper noise with density (0.05, 0.5) and Gaussian noise with variance (0.01, 0.1) into an encrypted image properly decoded using the correct key. Figure 8 show encrypted and decoded images. Figure 8 shows salt and pepper noise (0.002) and salt and pepper noise (0.005) in the encrypted image.

Figure 7. Noise attack with 002 and 005 before and after the attack.

4.5.2 | Data Cut Attack

Images transmitted over the network are vulnerable to noise or cropping (data cut). Successful image encryption algorithms should be robust against these attacks. The well-known measure, PSNR (peak signal-to-noise ratio), is used to mathematically evaluate the decrypted image quality for original and decrypted images. In Figures 9 and 10, we apply data cut with 128*128 and a circle with a radius 75.

Figure 9. Data cut attack before and after with circle. **Figure 8.** Data cut attack 128*128 before and after.

Table 6. Data cut and noise attack analysis.

Noise type	Peak_SN_1	Peak_SNR_2	Peak_SNR_3
SNP D=0.002	31.2237999	33.51049049	31.41920998
SNP D=0.005	27.5675073	30.18587825	26.64888536
Data Cut 128*128	13.2668872	16.07270294	12.8715033
Data Cut 64*64	19.2934996	22.04733239	18.84840079

The experimental findings, shown in Table 6, show that our technique is particularly effective at recovering encrypted images after noise and data cut attacks.

The PSNR: The Peak Signal-to-Noise Ratio (PSNR), which evaluates image quality, is mathematically defined by the mean square error (MSE), as shown in Eqs. (12) and (13).

Table 7 presents the MSE and PSNR values for the recommended method.

$$\text{PSNR}= = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \tag{12}$$

$$\text{MSE} = \frac{1}{\text{MN}}\sum_{i=1}^{M}\sum_{j=1}^{n}|I_0(i,j) - I_D(i,j)|^2 \tag{13}$$

Where I_0 : original image, I_D : encrypted image. PSNR values correlate closely with image quality; high values indicate high similarity between the original and decrypted images. The results show that the PSNR and MSE values for encrypted are low and plain images are large, providing the method's greater effectiveness and security. Discerning the difference between the original and decrypted images becomes difficult when the PSNR value exceeds 35. In Table 6, we conduct the following tests on the encrypted image to determine if the proposed technique can withstand these attacks: (1) now add "salt & pepper" noise (SPN) at 0.002 and

0.005 densities. (2) Cut attack by cropping in the left corner using 64 × 64 and 128 × 128 sizes. The ability to recognize image contents despite attacks demonstrates the resilience of our approach against noise and data cutoff attacks.

Table 7. MSE and PSNR results.

Images	MSE	PSNR
Lena	8955.3619	6.718248602
Baboon	8144.755505	9.056311238
Pepper	10294.53734	8.039421003
Couple	6766.041889	8.787299716

Table 8. Comparison with recent encryption methods for the encrypted Lena.

Method	ENTROPY	PSNR	MSE	NPCR	UACI
proposed	7.999314982	8.63973	8955.3619	99.6167501	30.4521069
33	7.99906	8.6285	8917.24	99.5926	30.3921
34	7.99887	8.63086	8912.4	99.5855	30.3873
35	7.9856	8.53462	9112.1	99.625	30.5681

4.6 | Time Complexity

The execution time results for several photos' encryption and decryption procedures are shown in Table 9. The Table 10 shows the encryption time, decryption time, and total time in seconds (s) for every image.

Table 9. Encryption and decryption time.

Size	Encryption time	Decryption Time	Total time
64*64	0.0080451	0.0110167	0.019062
128*128	0.0160739	0.0194619	0.035536
256*256	0.0721034	0.0715967	0.1437
512*512	0.2122354	0.2473213	0.459557

Table 10. Comparison between other methods for encryption time Lena 256.

Image	Encryption time	CPU and MEMORY
proposed	0.0721034	2.80GHz Intel® Core™ i7, 16 GB
[33]	0.021658	3.3 GHz AMD® Ryzen 9 5900HX, 32 GB
[34]	0.426243	2.9 GHz Intel® CoreTM i9, 32 GB
[35]	1.42545	2.9 GHz Intel®CoreTM i9, 32 GB

Encryption time comparison of multiple algorithms from recent literature for a 256 × 256 Lena image.

5 |Conclusion

In this paper, a chaos-based color image encryption scheme using a bijective function is designed. Each component of the color image is divided into blocks with the same size. For each block, a one-to-one corresponding 16 × 16 S-box is generated to substitute it. To ensure the bijection between block set B and S-box set S, the initial values and parameters for the Chen system are designed to change dynamically with the component number and the block number. Performance analysis shows that the S-boxes can meet all the testing criteria. Numerical simulation and security analysis demonstrate that the scheme is suitable for image encryption. The outcome of this research work is that it is found in all applications for secure data transfer.

A 6D hyperchaotic system operates in a six-dimensional phase space. This high dimensionality provides a large parameter space, making it more challenging for attackers to predict and reverse-engineer the encryption process. Highly nonlinear differential equations characterize hyperchaotic systems. This nonlinearity adds an extra layer of complexity to the encryption process, making it more resistant to standard cryptanalysis techniques. The randomness and unpredictability of hyperchaotic systems make them resistant to various statistical attacks, such as frequency analysis or correlation attacks. As we have seen from this work, a six-dimensional hyperchaotic system characterized by multiple positive Lyapunov exponents, indicating highly complex and unpredictable dynamics, was used for the encryption images. This 6D hyperchaotic system had a higher level of complexity and intricacy in its behavior, making it valuable for studying nonlinear dynamics and complex systems. The unpredictable nature of hyperchaotic systems is advantageous for information security applications, such as cryptography, as it makes it difficult for adversaries to decipher encrypted information. Also, the larger parameter space of a 6D hyperchaotic system provides more flexibility and control in shaping the system's behavior. The performance validation by metrics revealed the proficiency of the 6D hyperchaotic encryption model.

Acknowledgments

The authors are grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors

References

[1] Sun, C., Wang, E., & Zhao, B. (2021). Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyperchaotic system and plaintext-related scrambling. Entropy, 23(3), 291. https://doi.org/10.3390/e23030291

[2] Khairullah, M. K., Alkahtani, A. A., Bin Baharuddin, M. Z., & Al-Jubari, A. M. (2021). Designing 1D Chaotic Maps for Fast Chaotic Image Encryption. Electronics, 10(17), 2116. https://doi.org/10.3390 /electronics10172116

[3] Jasem, Narjes & A. Mehdi, Sadiq. (2023). Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System. International Journal of Intelligent Engineering and Systems DOI:10.22266/ijies2023.1031.49

[4] Jasem, N.N., Mehdi, S.A.:((2023). Multiple random keys for image encryption based on sensitivity of a new 6D chaotic system. Int. J. Intell. Eng. Syst. 16(5), 576–585 https://doi.org/10.22266/ijies2023.1031.49

[5] Hua, Z. Zhou, Y. and H. Huang, (2019). "Cosine transform-based chaotic system for image encryption", Inf. Sci. (NY), Vol. 480, pp. 403419, https://doi.org/10.1016/j.ins.2018.12.048

[6] Sahasrabuddhe,A& Laiphrakpam,D(2023) "Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System", Int. J. Intell. Eng. Syst., Vol. 16, No. 5, pp. 576-585 https://doi.org/10.1016/j.ins.2020.10.031

[7] Zhang, Q., & Han, J. (2021). A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding. Multimedia Tools and Applications, 80(9), 13841-13864 https://doi.org/10.1007/s11042-020-10437-z

[8] Rashid,A&Hussein,KH (2023.) Electr. Comput. Eng., Vol. 13, No. 2, pp. 1903-1913, http://doi.org/10.11591/ijece.v13i2.pp1903-1913

[9] Sun, S. (2023,)"A New Image Encryption Scheme Based on 6D Hyperchaotic System and Random Signal Insertion", IEEE Access, Vol. 11, No. June, 10.1109/ACCESS.2023.3290915

[10] Mehdi, S. &. Latif , Z, 2020. "Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper- Chaotic System", Al-Mustansiriyah J. Sci., Vol. 31, No. 1, pp. 54-63, 2020. DOI:10.23851/mjs.v31i1.739

[11] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system", Inf. Sci. (NY)., Vol. 349-350, pp. 137-153, 2016.

[12] MONDAL, H., PATHAK, ET AL(2023) Sparse Based Image Encryption Using 6D-Chaotic System and RC6", Sci. Cult., Vol. 89, No. November December, pp. 400-405,. I: https://doi.org/10.36094/sc.v89.2023.

[13] Yassir, S. andshakir,H (2023)Shakir, "Hybrid Image Encryption Technique for Securing Color Images Transmitted Over Cloud Networks", Int. J. Intell. Eng. Syst., Vol. 16, No. 6, pp. 850-862, DOI:10.22266/ijies2023.1231.70

[14] Yu, F. et al., (2022.) "A 6D Fractional-Order Memristive Hopfield Neural Network and its Application in Image Encryption", Front. Phys., Vol. 10, No. March, pp. 1-14, 10.3389/fphy.2022.847385. https://doi.org/10.3389/fphy.2022.847385

[15] M. Naim and A. A. Pacha, "A Novel Image Encryption Algorithm Based on Advanced Hill Cipher and 6D Hyperchaotic System", International Journal of Network Security, Vol. 25, No. 5, DOI:10.6633/IJNS.202309_25(5).13

[16] John, S.& Kumar, S. (2023). "6D Hyperchaotic Encryption Model for Ensuring Security to 3D Printed Models and Medical Images", J. Image Graph., Vol. 12, No. 2, pp. 117-126, doi: 10.18178/joig.12.2.117-126 117

[17] Dişkaya, O, Avaroğlu, E.(2022.)"A New Encryption Algorithm Based on Fibonacci Polynomials and Matrices", Trait. du Signal, Vol. 39, No. 5, pp. 1453-1462, https://doi.org/10.18280/ts.390501

[18] Abdel-Aziz MM, Hosny KM, Lashin NA (2021) Improved data hiding method for securing colorimages. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-10217-9

[19] Ali TS, Ali R (2020) A new chaos based color image encryption algorithm using permutation substi-tution and Boolean operation. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-08850-5

[20] Roy S, Shrivastava M, Vinodkumar C, Kumar S, Umashankar N (2020) IEVCA: an efficient imageencryption technique for IoT applications using 2-D Von-Neumann cellular automata. Multimed ToolsAppl 1–39. https://doi.org/10.1007/s11042-020-09880-9

[21] Xiang H, Liu L (2020) An improved digital logistic map and its application in image encryption. Mul-timed Tools Appl. https://doi.org/10.1007/s11042-020-09595-x

[22] Khan M, Shah T, Batool SI (2015) Construction of S-box on chaotic Boolean function and its application in image encryption. Neural computing and application, https://doi.org/10.1007/s 00521-015-1887

[23] Alexan, W. Elkandoz, M.et(2023) "Color image encryption through chaos and kaa map," IEEE Access, vol. 1pp. 11 541–11 554 10.1109/ACCESS.2023.3242311

[24] Gong, M., Chai, X., Lu, Y., & Zhang, Y. (2024). Exploiting Four-Dimensional Chaotic Systems with Dissipation and Optimized Logical Operations for Secure Image Compression and Encryption. IEEE Transactions on Circuits and Systems for Video Technology.10.1109 /TCSVT.2024.3375868

[25] Mandangan, A., & Ying, I. L. J. (2024). Chaotic Encryption Scheme for Colour Image using 3D Lorenz Chaotic Map and 3D Chen System. International Journal of Computational Thinking and Data Science, 1(1), 10-24. https://doi.org/10.37934/CTDS.1.1.1024

[26] Alexan, W., Gabr, M., Mamdouh, E., Elias, R., Aboshousha, A.: (2023) Color image cryptosystem based on sine chaotic map, 4d chen hyperchaotic map of fractional-order and hybrid dna coding. IEEE Access 11, 54928–54956

[27] Li, Z., Yang, S., Tan, W. et al. A remote sensing image encryption and compression scheme using novel hyperchaotic system and plaintext related random S-box. Nonlinear Dyn (2024). https://doi.org/10.1007/s11071-024-10317-3

[28] Monu Singh, Naman Baranwal, K.N. Singh, A.K. Singh, Huiyu Zhou,Deep learningbased biometric image feature extraction for securing medical images through data hiding and joint encryption–compression,Journal of Information Security and Applications,Volume 79,2023,103628,ISSN 2214-2126, https://doi.org/10.1016/ j.jisa.2023.103628.

[29] Venkatesh J, Pchelintsev AN, Karthikeyan A, Parastesh F, Jafari S. A fractionalorder memristive two-neuron-based hopfield neuron network: dynamical analysis and application for image encryption. Mathematics 2023;11:4470. https://doi.org/ 10.3390/math11214470

[30] Saeed Ullah, Xinge Liu,(2024),An efficient construction of Sbox based on the fractional-order Rabinovich–Fabrikant chaotic system, Integration,Volume94, ,102099,ISSN 0167-9260,https://doi.org/10.1016/j. vlsi.2023.102099.

[31] Vijayakumar, M. Ahilan, A(2024)An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map,Ain Shams Engineering Journal,Volume 15, Issue 4,102620,ISSN 2090-4479,https://doi.org/10.1016/j.asej.2023.102620.

[32] Alexan, W. L. Chen, Y.- (2023.) Hyperchaotic maps and the single neuron model: A novel framework for chaos-based Image Encryption, Apr. 2023. doi:10.20944/preprints

[33] W. El-Damak, and Gabr, M. "Image encryption based on Fourier-DNA coding for hyperchaotic Chen system, Chen-based binary quantization s-box, and variable-base modulo operation," IEEE Access, Feb. 2024. DOI: 10.1109/ACCESS.2024.3363018.

[34] Alexan, W. Alexan, N. 2023 "Multiple-layer image encryption utilizing fractional-order Chen hyperchaotic map and cryptographically secure PRNGs," Fractal and Fractional, vol. 7, no. 4, p. 287, Mar.. DOI: 10.3390/fractalfract7040287

[35] Gabr, M Younis, H. et, 2022. "Application of DNA coding, the Lorenz differential equations and a variation of the logistic map in a multi-stagecrypto system," Symmetry, vol. 14, no. 12, p. 2559, Dec. DOI: 10.3390/sym14122559.