JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 6 No. 1 (2025) 347-358
https://publisher.uthm.edu.my/ojs/index.php/jscdm

Enhanced Image Encryption Using Pixel-Block Permutation and Multi-Chaotic Maps with DNA-Based Diffusion

Merdin Shamal Salih[1]*, Subhi R. M. Zeebaree[2]

[1] *Department of Information Technology, Technical College of Informatics, Akre University for Applied Sciences, Akre, Kurdistan Region, IRAQ*

[2] *Energy Engineering Department, Technical College of Engineering, Duhok Polytechnic University, Duhok, Kurdistan Region, IRAQ*

*Corresponding Author: merdin.shamal@auas.edu.krd

DOI: https://doi.org/10.30880/jscdm.2025.06.01.023

Article Info

Received: 2 May 2025
Accepted: 8 June 2025
Available online: 30 June 2025

Keywords

Color image encryption, pixel-block scrambling, chaotic maps, DNA encoding, diffusion and confusion process

Abstract

As differential and statistical attacks become more prevalent, enhancing image encryption is a significant concern. The proposed method in this study implements dual security enhancement by integrating pixel-level techniques with block-level modifications while utilizing Hénon for the red channel and Logistic for both the green and blue channels to achieve encryption. The encryption algorithm begins by dividing the image into four main blocks before performing multiscale scrambling of increasing sub-blocks through permutation. This approach aims to enhance confusion and diffusion by mixing the data through multilevel chaotic scrambling. The encryption process incorporates pixel-level confusion, subsequently followed by block scrambling to maximize the scrambling effect and complexity. During diffusion, the confused image undergoes two operations, including DNA encoding and XOR operations, to create robust data protection methods. Experimental results demonstrate that the proposed algorithm achieves strong encryption, evidenced by a high entropy value, minimal correlation, and key change sensitivity, verifying its resistance to differential and statistical analysis attacks. In conclusion, the method provides both good speed and security, making it a suitable choice for protecting and distributing images.

1. Introduction

The advancement of communication technology and the emergence of the big data era have increased the importance of visual information in the online information landscape. This shift has made visual data the primary mode of interaction in social engagements [1]. The protection of digital images during transmission and storage has garnered considerable attention across various sectors, particularly in big data, healthcare, aerospace, and military applications. This field is crucial within information security. Unauthorized access, exploitation, or interruption of network data incurs financial costs for computer users and poses a significant threat to social and national security. Consequently, the study of image encryption has gained more relevance. A multitude of innovative image encryption methods have surfaced, with chaos-based techniques presenting a viable option. The use of chaotic system properties for data encoding has become a key research area in computer science. The attributes of chaotic systems, such as sensitivity to initial conditions, unpredictability, parameter sensitivity, and strong global stability, render them suitable for image encryption [2, 3].

Cryptography is a recognized method for safeguarding sensitive information. In cryptography, both pictures and text undergo encryption before transmission over the network. Encryption techniques vary from text encryption algorithms due to the intrinsic characteristics of picture pixels, which exhibit considerable correlation and redundancy. Information encryption is the process of transforming sensitive data into an incomprehensible format to obscure its meaning. Research on privacy protection for digital images reveals that digital photos intrinsically include private and sensitive information. The primary objective is to convert plaintext data in digital images into a noise-like format, rendering it unintelligible and preventing the attacker from deciphering the ciphertext image without the necessary key, thereby ensuring the security of image data encryption [4], [5].

Chaos-based encryption methods have shown significant efficacy in safeguarding digital photos. This performance is ascribed to the unique characteristics of chaotic systems, including nonlinearity, heightened sensitivity to initial conditions, pseudo-randomness, and non-periodicity. Scrambling and dispersion constitute the essential mechanisms of all encryption methodologies. The scrambling process alters pixel positions, while the diffusion process modifies pixel values. The exclusive use of either scrambling or diffusion in image cryptosystems compromises security; thus, both methods must be used concurrently to meet the necessary security standards [6, 7]. The employment of low-dimensional chaotic systems (i.e., 1D or 2D) poses a significant risk to these processes, potentially compromising the cryptosystem due to the increased likelihood of cryptographic key inference, restricted periodicity, and limited key space. Nonetheless, chaotic systems in higher dimensions (3D or more) include many parameters, intricate structures, extensive key spaces, and heightened sensitivity, making the decryption of picture cryptosystems a daunting challenge [8].

Confusion and dispersion are the two primary approaches used to facilitate image encryption. Due to its ease of implementation and positive outcomes, diffusion is a common procedure. As stated in reference [9], the purpose of diffusion is to change the value of each pixel in an image. A classical framework based on a chaotic system serves as the foundation for the image encryption strategy that employs confusion and dispersion. In light of this, the primary components of visual encryption are the stages of confusion and diffusion. During the confusion phase, the positions of the pixels are altered, while in the diffusion phase, the values of the pixels are changed, causing them to move in relation to one another. Confusion and dispersion work together to enhance the security of encryption systems. However, some cryptosystems remain vulnerable to compromise. Existing encryption methods face various issues, including a limited number of keys, inadequate information distribution, or sensitivity to attacks that utilize statistical or input variations.

Insufficient consideration is given to the performance of chaotic dynamics throughout the algorithm creation process, which explains this. The design of the encryption and the performance of chaotic maps are the two most important factors determining the effectiveness and security of a chaos-based encryption technique [10]. DNA computing is a technology used in security due to its extraordinary parallelism, large storage capacity, and minimal processing resource requirements. One of the most notable areas of recent research is the use of DNA sequences and DNA computing for image encryption [11]. DNA encodes information, and this information is encrypted using modern biological processes. However, DNA encoding is not a suitable method for encrypting and protecting photographs. As the DNA encryption method can encrypt information vital for sophisticated biological research, the cost of information encryption has increased [12].

This paper suggests a new algorithm for image encryption that combines multi-chaotic maps, scrambles blocks and pixels, and employs methods similar to those found in DNA diffusion to enhance both security and efficiency. The main contributions of this work are as follows: (i) Merging the strategies of scrambled pixels and blocks with chaotic maps (Hénon, Logistic, and Lorenzo) specifically designed for the RGB channels. (ii) A combined encryption approach utilizing pixel-based encryption, confusion at the block level, and diffusion with DNA for increased robustness. (iii) An analysis was conducted to determine whether the algorithm prevents statistical and differential attacks using entropy, correlation, and sensitivity tests.

This paper presents a new image encryption method that utilizes three distinct chaotic maps: the Hénon map for the red channel, the Logistic map for the green channel, and the Lorenzo map for the blue channel. The process begins with pixel scrambling through a sequential displacement method starting at the image core, followed by random block scrambling as a second stage. The system employs DNA rules and logical modifications to encode images through a diffusion process, resulting in the final encrypted output. Strong security is achieved by combining pixel and block scrambling techniques with chaotic key generation methods, providing high resistance against various types of attacks. The paper thoroughly demonstrates the proposed system, including experimental results and a security evaluation.

For the remainder of the paper, Section 2 provides a summary of related work. Section 3 explains how the methodology will be applied. Section 4 discusses the testing conducted and gives a detailed security overview. The paper concludes with Section 5, which outlines the future work to be done next.

2. Related Works

Prior methodologies may be categorized into two groups according on the characteristics of the scrambling method. The major objective is to maintain the original dimensions of the image. Certain study modified the basic representation by augmenting the Arnold map. The preliminary values derived from the chaotic map correspond with the pixel coordinates. The updated arrangements of the pixels are determined by repeating the chaotic system. The encryption model devised by Hosny et al. [13] has two fundamental processes: diffusing image pixels through the logistic map for color images and rearranging pixels employing the block scrambling approach. Teng et al. [14] used logistic and sine maps to develop a two-dimensional hyperchaotic map and a cryptographic encryption technique for grayscale pictures. Erkan et al. [15] used a 2D Schaffer hyperchaotic model to develop a framework for color picture encryption and decryption, including permutation and diffusion techniques. Wang et al. [16] used a 4D chaotic system and a DNA sequence to develop an encryption technique for color pictures. Yan et al. [17] examined an image encryption method via a 4D hyperchaotic model for color images. Li et al. [18] developed a framework for image encryption by integrating a DNA sequence with a novel 5D hyperchaotic system.

Wang et al. [19] integrate a four-dimensional chaotic system with DNA technology to create a color picture encryption technique. The approach transforms each pixel value into two 4-bit binary values for WSSM scrambling. The suggested 4D chaotic system generates four chaotic sequences to elucidate the principles of DNA encoding, decoding, and computation. The three matrices of Red, Green, and Blue are partitioned into blocks and randomized. Security evaluations involve histogram analysis, key sensitivity assessment, entropy measurement, correlation analysis, resistance to differential attacks, noise attacks, occlusion attacks, and other factors.

Wang et al. [20] provide a color picture encryption technique that incorporates novel elements based on a two-dimensional discrete memristor logistic map (2D-MLM), Deoxyribonucleic acid (DNA) encoding, and multi-wing hyperchaotic systems. The discrete memristor map and the four-wing hyperchaotic system are used to produce diverse pseudo-random sequences. Secondly, the initial picture undergoes processing in segments, with DNA encoding and procedures executed on the sub-segment image using different pseudo-random sequences. Eventually, by incorporating the pseudo-random sequence to obfuscate the sub-block picture and DNA decoding, we get the encrypted image. The approach generates a distinct key for each picture and utilizes multiple sub-keys to expand the key space. The use of multiple pseudo-random sequences for image scrambling effectively mitigates the security concerns associated with the use of a single chaotic sequence.

Lone and Qureshi [21] introduced an innovative color picture encryption method using symmetric keys, which incorporates the Arnold transform, a 3D logistic chaotic map combined with XOR operation, and the affine hill cipher algorithm. All three technologies work together to provide robust encryption, preventing unauthorized access to data.

Several shortcomings have been identified in prior studies. Keys can be obtained by analyzing a collection of photos that includes both unencrypted and encrypted versions. The encryption method lacks adequate sensitivity to changes in the plaintext images or the keys. This study introduces a color image encryption technique utilizing various chaotic maps to overcome the limitations of one-dimensional and two-dimensional maps. This goal is achieved by developing a system that combines both 1D and 2D maps, leveraging their respective advantages while ensuring strong security and high encryption efficiency.

3. Proposed Method

This section presents a novel encryption method that leverages the advantages of one-dimensional and two-dimensional chaotic maps to withstand multiple attack vectors, including classical attacks, differential attacks, statistical attacks, and brute-force attacks. Figure 1 illustrates the structure of the suggested method. These illustrations illustrate the encryption configuration for colored pictures. The suggested approach primarily relies on the confusion and diffusion phases.

The technique utilizes distinct key streams derived from three chaotic systems: the Hénon map, the Lorenz map, and the logistic map. This research employs many hyperchaotic systems. Subsequently, confusion-diffusion phases are constructed using scrambling and DNA computing. During the confusion phase, a multi-stream scrambling technique is employed to obfuscate the original plaintext picture using two distinct, randomly generated chaotic sequences. The ambiguous picture is disseminated according to the DNA notion and an XOR operation using two distinct, created chaotic sequences. Ultimately, the encrypted picture is derived from the obfuscation and dispersion of the original image. This study's encryption method securely encrypts the original picture while ensuring the superior performance of the proposed algorithm. This section outlines the pertinent resources and details of the proposed method.

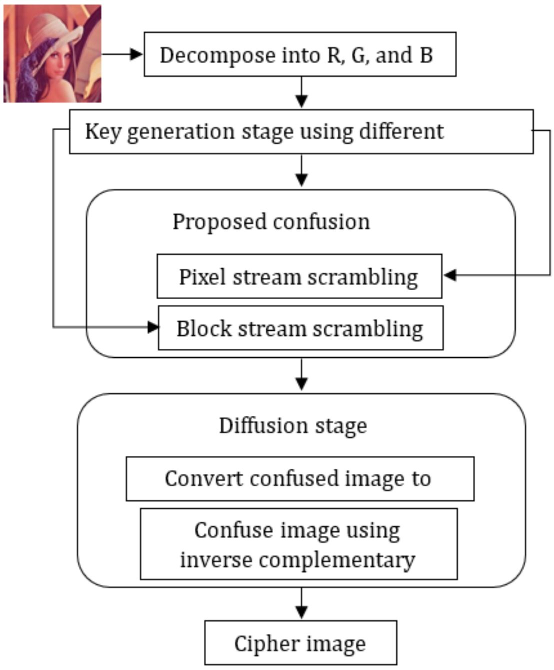

Decompose into R, G, and B
Key generation stage using different
Proposed confusion
Pixel stream scrambling
Block stream scrambling
Diffusion stage
Convert confused image to
Confuse image using inverse complementary
Cipher image

Fig. 1 *Proposed encryption framework*

3.1 Key Generation

In 1963, Lorenz attempted to elucidate the erratic nature of weather patterns by establishing a framework of differential equations. This study employs the picture encryption technique outlined in system [22]:

$$\begin{cases} x = a(\dot{y} - x) \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

The parameters of the Lorenz chaotic map are represented by the variables a, b, and c in equation (1). The Lorenz system exhibits chaotic behavior and may produce three distinct chaotic sequences with parameters a = 10, b = 8/3, and c = 28. Figure 2 illustrates a depiction of the attractor graph of the Lorenz map. The fourth-order Runge-Kutta method is used to solve the Lorenz equation [23].

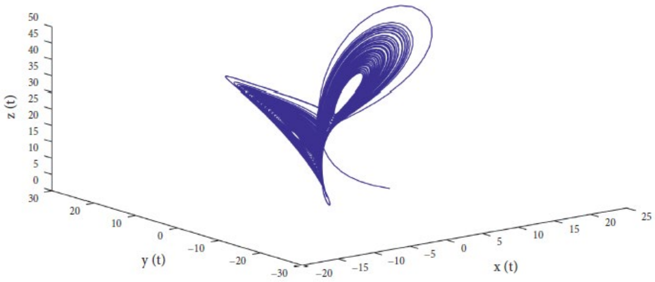


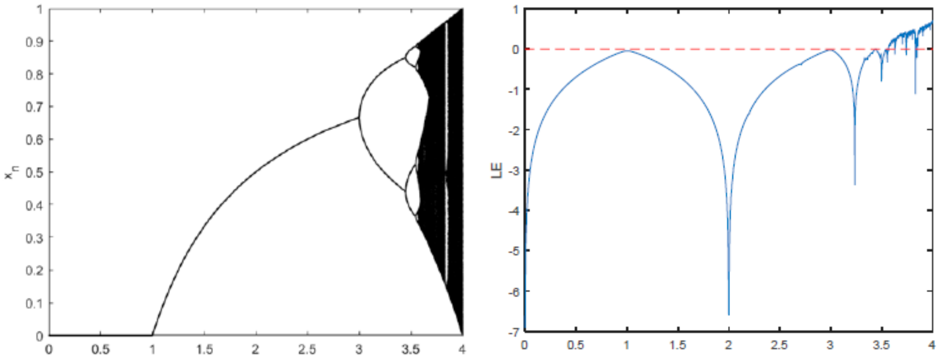
Fig. 2 *Lorenz chaotic map*

Logistic chaotic systems are the primary one-dimensional discrete chaotic systems, characterized by nonlinear dynamics, employing the following mapping equations:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{2}$$

The system control parameter μ together with the starting value x_0 fall within the range 0 < x_0 < 1. The variable μ exists within the range of (0,1) alongside the parameter x_n also residing within (0,1). The system establishes chaotic behavior if variable μ falls between values 3.5699 and 4. The chaotic system reaches its most complex state when the control parameter value is set to 4. When μ = 3.99, x_n = 0.555 and 0.556 [24]. Figures 3 illustrate the bifurcation diagram and Lyapunov exponent of the logistic chaotic mapping. The system enters chaotic behavior when parameter μ takes values from 3.5699456 to 4, while the bifurcations inside the system climb with increasing μ [25].

Where μ is the system control parameter, and x_0 represents the starting value of the system, constrained so that 0 < x_0 < 1. Where μ is an element of the interval (0,1), and x_n is also an element of the interval (0,1). When 3.5699 < μ ≤ 4, the system exhibits chaotic behavior. The complexity of the chaotic system is maximized when μ = 4. When μ = 3.99, x_n = 0.555 and 0.556 [24]. Figures 3 illustrate the bifurcation diagram and Lyapunov exponent of the logistic chaotic mapping. As μ increases and the number of bifurcations in the system rises, the system transitions into a chaotic state when μ ranges from 3.5699456 to 4 [25].



(a) **(b)**

Fig 3 *(a) The bifurcation diagram of the Logistic map; (b) The Lyapunov exponent of the logistic map*

Michel Henon first presented the Henon map in 1969. Being sensitive to its initial conditions [26], it is a discrete dynamic map exhibiting chaotic behavior. Its definition is:

$$X(n+1) = 1 - aX(n)^2 + Y(n) \tag{3}$$

$$Y(n+1) = b(X(n)) \tag{4}$$

The dynamic behavior of a chaotic system is dictated by the values of the control parameters *a* and *b*. The characteristics and requirements of the Henon map are as follows: The specifications and stipulations of the Henon map are as follows: *X(0)* represents the initial value; *a* ∈ [0, 1] is regarded as the control parameter; *K1 = (a, X (0))* denotes the secret key for the permutation phase. Notable attributes include the Lyapunov exponent, behavioral unpredictability, and uniform non-variation of the density variable. The Henon map is highly recommended for use in cryptography due to these attributes. For a = 1.4, *X* (0) = 0.766, b = 0.3, *Y* (0) = 0.3432, this system exhibits chaotic behavior. A little alteration in the parameter values may result in a change in the system's behavior.

3.2 Proposed Encryption Method

A secure relationship between ciphertext and encryption keys depends on the maximum complexity achieved through the Confusion method. The encryption process produces each cipher image element as a result of multiple key elements, thus concealing their relation. The retrieval of keys from cipher images becomes complicated because both one-bit changes and single-key variations result in significant transformations of the cipher image. The developed image encryption system functions through sequential confusion and diffusion procedures. Color image processing involves two stages in this method, which implements chaotic map-based advanced scrambling of pixels and blocks before performing DNA-based diffusion to enhance randomness and security.

The initial process splits an input color image into its basic red R, green G, and blue B color channels. The encryption proceeds through independent processing of each channel under separate chaotic encryption keys to achieve specific channel protection, thus increasing image security. The independent treatment of color layers during encryption protects the confidentiality of each pattern, so attackers encounter greater difficulties breaking the contents when one channel is compromised.

Pixel relationships must be disrupted at the confusion stage in order to accomplish encryption goals. The encryption process begins by distributing each color channel into four main blocks that match different image quadrants, starting from the top-left and moving down to the bottom-right. The segmentation integrates multi-scale sub-block extraction techniques that operate on main blocks through seven successive rounds. The initial step of the first round selects a 2×2 sub-block section from the middle area of each primary block. The sub-block extraction process moves from smaller divisions of 2×2 until it reaches 8×8, 16×16, 32×32, 64×64, 128×128, and 256×256. The method extends from the center to the outward areas to get diverse pixel positions across multiple spatial levels.

A two-dimensional sub-block array is formed by combining matching sections extracted from four main blocks in each round, before they are flattened into a one-dimensional image stream. Another chaotic key stream matching the length of each color channel also gets produced at the same time. Pixel stream scrambling takes place through a process that sorts plain image stream pixels according to the order of key stream values. The index-based permutation method is executed seven times across all rounds to achieve complete pixel-level disorder. The pixel-scrambled version of each color channel results from reconstructing the original structure through reversing the image flattening and sub-block extraction operations.

An additional security measure is achieved through block-level scrambling by implementing a second level of confusion. The scrambled channel repeats its division into four main blocks. The generation of a new chaotic key stream enables the rearrangement of block positions. The relocation of major image structural areas serves to increase complexity in the second security layer. The entropy of a scrambled image can be improved through optional permutation of sub-blocks inside main blocks.

The pixel value changes diffuse across the image during the diffusion stage to eliminate remaining patterns while resolving the confusion generated in the previous phase. To initiate the diffusion process, the algorithm converts every pixel in the confused image through a predefined binary nucleotide mapping, replacing 00 with A and 01 with T, and so forth. DNA encoding of the image completes just before the complementary process executes on its DNA format. The encoding procedure utilizes static or dynamically changing rules that replace letter pairs between A↔T and C↔G differently.

The application of the complementary rule generates a chaotic key stream, which is then converted into DNA sequences. A bitwise XOR operation enables the combination of DNA-encoded images with DNA key streams to reach the last stage of encryption. The encryption method produces substantial variations in the final encrypted output whenever there is a minimal alteration to the input image or key. An encrypted pixel pattern is obtained by decoding the XORed DNA sequences back into pixel values. The final encrypted image emerges when the completion of three-color channel diffusion leads to the combination of ciphered red, green, and blue components. The encryption method produces a resistant image against statistical attacks as well as differential and brute-force attacks because it applies multi-scale pixel scrambling and block permutation alongside chaotic DNA-based diffusion.

To enhance the security of our encrypted image, each color channel (RGB) is associated with a distinct type of chaotic map. Different behaviors and complexities are shown by each Hénon, Lorenz, and Logistic map, helping to produce the cryptographic key differently. The red channel relies on a two-dimensional Hénon map, which is renowned for its sensitivity to initial conditions and the generation of a complex type of attractor. Based on these characteristics, the red channel is a good home for AES since it has a lot of useful data for cryptography. When used in the green channel, the Lorenz system behaves as a hyperchaotic system with two or more positive Lyapunov exponents in continuous time. The fact that primary threats can be very hard to describe and predict makes the problem even more confusing and exacerbates the chaos in this color component. Using the blue channel, the Logistic map is a simple system that produces chaotic outputs when its initial values are set and repeatedly recalculated. Therefore, this is a suitable choice for the blue channel, as it achieves both high encryption speed and security by generating keys randomly. The system becomes more secure because each color channel has its chaotic key stream. When channels are disconnected in this manner, it becomes more difficult for hackers to target the system by relying on links between channels, thereby strengthening the encryption system.

3.3 Decryption Process

The decryption system works oppositely to encryption by resolving each color channel (R, G, B) independently in the encrypted image. Before processing begins on the cipher image, it receives a reversal of the diffusion operations. Separating the DNA code to recover pixel numbers requires running identical decryption steps, including DNA mapping operations with the complementary rule and XOR procedure, just like during the encoding process. The tool returns pixel data that contains complete confusion after reversing the DNA-based diffusion process. Moving forward, one must proceed with the reversal of block-level scrambling operations. The encryption keys generated from Hénon for R and Logistic for G and B channels are reactivated using their original initial conditions before being applied to the image, which was divided into four blocks. The inverse permutation derived from sorting the chaotic key is applied to the scrambled blocks to recover their original channel positions.

The pixel-level de-scrambling operation commences after the necessary block position recovery process. In the pixel-level descrambling phase, the sub-blocks that were scrambled in each color channel are obtained from the current image and placed in their proper positions according to the inverse permutation index used during encryption. The encryption process utilizes chaotic key streams for each scale and sorting indexes for pixel positions, which are regenerated and reversed, respectively, for decryption. The inverse permutations are appended to the specific sections of 1D pixel streams for sub-blocks before reconstructing their position into their original arrangement. The inverse reconstruction employs a multi-scale approach with center expansion for each sub-block across its seven levels, applied to all channels. Decryption of the final image occurs when both the confusion stage block and pixel reversal processes have been completed across the three-color channels, and the R, G, and B components are combined to create the final decrypted image.

4. Experimental Results

This section presents the efficiency and simulation results, along with comparisons to previously suggested picture encryption algorithms. The simulation aims to determine whether the aforementioned technique can disrupt and obscure the pixel values of the original test picture, hence concealing the essential plaintext information to ensure information secrecy. The decryption strategy is concurrently evaluated to determine if the legitimate information concealed within the encrypted image can be accurately decoded and the original plaintext image restored.

4.1 Key Sensitive Analysis

A very safe encryption algorithm must exhibit significant sensitivity to the key. Should the key undergo minor alterations, the resultant encrypted or decrypted picture must significantly vary from that generated by the original key. Utilizing a Lena picture as a reference, the ciphertext is decoded employing both the proper key and an erroneous key that exhibits a slight variation from the correct key, such as a one-bit discrepancy. The test results illustrating the algorithm's main sensitivity are shown in Figure 4. The inability to decode the accurate plaintext picture, even with a little alteration in the secret key, demonstrates the algorithm's pronounced sensitivity to the secret key, fulfilling the requisite security criteria. Figure 4 illustrates the impact of critical sensitivities of the suggested methodology. Figures 4 (a and b) show the original unencrypted photos alongside the encrypted versions. Figures 4 (c and d) illustrate the decrypted photos obtained with the erroneous key and those obtained with the right key, respectively.

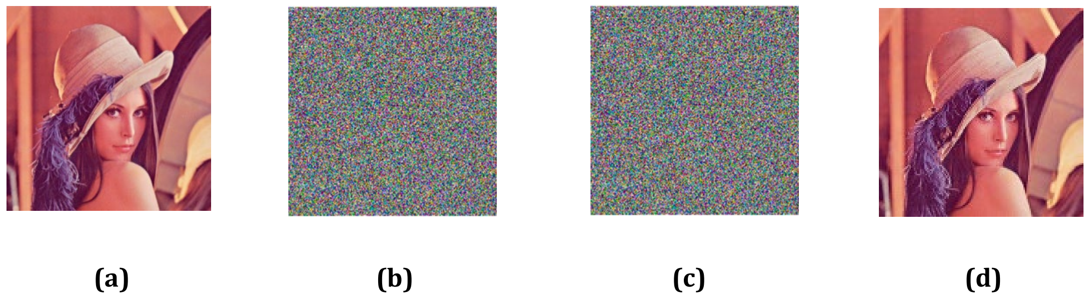


Fig 4 *Key sensitivity results for the proposed image encryption method*

4.2 Histogram Analysis

The histogram of an image is a crucial statistical attribute of the picture. The theory of stochastic processes asserts that an image can be viewed as a random field, with the histogram serving as an approximation of the image's density function. Thus, a more uniform histogram of the encrypted image renders it more difficult for an adversary to obtain statistical information about the pixels in the original image. Figure 5 illustrates the histogram of the Lena plaintext picture with the equivalent histograms of the ciphertext image for the R, G, and B color channels. The histogram curves of the original color channels R, G, and B show significant variations in height distribution. In contrast, the histogram of the encrypted image shows a uniform distribution of lines, with the height fluctuating around a certain value. Thus, our proposed strategy has a strong ability to withstand statistical examination.

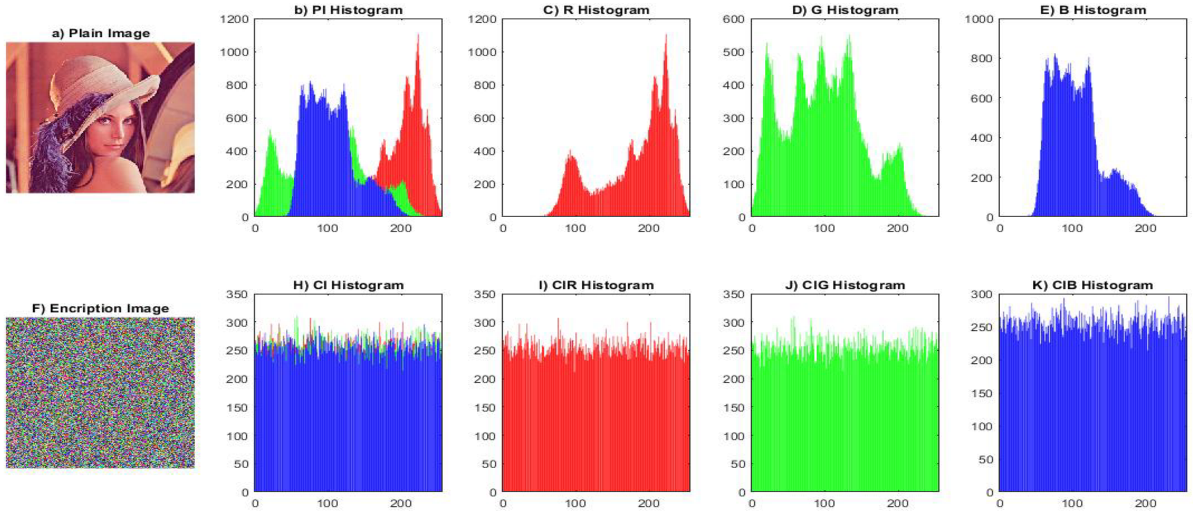


Fig 5 *Histogram analysis of Lena's plain image*

4.3 Information Entropy Analysis

Information entropy signifies the challenge of deducing the information included in a picture. Higher information entropy indicates higher chaos within the image's content, hence reducing the likelihood of successful decipherment. The definition in mathematical terms is as follows:

$$H(x) = -\sum_{i=0}^{2^N-1} p(x_i) log_2 p(x_i) \tag{5}$$

Here, 2*N* represents the gray level of the picture (ranging from 0 to 255), and *p(xi)* signifies the probability that a pixel corresponds to a certain gray value. In a grayscale picture with 256 levels, the maximum information entropy is 8 bits. A higher information entropy, approaching 8, indicates more randomness in the pixel value arrangement of the encrypted picture; hence, elevated ciphertext information entropy correlates with enhanced secrecy of the encryption process and increased security of the ciphertext information.

Table 1 *Entropy results*

Image	Original/cipher	Information entropy		
		R	G	B
Lena	Original	7.2795	7.6315	6.9891
	Cipher	7.9976	7.9977	7.9972
Peppers	Original	7.3318	7.5242	7.0792
	Cipher	7.9971	7.9974	7.9976
Lena [27]	Original	7.1898	7.5238	6.9024
	Cipher	7.9973	7.9974	7.9976

Table 1 illustrates a comparison of information entropy between the original and encrypted images for each test picture, revealing that the original image exhibits low information entropy, while the encrypted image approaches the maximum value of 8. This signifies that this encryption system is more efficient and can successfully withstand assaults predicated on information entropy.

4.4 Differential Attack Analysis

A differential attack is a prevalent decryption technique that identifies the correlation between the original and encrypted data by analyzing the minute discrepancies between the original and its matching encrypted picture, then targeting the encryption process. against evaluate the encryption algorithm's resistance against differential assaults, it is essential to distinguish between the original picture and its matching encrypted version. The new encrypted picture may be derived by altering the pixel value of any location in the original image. The degree of difference between the new encrypted image and the previous encrypted image is analyzed. A substantial level of disparity suggests that the encryption method proposed in this study may effectively counter differential assaults. The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are often used to evaluate the degree of variation between images. The NPCR and UACI are calculated as follows:

$$NCPR = \frac{1}{W \times \mathrm{H}} \sum_{i=1}^{W} \sum_{j=1}^{H} d_{ij} \times 100\% \tag{6}$$

$$UACI = \frac{1}{255 \times W \times \mathrm{H}} \sum_{i=1}^{W} \sum_{j=1}^{H} \left| C_{ij}^{1} - C_{ij}^{2} \right| \times 100\% \tag{7}$$

Where the dimensions of the encrypted picture are denoted by H for height and W for width, respectively. $C1$ and $C2$ depict two encrypted pictures, which correspond to two original plaintext images differing by a single pixel, denoted as C_{ij}^{1}.

$$d_{ij} = \begin{cases} 0, & C_{ij}^{1} = C_{ij}^{2} \\ 1, & C_{ij}^{1} \neq C_{ij}^{2} \end{cases} \tag{8}$$

This study presents the findings of differential attack analysis for the color photos of Lena and Peppers in Table 2. The NPCR and UACI values derived from the algorithm in this study are comparably proximate to the ideal values as those reported in the relevant literature. The data indicate that this technique is very responsive to variations in picture pixels and can successfully withstand differential attacks.

Table 2 *The result values for NPCR and UACI (%)*

Image	NPCR			UACI		
	R	G	B	R	G	B
Lena	99.6281	99.6195	99.6102	33.4608	33.4687	33.4256
Peppers	99.6109	99.6128	99.6318	33.4630	33.4650	33.4671
Lena [27]	99.5972	99.6262	99.5804	33.5757	33.2772	33.3863

4.5 Correlation Analysis

The correlation between adjacent pixels measures the degree of relationship between nearby data in an image. Correlation analysis investigates the link between adjacent pixels in a digital image. A significant connection between adjacent pixels in an image enables an attacker to infer information about the original image by analyzing the correlation distribution. Thus, when the correlation coefficient between adjacent pixels in an encrypted image approaches 0, the security of the encrypted image and the effectiveness of the encryption increase. The formula for computation is:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{9}$$

$$cov(x,y) = \frac{1}{N} \sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{10}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \tag{11}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{12}$$

Based on the above Equation, *N* represents the total number of pixel points, the gray values of adjacent pixels are represented by *x* and *y*, *E(x)* indicates the pixel's average value, and the variance is represented by *D(x)*, *cov(x, y)* indicates the correlation function, and r_{xy} is the correlation coefficient. The formula also shows that when the absolute value is high, the correlation is stronger. Table 3 shows the correlation analysis of the results.

Table 3 *Correlation analysis results*

Image	Channel	Original image			Cipher image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	0.9038	0.9418	0.9437	-0.0028	-0.0213	-0.0139
	G	0.8737	0.9038	0.8991	0.0068	-0.0087	0.0050
	B	0.8400	0.8673	0.8548	0.0134	0.0149	-0.0262
Peppers	R	0.9246	0.9061	0.9437	0.0189	-0.0094	0.0205
	G	0.9243	0.9429	0.9526	-0.0010	-0.0214	-0.0045
	B	0.8937	0.8932	0.9420	-0.0114	-0.0016	0.0301
Lena [27]	R	0.952	0.97608	0.92986	-0.016983	0.0081473	-0.00649
	G	0.93915	0.96889	0.91604	0.00013987	0.019388	0.00018398
	B	0.90861	0.94499	0.88624	- 0.0050275	- 0.000293	- 0.0016697

Figure 6 shows the distribution maps of adjacent pixels of the original images and the cipher images in all Directions.

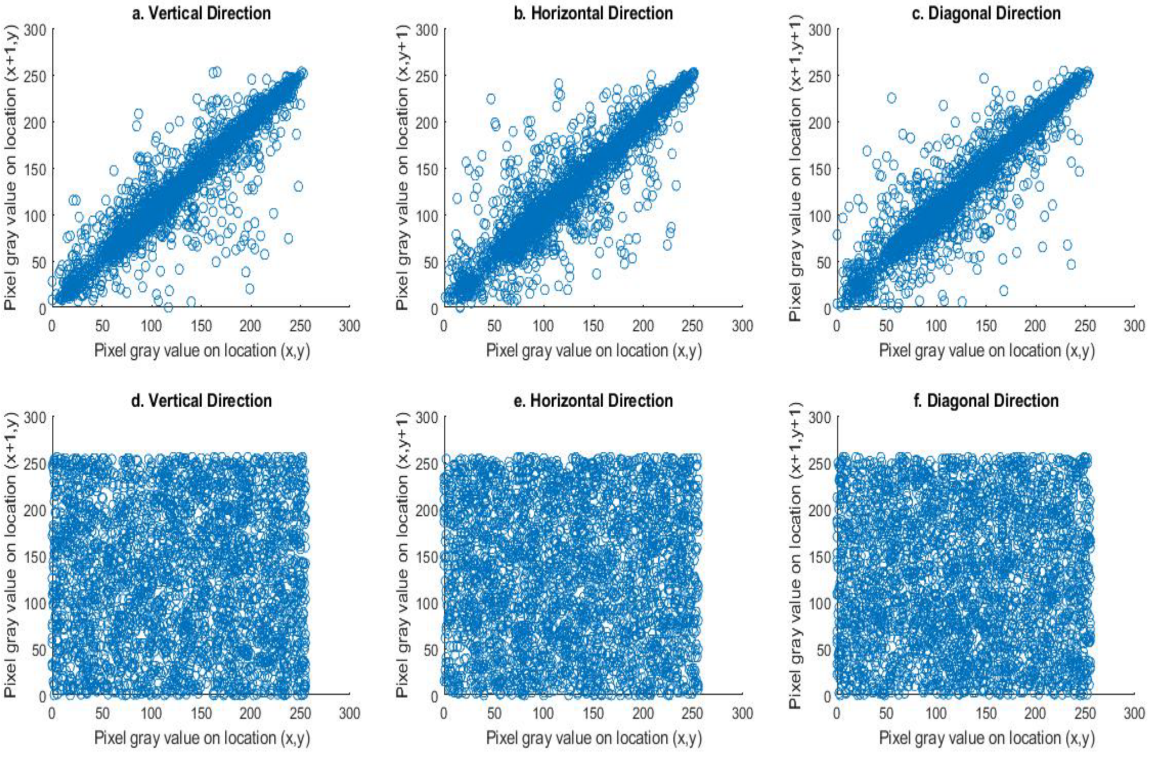


Fig. 6 *Distribution maps of adjacent pixels of the original images and the cipher images*

5. Conclusion

In this work, we introduce a new image encryption approach that utilizes chaotic maps to enhance the security of color images. The encryption process becomes extremely hard to penetrate because our method first scrambles pixels, followed by block-level scrambling techniques. The encryption process gains additional security through the implementation of DNA encoding techniques together with logical operation execution during the diffusion stage. Experimental data indicate that our encryption method exhibits both strong security attributes and excellent entropy values, as well as minimal correlations, establishing it as a practical solution for real-world image defense. Researchers should concentrate on efficiency enhancements for this encryption algorithm and study its implementation for real-time encryption applications. The approach being suggested is effective to a certain extent, though there are disadvantages. Security requires properly adjusting the map's parameters, which can be a complex process. Because the genetic maps are so complex, this process can run slowly, which may make it less useful for real-time tasks. It is most efficient for color images, but may require adjustments to handle grayscale images.

Acknowledgement

The authors would like to thank the Technical College of Informatics, Akre University for Applied Sciences, and the Technical College of Engineering, Duhok Polytechnic University, for their valuable support.

Conflict of Interest

Authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *M. S. S.;* ***data collection:*** *M. S. S.;* ***analysis and interpretation of results:*** *M. S. S.;* ***draft manuscript preparation:*** *M. S. S. S. R. M. Z. provided overall supervision, critical revision, and guidance throughout the research and manuscript preparation process. Both authors reviewed the results and approved the final version of the manuscript.*

References

[1] Banning, S., H¨oglinger, M., Meyer, D., & Reich, O. (2023). Evaluation of the effect of a multifunctional telemedicine device on health care use and costs: A nonrandomized pragmatic trial. Telemedicine and e-Health, 29(4), 510–517.

[2] Adil Yazdeen, A., Zeebaree, S. R., Mohammed Sadeeq, M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021). FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review. Qubahan Academic Journal, 1 (2), 8–16.

[3] Es-sabry, M., El Akkad, N., Khrissi, L., Satori, K., El-Shafai, W., Altameem, T., & Rathore, R. S. (2024). An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. Egyptian Informatics Journal, 25, 100449.

[4] Meng, F. Q., & Wu, G. (2024). A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. Expert Systems with Applications, 254, 124413.

[5] Selvamani, R., & Yusoff, Y. (2024). Effectiveness of the Spatial Domain Techniques in Digital Image Steganography. Qubahan Academic Journal, 4(1), 341-350.

[6] Alsandi, N. S. A., Zebari, D. A., Al-Zebari, A., Ahmed, F. Y., Mohammed, M. A., Albahar, M., & Albahr, A. A. (2023). A Multi-Stream Scrambling and DNA Encoding Method Based Image Encryption. Computer Systems Science & Engineering, 47(2).

[7] Yousif, S. F., Abboud, A. J., & Alhumaima, R. S. (2022). A new image encryption based on bit replacing, chaos and DNA coding techniques. Multimedia Tools and Applications, 81(19), 27453-27493.

[8] Hussien, A. Y. (2022). Review on social media and digital security. Qubahan Academic Journal, 2(2), 1-4.

[9] Liu, J. B., Peng, X. B., & Hayat, S. (2022). Topological index analysis of a class of networks analogous to alicyclic hydrocarbons and their derivatives. International Journal of Quantum Chemistry, 122(2), e26827.

[10] Zhu, S., & Zhu, C. (2020). Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. Entropy, 22(7), 772.

[11] Azimi, Z., & Ahadpour, S. (2020). Color image encryption based on DNA encoding and pair coupled chaotic maps. Multimedia Tools and Applications, 79, 1727-1744.

[12] Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018). Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 312-317). IEEE.

[13] Hosny, K. M., Kamal, S. T., & Darwish, M. M. (2022). A color image encryption technique using block scrambling and chaos. Multimedia Tools and Applications, 81(1), 505-525.

[14] Teng, L., Wang, X., & Xian, Y. (2022). Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Information Sciences, 605, 71-85.

[15] Erkan, U., Toktas, A., & Lai, Q. (2023). 2D hyperchaotic system based on Schaffer function for image encryption. Expert Systems with Applications, 213, 119076.

[16] Wang, S., Peng, Q., & Du, B. (2022). Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Optics & Laser Technology, 148, 107753.

[17] Yan, S., Li, L., Gu, B., Cui, Y., Wang, J., & Song, J. (2023). Design of hyperchaotic system based on multi-scroll and its encryption algorithm in color image. Integration, 88, 203-221.

[18] Li, X., Zeng, J., Ding, Q., & Fan, C. (2022). A novel color image encryption algorithm based on 5-D hyperchaotic system and DNA sequence. Entropy, 24(9), 1270.

[19] Wang, S., Peng, Q., & Du, B. (2022). Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Optics & Laser Technology, 148, 107753.

[20] Wang, C., Chong, Z., Zhang, H., Ma, P., & Dong, W. (2024). Color image encryption based on discrete memristor logistic map and DNA encoding. Integration, 96, 102138.

[21] Lone, M. A., & Qureshi, S. (2022). RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher. Optik, 260, 168880.

[22] Zhou, S., He, P., & Kasabov, N. (2020). A dynamic DNA color image encryption method based on SHA-512. Entropy, 22(10), 1091.

[23] Tang, Z., Yin, Z., Wang, R., Wang, X., Yang, J., & Cui, J. (2022). [Retracted] A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement. Journal of Chemistry, 2022(1), 3906392.

[24] Xu, J., Zhao, B., & Wu, Z. (2022). Research on color image encryption algorithm based on bit-plane and Chen Chaotic System. Entropy, 24(2), 186.

[25] Wan, Y., Gu, S., & Du, B. (2020). A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy, 22(2), 171.

[26] Kanwal, S., Inam, S., Othman, M. T. B., Waqar, A., Ibrahim, M., Nawaz, F., ... & Hamam, H. (2022). An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. Sensors, 22(12), 4359.

[27] Meng, F. Q., & Wu, G. (2024). A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. Expert Systems with Applications, 254, 124413.