FeistelX Network-Based Image Encryption Leveraging Hyperchaotic Fusion and Extended DNA Coding

by De Rosal Ignatius Moses Setiadi

Submission date: 28-Apr-2025 12:48AM (UTC+0700)
Submission ID: 2425192734
File name: R1_Kris_SubmissionEN-EGIJ-withoutAuthorDetails.docx (3.42M)
Word count: 9322
Character count: 54271

FeistelX Network-Based Image Encryption Leveraging Hyperchaotic Fusion and Extended DNA Coding

Abstract – The rising frequency of cyberattacks has heightened the need for more secure and efficient image encryption techniques. Traditional chaotic and DNA-based methods often struggle with limited key space, low diffusion efficiency, or vulnerability to statistical attacks, especially when handling large or high-dimensional image data. This study introduces an image encryption technique that integrates the FeistelX Network with extended DNA cryptography and two distinct two-dimensional hyperchaotic maps, namely the two-dimensional symbolic chaotic map (2D-SCM) and the two-dimensional hyperchaotic exponential adjusted Logistic and Sine map (2D-HELS), to bolster data security. The proposed method synergizes three key components: the FeistelX Network offers a robust encryption framework with bijectivity ensured by property H; the extended DNA cryptography expands the key space and minimizes pixel correlation through advanced DNA operations; and the two hyperchaotic maps generate highly intricate chaotic sequences, ensuring greater randomness and resilience. Compared to existing schemes, the proposed method demonstrates improved diffusion, randomness, and resistance to statistical attacks. Experimental results show that this method achieves high-security indicators, with Chi-square values consistently below the critical threshold, average entropy values of 7.9994, and UACI and NPCR metrics remaining within the optimal theoretical ranges. Moreover, the method passed all sixteen NIST randomness tests with an average p-value of 0.6278. It demonstrated resilience to noise and data loss with PSNR values above 18 dB under attack scenarios. This combination of FeistelX structure, extended DNA operations, and dual hyperchaotic maps offers a novel and effective solution for enhancing image encryption security beyond traditional approaches.

Keywords: Chaotic Sequence; DNA Cryptography; Feistel Network; Hyperchaotic Encryption; Image Security.

1. Introduction

With the advancement of information technology, digital security is becoming increasingly important. Unauthorized access or disruption to digital data can cause significant economic losses and threaten national security [1,2]. Based on the CrowdStrike report, it is known that there has been an increase in cyber attacks of up to 75% [3]. Therefore, developing security protection methods must continue to be improved [4–6]. Images are widely used in social communications and various fields such as big data, health, aerospace, and military to store and transfer important and confidential information. Therefore, digital image security is a top priority to prevent unauthorized access and ensure the integrity and confidentiality of information.

Image encryption is one of the effective methods to protect visual data from cyber threats [7,8]. However, traditional encryption algorithms such as DES, AES, and RSA, although strong for text encryption, because of the enormous volume, make them inefficient and secure enough for image encryption due to the high correlation and redundancy properties of image pixels [9–12]. In addition, cryptanalysis encourages researchers to continue to develop new techniques to improve cryptographic security and overcome increasingly sophisticated attacks [5,13].

Chaotic systems are characterized by being highly sensitive to initial conditions and producing irregular and unpredictable sequences, making them suitable for high-security cryptosystems [12,14–19]. Higher-dimensional chaotic systems, such as hyperchaotic systems, have larger key spaces and stronger attack resistance, making them more suitable for image encryption [20–22]. Hyperchaotic systems can produce more complex and unpredictable pseudorandom sequences, providing a higher level of security than conventional chaotic systems. The Lyapunov exponent measures the sensitivity of a chaotic system to its initial conditions. In a hyperchaotic system, there is more than one positive Lyapunov exponent, indicating that the system has a higher degree of randomness and uncertainty. This makes hyperchaotic systems very difficult to predict and analyze, enhancing the security of image encryption [23].

In addition, DNA encoding technology has emerged as a promising innovation in cryptography. DNA encoding uses the sequence of nucleotide bases to encode information, providing an additional layer of security through DNA operations such as addition,

subtraction, XOR, and XNOR that follow binary rules [24–26]. Combining chaotic systems and DNA coding technology can significantly improve the security of image encryption by reducing pixel correlation and improving resistance to statistical and differential attacks [27]. However, standard DNA encryption based on 2-bit mappings still faces challenges in expanding the key space and achieving stronger diffusion, especially when processing high-dimensional image data.

Several studies have explored using chaotic systems and DNA coding in image encryption. For example, Meng and Wu [9] proposed a 5D hyperchaotic system to generate chaotic sequences for permutation and diffusion processes. They used an extended DNA coding scheme to improve the DNA coding rules and DNA computation methods, thereby improving the security of the encryption scheme. In addition, many studies have shown that combining DNA technology with chaotic sequences can reduce image pixel correlation and improve resistance to statistical and differential attacks [28–31]. Nevertheless, prior works often either relied on fixed DNA coding schemes or lacked an integrated structure that systematically combines hyperchaotic dynamics and DNA-based diffusion within a flexible encryption framework.

The Feistel network is a basic structure used in many modern encryption algorithms, such as DES and AES, to help improve the avalanche effect. The Feistel network has the advantage of separating data into two parts and processing them iteratively through multiple rounds of encryption with complex key functions [32,33]. This structure allows the decryption process to use almost identical steps as encryption, only with the key order reversed, thereby improving the reliability and flexibility of the algorithm. In addition, the Feistel network is designed to resist various types of cryptanalysis attacks, including differential and linear attacks. However, conventional Feistel-based approaches for image encryption typically rely on simple permutation-substitution mechanisms, limiting their effectiveness against modern attack strategies targeting pixel correlation and statistical patterns.

Motivated by these limitations, this study proposes a novel approach by extending the Feistel structure into FeistelX, which integrates property H for invertibility, employs extended DNA operations for enhanced diffusion, and utilizes two complementary hyperchaotic maps (2D-HELS and 2D-SCM) to achieve robust and scalable image encryption. Further contributions of this research are:

1. Develop a stronger Feaistel network design by dividing the image into four parts and adding H properties, called FeistelX.
2. Combine extended DNA and mixed chaotic methods based on FeistelX.
3. Implement this encryption scheme on digital images to evaluate its performance and resilience to various attacks and compare it with related work.

Thus, this research proposes a potential approach to improve image encryption security in response to the challenges of an increasingly complex and cyber-attack-prone digital environment. The remainder of this paper is organized as follows: Section 2 presents the preliminaries and background information necessary to understand the proposed method. Section 3 describes the proposed image encryption method in detail. Section 4 discusses the implementation and results of the proposed method. Finally, Section 5 concludes the paper and outlines potential directions for future work.

2. Preliminaries

2.1 Feistel Networks

A Feistel Network is a fundamental structure commonly used in many symmetric block encryption algorithms to ensure secure and reversible data transformation. It operates by dividing the plaintext data (M) into two equal parts, typically the left and right halves [34]. The encryption process involves multiple rounds of operations to increase security gradually. In each round: 1) The left half is processed through a complex encryption function with a round-specific key. 2) The output of this function is then combined with the right half using an XOR operation. 3) The two halves are swapped before proceeding to the next round.

In the study [35], the Feistel Network was developed by adding property H. A new property that allows the encryption function to be inverted exactly, improving the bijectivity and security of encryption. Property H states that the encryption function f is invertible with the function t. If f is as in Equation (1), then the inverting function t is in Equation (2).

$$f(x, K) = g(x, K) \quad (1)$$

$$t(z, K) = g^{-1}(z, K) \quad (2)$$

Where K is the key, g is the encryption function and g^{-1} is the inverse function, x is the plaintext, and z is the ciphertext.

Other image encryption studies also apply Feistel Network, such as [36,37]. The study [36] proposed an extended Feistel network encryption scheme. The extended Feistel network utilizes four input sub-blocks and performs encryption in seven iterations to ensure security. The function F in this network consists of S-boxes and P-boxes generated dynamically using chaos maps and Rubik's cubes, increasing the encryption scheme's complexity and security. The study [37] uses a Feistel network and dynamic DNA coding. The problems of secret keys, chaotic sequences, Hill encryption, Feistel networks, and pixel diffusion inspire this. To overcome these problems, several improvements, including redesigning the secret key as a 256-bit binary sequence, using a suitable hyper-chaotic Chen system, and improving the pixel diffusion process. The latest study [32] develops the Feistel Network by dividing M into four parts, namely A, B, C and D [32]. Its operations are complexed with a combination of permutation, substitution based on XOR and modulus. Inspired by these studies, this study proposes a method called FesitelX, which divides M into four parts with property H. FeistelX Network is a Feistel Network with property H and is divided into four parts using permutation operations, extended DNA, XOR operations and modulation operations, providing additional security by ensuring that each encryption function has a corresponding reversal function, which is essential for accurate and secure decryption. Property H ensures that the encryption process can be reversed exactly, providing assurance that the original data can be recovered after decryption. However, existing Feistel-based approaches often focus only on simple permutation-substitution operations or require complex S-box/P-box design, limiting flexibility and scalability for higher-dimensional encryption needs.

2.2 DNA Coding

DNA coding is a cryptographic technique that draws inspiration from the structure of biological DNA to represent digital information in a highly complex and secure form. In DNA molecules, information is naturally stored using four types of nucleotide bases: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) [38,39]. These bases can be mapped to binary bits, transforming digital data into DNA-like sequences. By leveraging the vast combinations and complexity of DNA sequences, DNA coding introduces an additional layer of security in encryption systems, making it more resistant to attacks.

The DNA encoding involves several basic steps [38,40]: 1) Binary to DNA Conversion: Digital information is converted into a binary sequence, which is then mapped to the DNA nucleotide

base sequence using a specific encoding scheme. 2) DNA Operations: Once the data is converted into a DNA sequence, basic DNA operations such as addition, subtraction, XOR, and XNOR are performed. These operations follow the rules of binary computation applied to DNA bases. 3) Decryption: Decryption involves reversing the DNA operations to recover the original information in binary format. Advances in DNA encoding technology have resulted in several new techniques and methods to improve the security and efficiency of encryption. Research [41] proposed the use of DNA encoding in the encryption of medical images and medical reports using the RSA algorithm. They mixed the DNA sequences obtained from image encoding and reports to improve the security level of IoT networks. Research [42] introduced a hybrid adaptive image encryption algorithm using DNA encoding and one-dimensional chaos maps to generate sequences. This scheme uses logistic maps and tent maps to permute half of the images, then combines the results and applies DNA operations for diffusion. Research [43] proposed an encryption scheme based on DNA cryptography, a four-dimensional hyperchaotic system, and a Moore machine. The hyperchaotic system generates four chaotic sequences used in DNA-based operations. The Moore machine is used for substitution in the DNA sequence, improving the scheme's security. The use of the DNA method plays a role in improving the security of image encryption.

In research [9], the DNA method is applied and extended to DNA encoding, making this DNA method complex and strong when combined with other methods. Suppose standard DNA coding uses four DNA nucleotides: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G), which are represented by binary values: A = 00, T = 11, C = 01, and G = 10. Extended DNA coding extends this approach by using 3-bit binary values for each nucleotide, resulting in more combinations: A = 000, a = 001, C = 010, c = 011, G = 100, g = 101, T = 110, t = 111. The above provides several advantages: higher complexity, expanding the key space, and being more resistant to statistical and differential attacks. Although DNA cryptography has enhanced security levels, many schemes using standard 2-bit encoding still face challenges in expanding the key space and resisting sophisticated statistical attacks, necessitating further improvements like extended DNA coding.

2.3 Chaotic Image Encryption

Chaotic image encryption utilizes the principles of chaos theory, where small changes in initial conditions can lead to highly unpredictable outcomes. In this approach, chaotic maps, nonlinear systems highly sensitive to initial values, generate pseudorandom sequences known as chaotic sequences or keystreams. These sequences are used to randomize and scatter the pixel values of an image, thereby making the encrypted data extremely difficult to reconstruct without the correct key. This method significantly enhances security against various types of cryptographic attacks by leveraging chaotic systems' inherent unpredictability and complexity.

Hyperchaotic, in general, is a dynamical system that has more than one positive Lyapunov exponent (LE), indicating that the system is susceptible to initial conditions in more than one direction. A 2D chaotic map can be called hyperchaotic if it has two positive Lyapunov exponents, indicating a more complex chaos than a regular chaotic system with only one positive LE [44,45]. The advantages of a 2D hyperchaotic map over a 3D or more hyperchaotic map are its lower computational complexity and simplicity of implementation while still offering high-security properties due to its hyperchaotic nature.

Several previous studies have proposed 2D hyperchaotics, such as the study [38], which proposed 2D-SCMCI hyperchaotics. The 2D-SCMCI method is built to overcome the weaknesses of existing chaotic cryptography systems, such as chaotic degradation and uneven output distribution. 2D-SCMCI is designed based on cascade couple modulation and two 1D chaos maps. Based on the test results, two positive LE values are obtained, which means it can be called hyperchaotic.

Lai et al. [46] introduced a new image encryption scheme based on two-dimensional (2D) Salomon maps that offer high security by utilizing chaotic properties. This 2D Salomon map is developed from a one-dimensional function to two dimensions to increase the complexity and uncertainty of the chaotic sequence. This encryption algorithm splits and swaps pixel bits and global pixel distribution, erasing the original image information.

Research [47] proposed an image encryption algorithm using a new hyperchaotic map called a two-dimensional symbolic map (2D-SCM). This method utilizes fission diffusion and permutation operations to improve encryption security. The 2D-SCM hyperchaotic map offers better ergodicity, more complex behavior, and a wider chaotic range, providing high security.

The fission diffusion process spreads small changes throughout the image, increasing the difficulty of identifying changes in the encrypted image. This method is susceptible to initial conditions, making it safe from brute force attacks. This algorithm is also resistant to differential attacks, noise, and data loss and has high encryption efficiency for fast processing. Overall, the 2D-SCM method offers better security and efficiency than conventional algorithms.

Wang et al. [48] proposed a new image encryption algorithm using a two-dimensional hyperchaotic map called hyperchaotic exponential adjusted Logistic and Sine map (2D-HELS). The 2D-HELS map combines Logistic and Sine maps with exponential adjustment to enhance the chaotic characteristics. The main advantages of 2D-HELS include high ergodicity, which provides a wider chaotic range and more complex behavior, thus improving encryption security. In addition, 2D-HELS is very sensitive to initial conditions, so small changes can produce different results, improving the resistance to brute-force attacks. While various 2D hyperchaotic maps have improved randomness, certain methods still suffer from chaotic degradation, limited diffusion effects, or increased computational complexity, which may affect encryption robustness.

2.4 Summary and Identified Research Gaps

To better illustrate the research gap and the motivation for the proposed method, Table 1 summarizes key existing studies related to Feistel networks, DNA cryptography, and chaotic encryption. It highlights their respective approaches and limitations and how the proposed method addresses these shortcomings through a novel integration of FeistelX structure, extended DNA operations, and dual hyperchaotic systems.

Table 1. Comparison of existing studies and the proposed method regarding approach, limitations, and improvements.

Ref	Approach	Limitations	Remarks
[36]	Extended Feistel with S-box/P-box chaos	Complex S-box/P-box design, limited scalability	Complex structure, less flexible for higher dimensions

[37]	Feistel with dynamic DNA coding	Standard DNA coding (2-bit), limited keyspace	Key expansion and security need improvement
[42]	DNA coding + hyperchaotic system	Moderate diffusion strength, limited flexibility	Focused on 1D chaos maps, no extended DNA
[47]	2D-SCM hyperchaotic encryption	Stronger diffusion but increased structural complexity	No integration with DNA-based operations
[48]	2D-HELS hyperchaotic encryption	High chaotic complexity but no modular integration	No DNA or multi-layered modularity
Ours	FeistelX + extended DNA + 2D-HELS & 2D-SCM	—	Combining property H-based Feistel, extended DNA, and dual 2D hyperchaotic maps for stronger confusion and diffusion

3. Proposed Method

Based on the literature above, this study proposes an image encryption method that combines three main components: two 2D hyperchaotic methods, namely 2D-SCM and 2D-HELS, FeistelX Network, and extended DNA Cryptography. Two 2D hyperchaotic methods are used to generate very complex pseudorandom sequences. FeistelX Network provides a strong and flexible encryption structure with H property that guarantees the bijectivity and security of the encryption and decryption process. Meanwhile, extended DNA Cryptography will add additional layers of security through complex DNA operations, expanding the key space and reducing pixel correlation. The main contribution of this work is developing an image encryption method based on an extended FeistelX structure integrated with dynamic DNA operations and controlled by two distinct 2D hyperchaotic maps (2D-SCM and 2D-HELS). The proposed method is further illustrated in Figure 1.

3.1. Image Preprocessing and Parameter Initialization

Image preprocessing is performed by reshaping the read image into a one-dimensional vector (I). This is done to facilitate the application of pixel and bit permutation and substitution in the subsequent stages. Equation (3) is used to perform the reshaping process.

$$I = \text{reshape}(\text{imread}(img), 1, [\,]) \quad (3)$$

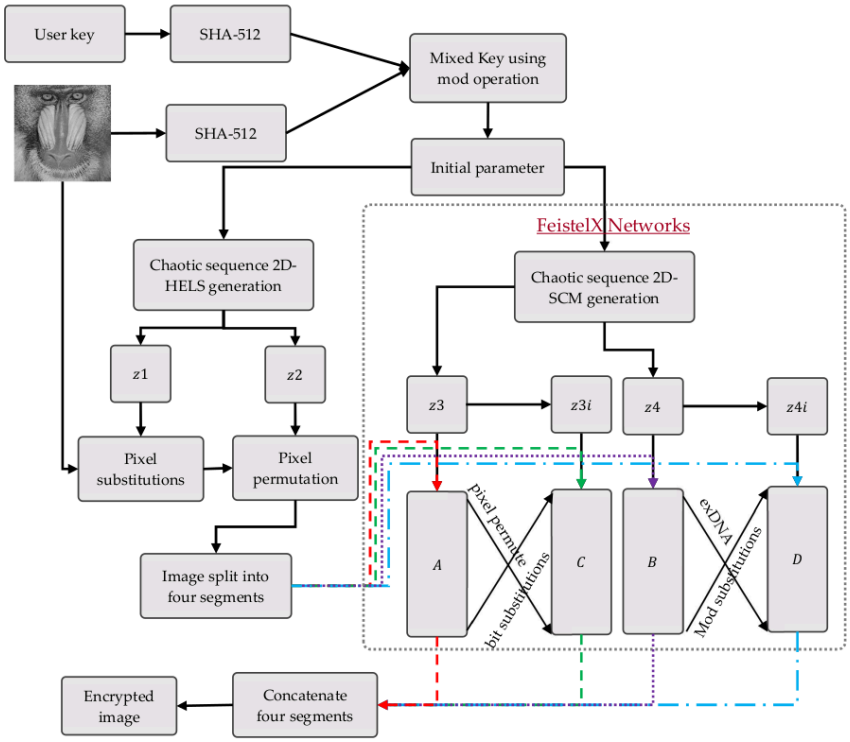


Figure 1. The flow of the proposed encryption scheme

Where img is the image that has been read, reshape is the function used to change the shape, imread is the image reading function, 1 means 1 row, and [] indicates that the number of columns is adjusted according to the image dimensions.

At this stage, several parameters are also set, such as determining the number of rounds (N), control factors α and μ, and the initial values for the chaotic sequence, namely $x1_o$, $y1_o$, $x2_o$,

and $y2_o$. These highly sensitive initial values will determine the chaotic sequence generated, a key component of this encryption method. To make these values unique, the initial values are generated from the user's input key (K), and the plaintext (I) hashed with SHA-512. As a result, SHA-512(K) and SHA-512(I) are obtained, each consisting of 128 hexadecimal values, which are then converted into 64 ASCII numbers and mixed using a modulus operation, as shown in Equation (4).

$$K = \text{mod}((K1 + K2), 256) \tag{4}$$

Where $K1$ is the ASCII number from the user's key that has been SHA-hashed, while $K2$ is the ASCII number from the plaintext that has been SHA-hashed. Next, to obtain the values $x1_o$, $y1_o$, $x2_o$, and $y2_o$ Equations (5)-(8) are used.

$$x1_0 = \text{std}(K_{1:16}) \tag{5}$$

$$y1_0 = \text{std}(K_{17:32}) \tag{6}$$

$$x2_0 = \text{std}(K_{33:48}) \tag{7}$$

$$y2_0 = \text{std}(K_{49:64}) \tag{8}$$

Where std a is the function used to calculate the standard deviation.

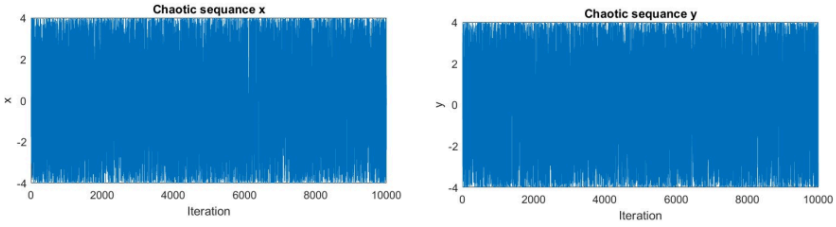
3.2 First Stage Encryption

In the first stage, the generation of the 2D-HELS chaotic sequence is used for pixel permutation and bit substitution in the image. The length of the chaotic sequence (n) is equal to the number of pixels in the image. The 2D-HELS chaotic sequence is calculated using Equations (9) and (10), with input μ and initial values $x1_0$ and $y1_0$.

$$x_{n+1} = 4\sin\left(\pi(4\exp(\mu) \cdot x_n \cdot (1 - x_n) + (1 - \exp(\mu)) \cdot \sin(\pi \cdot y_n))\right) \tag{9}$$

$$y_{n+1} = 4\sin\left(\pi(4\exp(\mu) \cdot y_n \cdot (1 - y_n) + (1 - \exp(\mu)) \cdot \sin(\pi \cdot x_{n+1}))\right) \tag{10}$$

The plot of the chaotic sequence for x and y and its bifurcation are presented in Figure 2, where the visualization shows the randomness and complexity of the generated sequence.



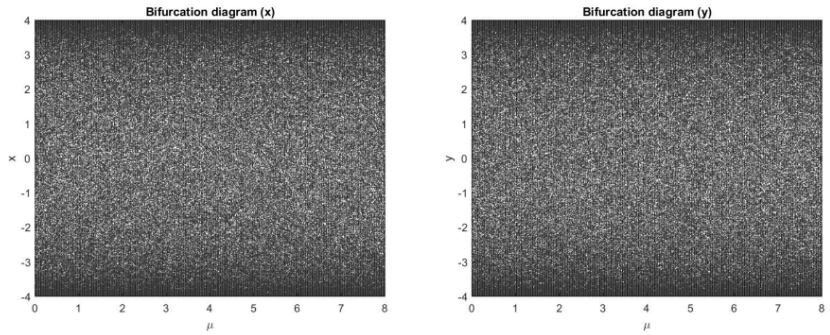


Figure 2. Chaotic sequence and bifurcation diagram plot of 2D-HELS

If $z1$ is the first chaotic sequence, then $z2$ is the second from 2D-HELS. Convert $z1$ into an integer form using Equation (11), then perform the bitwise XOR operation between $z1$ d and the 1D image vector (I) to obtain the cipher image $C1$, as shown in Equation (12).

$$z1 = (\mathrm{z} \times 10^5) \bmod 256 \tag{11}$$

$$C1 = z1 \oplus I \tag{12}$$

Perform the permutation process on $C1$ based on the sorting operation on $z2$ to obtain $C2$, as shown in Equation (13).

$$C2 = C1\big(\mathrm{sort}(z2)\big) \tag{14}$$

The substitution and permutation processes in this first stage provide strong confusion and diffusion, as the complexity level of 2D-HELS is very high, demonstrated by a LE value greater than 8 when μ=4 [48].

3.3 Second Stage Encryption

After achieving strong confusion and diffusion in the first stage, the second stage encryption is performed using 2D-SCM and extended DNA based on the FeistelX Network to enhance image security further. First, the image is divided into four equal segments (A, B, C, and D) for the encryption process based on the FeistelX network. If N is the length of the image vector, then each segment has a size ($segSize$) calculated using Equation (15), and each segment is defined using Equation (16).

$$segSize = \left\lfloor \frac{N}{4} \right\rfloor \tag{15}$$

$$\begin{aligned} A &= C2(1{:}\,\text{segSize}), \\ \text{B} &= C2(\text{segSize}+1{:}\,2\cdot\text{segSize}), \\ \text{C} &= C2(2\cdot\text{segSize}+1{:}\,3\cdot\text{segSize}), \\ \text{D} &= C2(3\cdot\text{segSize}+1{:}\,\text{N}) \end{aligned} \tag{16}$$

In the FeistelX network, there are four different operations on each image segment. Where in these operations 2D-SCM and extended DNA are used in each round of FeistelX. Equation (17),(18) are used for the generation of chaotic sequence 2D-SCM, where input value α is used as the control factor [47], $x2_o$ and $y2_o$ as initial values and the length of the chaotic sequence is $segSize$.

$$x_{n+1} = -\alpha \cdot y_n + \frac{x_n}{\exp|y_n|} \tag{17}$$

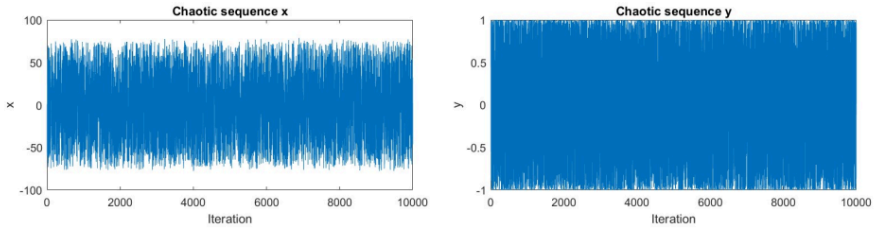
$$y_{n+1} = \sin(x_n + y_n) \tag{18}$$

Based on Equations (17) and (18), the plot of the chaotic sequence for x and y and the 2D-SCM bifurcation is presented in Figure 3.

From Figure 3, it can be seen that the complexity of the chaotic sequence is very good. The first chaotic sequence of 2D-SCM is stored in the variable $z3$ and the second chaotic sequence is stored in the variable $z4$. In each round of Feistel encryption, the encryption functions f and g which have the H property, are used. The H property ensures that the encryption functions f and g can be reversed with the function t. Therefore, in the i-th round, Equation (19) is used.

$$\begin{cases} A_{i+1} = \text{permute}\big(C_i, \text{sort}(z3)\big) \\ C_{i+1} = A_i \oplus F(C_i, K(z3i)) \\ B_{i+1} = \text{DNAop}(D_i, K(z4)) \\ D_{i+1} = G(B_i, K(z4i)) \end{cases} \tag{19}$$

Where $F(C_i, K(z3)) = \text{permute}\big(C_i, \text{sort}(z3)\big) \oplus K(z3)$ and $G(B_i, K(z4i)) = (B_i + K(z4i)) \bmod 256$



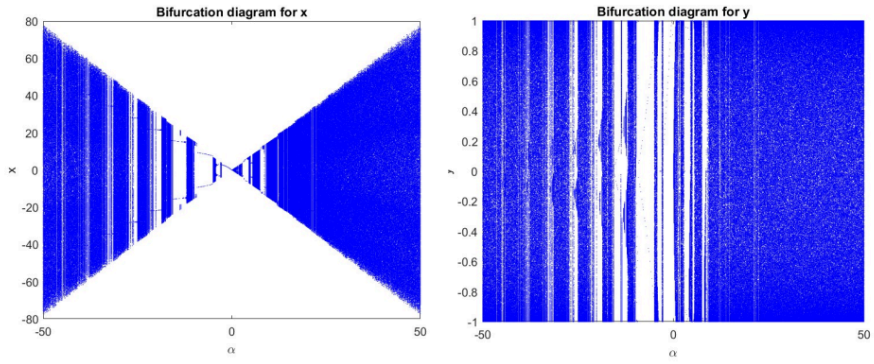


Figure 3. Chaotic sequence and bifurcation diagram plot of 2D-SCM

More details on each FeistelX stage are as follows:

1. Pixel Permutation (A to C)

   First, the chaotic sequence $z3$ is used to perform permutation on segment C_i resulting in segment A_{i+1} through the operation permute$(C_i, \text{sort}(z3))$.

2. XOR Operation (C to A)

   Then, segment C_i is combined with segment A_i using the XOR operation after the permutation of C_i. The key $K(z3i)$ is calculated as $z3i = \text{mod}\,(z3 \times 10^5, 256)$ and is used in this operation, resulting in C_{i+1}.

3. DNA Operation (B to D)

   Segment D_i is converted into a DNA sequence using the extended DNA coding method, then subjected to DNA operations with the key $K(z4)$. The extended DNA coding is performed as follows:

   a) Convert the segment into binary form, then divide it into triplet groups. Each binary triplet is converted into a nucleotide, with A = 000, a = 001, C = 010, c = 011, G = 100, g = 101, T = 110, and t = 111.

   b) Each nucleotide in the extended DNA sequence (DNA_1), is added to the corresponding nucleotide from the chaotic DNA sequence (DNA_2). The addition is performed using Equation (20).

$$DNA_{result} = mod(DNA_1 + DNA_2, 8) \quad (20)$$

Each nucleotide is mapped to the corresponding index from 0 to 7, and the result is converted back to nucleotides according to the sum result.

c) Convert DNA_{result} back to binary triplets according to the predetermined conversion rules.

d) The remaining bits from the initial conversion process (if any) are added to the end of the resulting binary sequence so that the final binary sequence is complete again.

4. Modular Operation (B and D)

Segment B_i is combined with the key $K(z4i)$ calculated as $z4i = \text{mod}\,(z4 \times 10^5, 256)$ using a modular addition operation, resulting in D_{i+1}.

Note: The above describes the first round of the FeistelX network. In the second to the last round, there is a slight modification by adding a constant value ($cons$) to $x2_o$ and $y2_o$ as inputs. This constant value can be set, but by default, it is very small, i.e., $0 < cons \leq 0.01$. The use of cons in each round further increases the complexity of 2D-SCM's randomness.

For decryption, the inverse of the encryption process is performed with the inverse function t that corresponds to property H, so in the i-th round of decryption, Equation (21) is used.

$$\begin{cases} C_i = \text{permute}^{-1}\left(A_{i+1}, \text{sort}(z3)\right) \\ A_i = C_{i+1} \oplus t\left(F(C_i, K(z31))\right) \\ D_i = \text{DNAop}^{-1}\left(B_{i+1}, \text{K}(z4)\right) \\ B_i = t\left(G(D_i, K(z4i))\right) \end{cases} \tag{21}$$

Here, $t\left(F(C_i, K(z3i))\right)$ and $t\left(G(D_i, K(z4i))\right)$ are the inverse functions of operations F and G, allowing for reconstructing the original data after the encryption process.

The extended DNA operations expand the key space and introduce a nonlinear diffusion process. The correlation between adjacent pixels is further broken by operating at the binary and nucleotide levels. The modular addition operation applied to the DNA sequences ensures that even slight differences in pixel values are significantly diffused across the ciphertext. The proposed method's two hyperchaotic maps serve distinct purposes: 2D-HELS is utilized in the first stage to perform intensive pixel scrambling and substitution, providing strong initial confusion and diffusion. Meanwhile, 2D-SCM is employed during the FeistelX rounds to generate dynamic chaotic sequences for additional permutation and diffusion operations, enhancing the complexity and security of each encryption round.

4. Results

Implementation and testing of the proposed method using datasets from the SIPI Image Database [49], as shown in Figure 4. Most of the images have dimensions of 512 × 512 pixels and were converted into grayscale format to standardize the evaluation. Some images, such as Aerial and Moon Surface, have 256 × 256 pixels, while the Male image has a dimension of 1024 × 1024 pixels. These images were selected to facilitate comparison with related studies because they represent diverse characteristics: Aerial and Moon Surface exhibit large smooth regions, Baboon and Boat display complex textures, Ruler represents highly homogeneous content, and Peppers and Male images offer moderate structural complexity. Additionally, the Lena image was also used for comparison purposes, although it is not displayed in Figure 4 due to usage restrictions by some publishers.

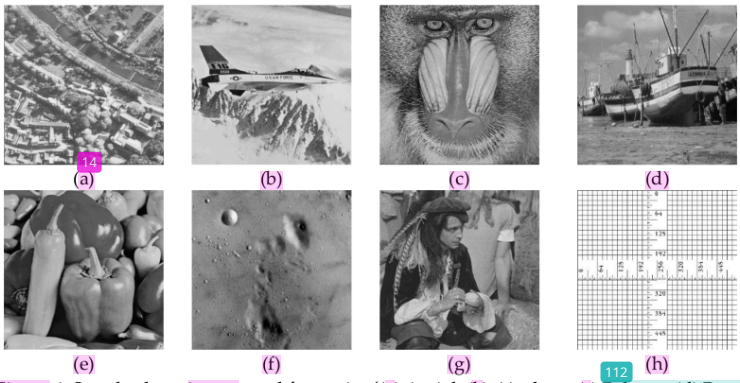


Figure 4. Standard test image used for testing{(a) Aerial; (b) Airplane; (c) Baboon; (d) Boat; (e) Peppers; (f) Moon surface; (g) Male; (h) Ruler}

4.1 Encryption Results

In this section, we present a sample of image encryption results. Not all images are shown because they relate to the number of pages. Here, we choose the ruler image, which is considered to have the highest homogeneity, as evidenced by the histogram presented in Figure 5 (d) where there are only pixels 0 and 255.

In addition to visual results, the encryption and decryption efficiency of the proposed method was also evaluated. Preliminary tests conducted on a 512×512 grayscale image showed that the average encryption time was approximately 0.95 seconds, and the decryption time was

approximately 0.88 seconds on a standard desktop computer (Intel i7, 16GB RAM). These results indicate that the method maintains acceptable computational efficiency, making it feasible for practical applications where moderate-speed processing is acceptable.

Based on the results presented in Figure 5, the proposed method successfully encrypts the most homogeneous image very well, as evidenced by the significant changes in the histogram. In the original image, there are only two bins, but after encryption, all bins from 0 to 255 have relatively uniform frequencies. However, visual measurements do not seem to be sufficient. Sections 4.2 to 4.9 will show more detailed assessments with statistical values to prove the performance of the proposed encryption method.

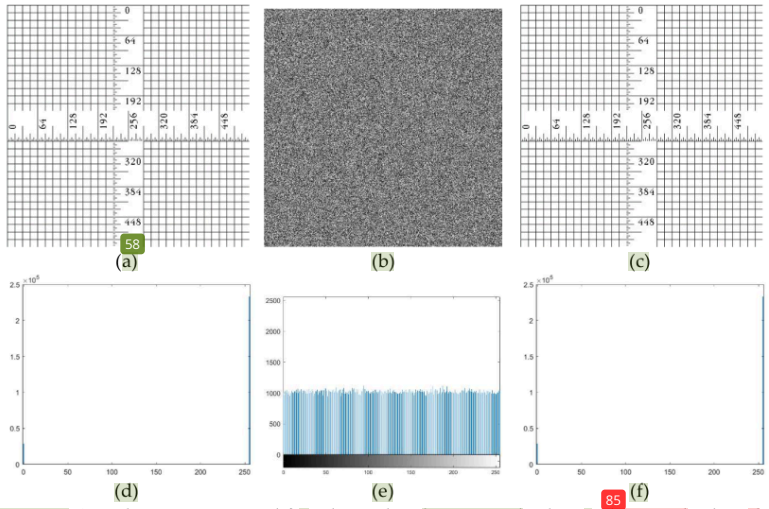


Figure 5. Sample encryption result{(a) plain ruler; (b)encrypted ruler; (c) decrypted ruler; (d) plain ruler histogram; (e) encrypted ruler histogram; (f) decrypted ruler histogram}

4.2 Chi-square assessment

The Chi-square assessment is used to measure the randomness of encrypted data by comparing the distribution of pixel values in the ciphered image to a uniform distribution. A well-encrypted image should have a near-uniform distribution of pixel values, indicating high randomness and resistance to statistical attacks. The Chi-square statistic typically ranges from 0 to infinity. Lower values indicate that the observed distribution is close to the expected uniform distribution, suggesting good randomness. For a well-encrypted image, the Chi-

square value should be low, close to the critical value corresponding to the degrees of freedom (255 for grayscale images), indicating no significant deviation from the expected distribution. In this case, a good chi-square value is less than or equal to 293.2478. Chi-square can be calculated using Equation (22), and the assessment results are presented in Table 2.

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad (22)$$

Where O_i is the observed frequency of pixel value i; E_i is the expected frequency of pixel value i, typically $E_i = \frac{\text{Total Number of Pixels}}{256}$

Table 2. Chi-square assessment and comparison with related study

Image	Ref [18]	Ref [32]	Ref [45]	Ref [47]	Ours
Lena	244.125	-	255.7102	-	224.231
Aerial	-	-	-	-	235.234
Airplane	243.654	-	-	231.697	215.343
Baboon	246.271	248.8271	250.6958	249.974	241.234
Boat	244.456	214.8063	255.2072	-	213.234
Peppers	241.462	229.6903	254.8962	237.615	225.235
Moon surface	-	-	-	-	249.324
Male	-	232.5359	-	206.254	219.232
Ruler	-	-	-	-	251.497

Based on the Chi-square assessment results in Table 2, the FeistelX encryption method combined with extended DNA and hyperchaotic systems shows consistent Chi-square values below the critical value for all test images. This indicates a nearly even pixel distribution, indicating high randomness and resistance to statistical attacks. All chi-square values are less than 293.2478. This proves that the proposed method effectively eliminates recognizable patterns in encrypted images. Thus, these results confirm that the proposed encryption method successfully improves the security of image encryption, especially against attacks based on pixel statistical analysis. Thus, the Chi-square assessment results support the claim that the proposed encryption method effectively improves the security of image encryption, especially in protecting against attacks that exploit pixel statistical distribution.

4.3 Correlation Coefficient Assessment

This metric measures the correlation between adjacent pixels in an image. In a secure cryptographic system, the correlation between adjacent pixels in the encrypted image should be close to zero, indicating that the encryption process has effectively disrupted the inherent correlation present in the original image. The correlation coefficient (r) ranges from -1 to 1. A value close to 0 indicates no correlation (ideal for encrypted images), while values close to 1 or -1 indicate a high correlation (undesirable in encryption). The correlation Coefficient of two adjacent pixels in the gray levels image (x and y) can be calculated with Equation (23), which is commonly calculated based on horizontal, diagonal, and vertical direction.

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{N}(x_i - \mu_x)^2 \sum_{i=1}^{N}(y_i - \mu_y)^2}} \quad (23)$$

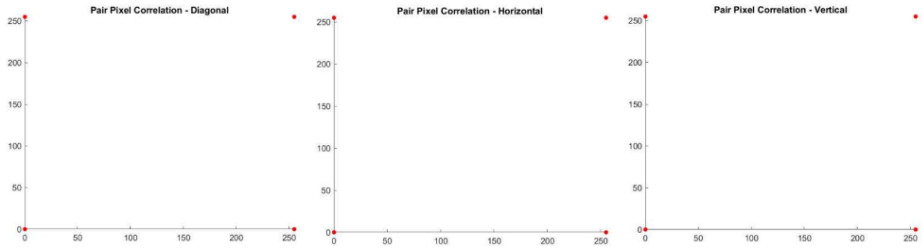
Where x_i and y_i are the gray levels of two adjacent pixels in the image; μ_x and μ_y are the means of x and y.

The assessment result of r is presented in Table 3. Meanwhile, the sample plot result of r presented in Figure 6. The r values in Table 3 show that the FeistelX encryption method produces correlation values close to zero for all directions (horizontal, vertical, and diagonal), indicating the loss of expected inter-pixel correlation in a secure encrypted image. The highest and lowest values obtained in this assessment show very minimal differences, indicating the stability and consistency of this encryption method in maintaining randomness regardless of the pixel direction. With a small gap between the highest and lowest values, the proposed method is proven stable and effective in disrupting inter-pixel correlation, strengthening image security against attacks that rely on correlation analysis.

Table 3. Correlation between adjacent pixels assessment and comparison with related study

Image	Direction	Ref [18]	Ref [42]	Ref [45]	Ref [48]	Ref [26]	Ours
Lena	D	0.0016	0.0042	0.0009	-	0.0005	0.0009
	H	0.0017	−0.0013	0.0019	-	−0.0005	-0.0011
	V	-0.0012	−0.0511	0.0012	-	−0.0028	0.0006
Aerial	D	-	-	-	−0.0019	-	0.0017

	H	-	-	-	0.0009	-	0.0025
	V	-	-	-	−0.0014	-	-0.0001
Airplane	D	0.0019	0.0008	-	-	-	-0.0009
	H	0.0023	0.0022	-	-	-	0.0015
	V	0.0018	−0.0015	-	-	-	0.0005
Baboon	D	0.0022	-	0.0004	-	0.0004	0.0007
	H	0.0015	-	0.0054	-	0.0013	-0.0001
	V	0.0021	-	0.0004	-	−0.0030	0.0031
Boat	D	0.0018	-	0.0028	0.0015	-	0.0014
	H	0.0023	-	0.0007	0.0018	-	-0.0006
	V	0.0022	-	0.0003	0.0019	-	0.0020
Peppers	D	0.0015	0.0001	0.0007	-	0.0016	0.0009
	H	0.0017	0.0047	0.0004	-	0.0001	0.0003
	V	0.0015	−0.0171	0.0014	-	−0.0046	0.0027
Moon surface	D	-	-	-	−0.0007	-	0.0019
	H	-	-	-	0.0024	-	-0.0008
	V	-	-	-	0.0032	-	0.0025
Male	D	-	-	-	0.0005	-	0.0007
	H	-	-	-	0.0031	-	0.0017
	V	-	-	-	0.0003	-	0.0011
Ruler	D	-	-	-	0.0036	-	0.0026
	H	-	-	-	0.0016	-	0.0011
	V	-	-	-	0.0039	-	0.0031



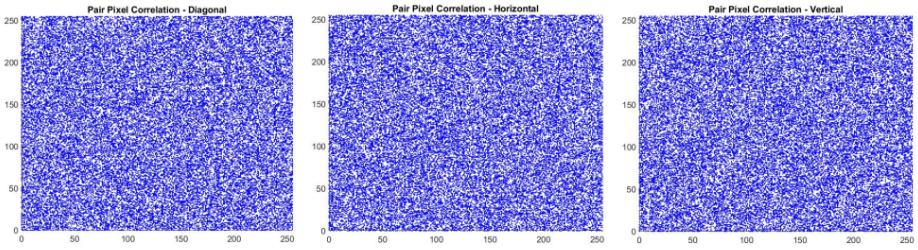


Figure 6. Sample of r plot of ruler image {top row is original r plot, bottom is encrypted r plot}

In Figure 6, it can be seen that the original r plot only has four red points on the top left, top right, bottom left, and bottom right because it only consists of pixels 0 and 255. After being encrypted, the r plot is spread evenly, consistently like the histogram shown in Figure 5 (e). The significance of achieving low correlation across different orientations is that natural images often exhibit stronger correlations along specific directions, particularly horizontal, due to common object alignments. If encryption only disrupts correlation in certain directions, residual structures may still be exploited through statistical analysis. The proposed method ensures that no exploitable structural information remains by achieving low correlation uniformly across horizontal, vertical, and diagonal directions. Integrating chaotic sequences, extended DNA operations, and FeistelX network architecture effectively disperse pixel relationships in all spatial directions, enhancing resistance against structure-based statistical attacks.

4.4 Information entropy assessment

Information entropy measures the uncertainty or randomness in an image. Higher entropy values indicate more randomness, desirable in an encrypted image to prevent statistical attacks. Entropy values range from 0 to 8 for an 8-bit grayscale image. Higher entropy values indicate higher randomness [50]. For a perfectly random image, entropy should be close to 8. For encrypted images, an entropy value close to 8 is considered ideal. Entropy can be calculated with Equation (24).

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{24}$$

Where $p(x_i)$ is the probability of occurrence of the pixel value x_i. The results of the entropy assessment and comparison with those of the prior are presented in Table 4.

Table 4. Information entropy assessment and comparison with related study

Image	Ref [18]	Ref [42]	Ref [45]	Ref [47]	Ref [48]	Ref [26]	Ours
Aerial	-		-	-	7.9974	-	7.9974
Moon surface	-	-	-	-	7.9973	-	7.9974
Lena	7.9993	7.9993	-	-	-	7.9992	7.9994
Airplane	-	7.9994	-	-	-	-	7.9993
Baboon	7.9993	7.9993	-	7.9992	-	7.9994	7.9994
Boat	-	-	7.9996	-	7.9992	-	7.9994
Peppers	7.9993	7.9992	7.9993	-	-	7.9993	7.9994
Ruler	-	-	-	-	7.9994	-	7.9993
Male	-	-	-	7.9993	7.9998	-	7.9998

The results of the information entropy assessment in Table 4 show that the proposed encryption method consistently produces entropy values close to 8, indicating a very high degree of randomness in the encrypted image. This value is close to the theoretical maximum limit for 8-bit images, indicating that this method effectively ensures that the pixel distribution does not provide information that statistical attacks can exploit. In addition, the results are slightly better than those of related studies.

These near-ideal entropy values have important implications for practical encryption scenarios. High entropy ensures that the encrypted image appears statistically uniform, significantly reducing the effectiveness of statistical attacks such as histogram analysis and entropy-based distinguishers. Furthermore, in real-world applications such as secure cloud storage and transmission over insecure networks, high-entropy ciphertexts make it extremely difficult for attackers to infer meaningful information, even in ciphertext-only or chosen-plaintext attack scenarios. Thus, the observed entropy values validate the theoretical security properties and demonstrate the proposed method's robustness in practical cryptographic environments.

4.5 Unified Average Changing Intensity (UACI) assessment

UACI quantifies the average intensity of differences between two encrypted images derived from slightly different plaintexts. High UACI values indicate that the encryption algorithm effectively diffuses plaintext changes throughout the ciphertext. An ideal UACI value should be around 33.33%, indicating effective diffusion properties of the encryption algorithm. But more detailed image dimensions also affect the ideal UACI value on the image (significance level ±0.05) with dimensions of 256×256 from 33.2824 to 33.6447, dimensions of 512×512 images from 33.3730 to 33.5541, dimensions of 1024×1024 from 33.4183 to 33.5088. UACI can be calculated with Equation (25). While the results of the UACI assessment are presented in Table 5.

$$\text{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (25)$$

Where $C1(i,j)$ and $C2(i,j)$ are the pixel values of the two encrypted images; M and N are the image's dimensions in pixels.

Table 5. UACI (%) assessment and comparison with related study

Image	Ref [18]	Ref [42]	Ref [45]	Ref [48]	Ref [26]	Ours
Aerial	-		33.4585	33.4569	-	33.3776
Moon surface	-	-	33.4161	33.4747	-	33.4805
Lena	33.4599	33.44	33.4574	-	33.48	33.4959
Airplane	33.4526	32.87	-	-	-	33.5102
Baboon	33.4772	32.64	-	-	-	33.5075
Boat	33.4890	-	-	33.4791	-	33.4440
Peppers	33.4838	33.20	-	-	33.43	33.4917
Ruler	33.4785	-	-	33.4168	-	33.5164
Male	-	-	-	33.4409	-	33.4794

The UACI values obtained and presented in Table 5 are within the specified significance limits for images with dimensions of 256×256, 512×512, and 1024×1024, indicating that the algorithm effectively propagates plaintext changes throughout the ciphertext. Although slight variations in UACI values are observed among different images, these differences are expected due to the inherent characteristics of each image, such as texture complexity and pixel distribution.

Nevertheless, all values remain within the ideal range, confirming that the proposed method maintains strong diffusion capability, ensuring that small changes in the plaintext result in significant changes in the ciphertext, which is crucial for encryption security.

4.6 Number of Pixel Change Rate (NPCR) Assessment

NPCR measures the sensitivity of the encryption algorithm to small changes in the plaintext (e.g., a single bit of pixel change). It calculates the percentage of different pixels between two encrypted images produced from slightly different plaintexts. The ideal NPCR value should be close to 100%, indicating that the encryption is highly sensitive to changes in the plaintext, thus ensuring high security. But in more detail, the NPCR value is also influenced by the image dimension with a significance level of ±0.05 for images with dimensions of 256×256, dimensions of 512×512 from ≥ 99.5893, dimensions of 1024×1024 ≥ 99.5994. NPCR can be calculated using Equation (26). The results of the NPCR assessment are presented in Table 6.

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{26}$$

Where $D(i,j)$ is a binary function to compare the binary values of the pixels of two encrypted images, 0 if the pixels are the same, 1 if different.

Table 6. NPCR (%) assessment and comparison with related study

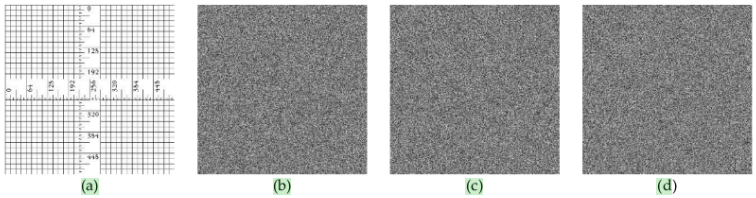
Image	Ref [18]	Ref [42]	Ref [45]	Ref [48]	Ref [26]	Ours
Aerial	-		99.6059	99.6109	-	99.5946
Moon surface	-	-	99.6063	99.5941	-	99.5978
Lena	99.6078	99.61	99.6096	-	99.61	99.6191
Airplane	99.6063	99.61	-	-	-	99.6068
Baboon	99.6092	99.60	-	-	-	99.6054
Boat	99.6014	-	-	99.6128	-	99.6146
Peppers	99.6061	99.60	-	-	99.61	99.6118
Ruler	-	-	-	99.6075	-	99.6080
Male	-	-	-	99.6190	-	99.6194

The NPCR evaluation results show that the proposed encryption method consistently produces NPCR values close to 100%, which aligns with expectations for encryption sensitive to small changes in the plaintext. All obtained NPCR values are within the ideal range

determined based on the image dimensions, indicating that the method effectively ensures that small changes in the plaintext cause significant changes in the ciphertext. This stability confirms the ability of FeistelX to maintain encryption security against attacks that exploit minimal changes in the original data. Similarly, minor variations in NPCR values among different images are consistent with theoretical expectations. Images with highly structured or homogeneous regions like Ruler and Aerial may show marginally different NPCR values than complex textured images. However, all results fall within the statistically ideal thresholds, indicating the stability and robustness of the encryption method.

4.7 Key Sensitivity Analysis

Key sensitivity analysis ensures that small changes in the encryption key lead to significant changes in the encrypted image, which is crucial for security. The encryption process should be susceptible to the key, meaning that even a single-bit change in the key should result in a completely different encrypted image. Figure 7 shows the differences in the results of image decryption with the correct key and the changes in the single-bit key, respectively, at the beginning, middle, and end of the key.



(a) (b) (c) (d)

Figure 7. Sample results of key sensitivity test {(a) correct key; (b) single-bit key modification at the beginning; (c) single-bit key modification at the middle; (d) single-bit key modification at the end}

The key sensitivity test results shown in Figure 7 confirm that the proposed encryption method is very sensitive to small changes in the encryption key. As seen in Figure 7(b), (c), and (d), changing only one bit in the key at the beginning, middle, or end produces an entirely different encrypted image from the result encrypted using the correct key (Figure 7a). This shows that the proposed method has high resistance to brute force attacks and ensures that without the proper key, decryption is impossible. Furthermore, to quantify the sensitivity, the Peak Signal-to-Noise Ratio (PSNR) between the incorrectly decrypted images and the original plaintext image was calculated, resulting in an average value below 8.2 dB. This extremely

low PSNR indicates a high level of difference, thereby validating the robustness of the proposed method against minor key modifications. This sensitivity is a key factor in ensuring the security of the encryption scheme.

4.8 NIST Assessment

The National Institute of Standards and Technology (NIST) statistical test suite is a collection of tests designed to evaluate the randomness of binary sequences generated by cryptographic algorithms. These tests help ensure that the encryption process produces outputs indistinguishable from random noise, which is essential for security. The NIST test suite involves multiple statistical tests; each test computes a p-value as $p = P(\text{Test Statistic} \leq \text{Observed Value})$, where p is the probability that the observed test statistic is less than or equal to the observed value, assuming the sequence is random. A sequence is considered random if the p-value is greater than the significance level (commonly 0.01) in most tests. Most of the NIST tests should pass for a well-encrypted sequence, indicating that the sequence behaves like a truly random sequence.

This study applied the NIST tests to binary sequences extracted from the ciphertexts generated by encrypting standard test images. Each ciphertext was converted into a binary bitstream, and the tests were conducted using a significance level of 0.01, following the default parameters of the NIST SP800-22r1a guidelines. The length of the bitstreams exceeded 10^6 bits to ensure the statistical validity of the tests and enable other researchers to reproduce the results. The NIST test result is presented in Table 7.

Table 7. NIST test assessment

No	Test Name	p-Value	Pass [y/n]
1	Frequency	0.314833449637457	y
2	Block Frequency	0.763180133167920	y
3	Cumulative Sums (Forward)	0.862046061569866	y
4	Cumulative Sums (Reverse)	0.729012438993691	y
5	Runs	0.886120007978069	y
6	Longest Run of Ones	0.747789612854265	y
7	Rank	0.788956631750734	y
8	Discrete Fourier Transform	0.339750295590680	y

9	Nonperiodic Template Matchings	0.132614268733269	y
10	Overlapping Template Matchings	0.978892696165680	y
11	Universal Statistical	0.540252373693167	y
12	Approximate Entropy	0.667269384066956	y
13	Random Excursions	0.492641866097250	y
14	Random Excursions Variant	0.280752695957940	y
15	Serial	0.837347320780669	y
16	Linear Complexity	0.683218649095200	y
Mean		0.627792367883301	16/16

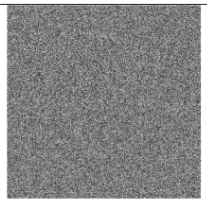
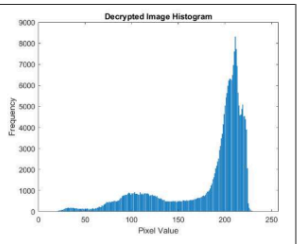
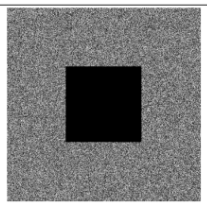
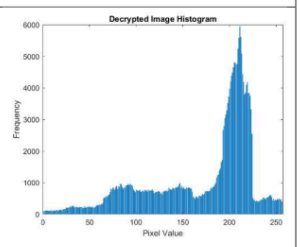
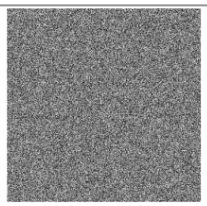
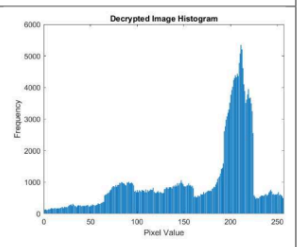
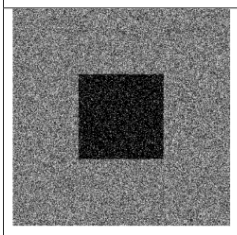
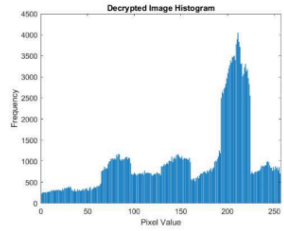
The test results using the NIST Statistical Test Suite, as shown in Table 7, confirm that all statistical tests performed on the encrypted binary sequences produce p-values greater than the significance level, demonstrating the high quality of randomness achieved. This indicates that the binary sequences generated by the proposed encryption method meet the criteria of randomness and indistinguishability from random noise, which is very important for cryptographic security. Success in all 16 NIST tests highlights the robustness of the method and its ability to generate secure ciphertexts that effectively resist statistical and distinguishability-based attacks.

4.9 Noise and Loss Attack Assessment

This assessment evaluates the robustness of the encryption algorithm against noise addition and data loss. In practical scenarios, encrypted images might be transmitted over unreliable channels where noise or data loss can occur. The resilience of the encryption algorithm under such conditions is crucial for maintaining security. Several attack tests were used in the study, namely loss with dimensions of 200×200 pixels, salt and paper noise 0.2, and their combinations, which are presented in Table 8.

Table 8. Noise and Loss Attack Assessment

Attack	Decrypted Image	Decrypted Histogram

 Without Attack		
 Loss 200×200 pixels		
 Salt and pepper (sp) 0.2		
 Loss 200×200 pixels + sp 0.2		

The test results on the robustness of the proposed encryption algorithm against noise and data loss, as shown in Table 8, show that this algorithm can preserve most of the visual information even though an attack occurs. In the scenario without attack, the decrypted image is identical to the original image, with the histogram showing the appropriate pixel distribution. When

there is a data loss of 200×200 pixels, the decrypted image maintains its primary structure, although some visible artifacts exist. The histogram shows slight deviations, but the general shape is still recognizable.

In adding salt and pepper noise of 0.2, the decrypted image shows increased noise but is still recognizable, with histograms showing only slight distortion. The combination of data loss and salt and pepper noise results in decrypted images with more artifacts and distortion, but the algorithm still manages to preserve some key details of the image. Overall, these results show that the proposed method is quite robust to noise and data loss, making it a reliable choice for use in unstable environments.

The PSNR between the decrypted and original images was measured under different attack scenarios to assess the artifact tolerance. The PSNR values were around 21 dB for salt and pepper noise, 20 dB for data loss, and 18 dB for the combined noise and loss condition. These values indicate that despite noise and data loss, the decrypted images maintain an acceptable level of visual quality, confirming the method's resilience against moderate levels of channel degradation. Overall, these results show that the proposed method is quite robust to noise and data loss, making it a reliable choice for use in unstable environments.

5. Conclusions

This study proposes an image encryption method that combines FeistelX Network with extended DNA Cryptography and two 2D hyperchaotic maps, namely 2D-SCM and 2D-HELS. The results of various tests show that the proposed method has superior performance in terms of randomness, sensitivity to key changes, resilience to statistical attacks, noise-based attacks, and data loss. The Chi-square value is consistently below the critical value, and the entropy value is close to 8, indicating high randomness. In addition, the UACI and NPCR values close to the ideal value confirm that this method is very effective in propagating plaintext changes throughout the ciphertext, ensuring strong security. Testing using the NIST Statistical Test Suite also proves that the binary sequence generated by this method meets the randomness criteria required for strong cryptographic security. The method's sensitivity to key changes, as proven through key sensitivity testing, confirms that this method is highly resistant to brute force attacks. Overall, the proposed encryption method has proven reliable and effective, making it a viable choice for image encryption applications in environments

that require high security. Based on these properties, the proposed method may also be applicable for securing sensitive images in fields such as military surveillance, medical imaging, and cloud-based storage.

Acknowledgment

This work was supported by Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, Indonesia, under Grant no 108/E5/PG.02.00.PL/2024

References

[1] M. D, M. B. Image encryption using modified perfect shuffle-based bit level permutation and learning with errors based diffusion for IoT devices. Comput Electr Eng 2022;100:107954. https://doi.org/10.1016/j.compeleceng.2022.107954.

[2] Dhahir ZS. A Hybrid Approach for Efficient DDoS Detection in Network Traffic Using CBLOF-Based Feature Engineering and XGBoost. J Futur Artif Intell Technol 2024;1:174–90. https://doi.org/10.62411/faith.2024-33.

[3] CrowdStrike. CrowdStrike 2024 Global Threat Report 2024. https://www.crowdstrike.com/global-threat-report/ (accessed July 10, 2024).

[4] Nguyen MD, Nguyen MT, Vu TC, Ta TM, Tran QA, Nguyen DT. A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes. J Comput Theor Appl 2024;2:102–17. https://doi.org/10.62411/jcta.10486.

[5] Singh A, Sivangi KB, Tentu AN. Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential. J Comput Theor Appl 2024;1:257–72. https://doi.org/10.62411/jcta.9851.

[6] Setiadi DRIM, Ghosal SK, Sahu AK. AI-Powered Steganography: Advances in Image, Linguistic, and 3D Mesh Data Hiding – A Survey. J Futur Artif Intell Technol 2025;2:1–23. https://doi.org/10.62411/faith.3048-3719-76.

[7] Zakaria SB, Navi K. Image encryption and decryption using exclusive-OR based on ternary value logic. Comput Electr Eng 2022;101:108021. https://doi.org/10.1016/j.compeleceng.2022.108021.

[8] Alsubaei FS, Eltoukhy MM, Ahmed AA, Diab H. An image encryption approach combining cross-interaction region scrambling and plainimage-related diffusion using

a dynamic external key. Alexandria Eng J 2025;114:198–230. https://doi.org/10.1016/j.aej.2024.11.040.

[9] Meng FQ, Wu G. A color image encryption and decryption scheme based on extended DNA coding and fractional-order 5D hyper-chaotic system. Expert Syst Appl 2024;254:124413. https://doi.org/10.1016/j.eswa.2024.124413.

[10] Dong Y, Zhao G, Ma Y, Pan Z, Wu R. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. Inf Sci (Ny) 2022;593:121–54. https://doi.org/10.1016/j.ins.2022.01.031.

[11] Lai Q, Zhang H. A new image encryption method based on memristive hyperchaos. Opt Laser Technol 2023;166:109626. https://doi.org/10.1016/j.optlastec.2023.109626.

[12] Es-sabry M, El Akkad N, Khrissi L, Satori K, El-Shafai W, Altameem T, et al. An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. Egypt Informatics J 2024;25:100449. https://doi.org/10.1016/j.eij.2024.100449.

[13] Wang H, Xiao D, Chen X, Huang H. Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Processing 2018;144:444–52. https://doi.org/10.1016/j.sigpro.2017.11.005.

[14] Su Y, Wang X, Gao H. Chaotic image encryption algorithm based on bit-level feedback adjustment. Inf Sci (Ny) 2024;679:121088. https://doi.org/10.1016/j.ins.2024.121088.

[15] Setiadi DRIM, Robet R, Pribadi O, Widiono S, Sarker MK. Image Encryption using Half-Inverted Cascading Chaos Cipheration. J Comput Theor Appl 2023;1:61–77. https://doi.org/10.33633/jcta.v1i2.9388.

[16] Setiadi DRIM, Rijati N. An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations. Computation 2023;11:178. https://doi.org/10.3390/computation11090178.

[17] Setiadi DRIM, Rachmawanto EH, Zulfiningrum R. Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling. J King Saud Univ - Comput Inf Sci 2022;34:6818–28. https://doi.org/10.1016/j.jksuci.2022.04.002.

[18] Bhowmik S, Acharyya S. Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm. J Inf Secur Appl 2023;72:103391. https://doi.org/10.1016/j.jisa.2022.103391.

[19] Ge M, Ye R. A novel image encryption scheme based on 3D bit matrix and chaotic map

with Markov properties. Egypt Informatics J 2019;20:45–54. https://doi.org/10.1016/j.eij.2018.10.001.

[20] Yu J, Xie W, Zhong Z, Wang H. Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. Chaos, Solitons & Fractals 2022;162:112456. https://doi.org/10.1016/j.chaos.2022.112456.

[21] Girdhar A, Kumar V. Color image encryption based on planetary encoding paradigm and 5D hyper chaotic lorenz system. Comput Electr Eng 2024;118:109352. https://doi.org/10.1016/j.compeleceng.2024.109352.

[22] Fauzyah ZAN, Sambas A, Adi PW, Setiadi DRIM. Quantum Key Distribution-Assisted Image Encryption Using 7D and 2D Hyperchaotic Systems. J Futur Artif Intell Technol 2025;2:47–62. https://doi.org/10.62411/faith.3048-3719-93.

[23] Winarno E, Nugroho K, Adi PW, Setiadi DRIM. Integrated dual hyperchaotic and Josephus traversing based 3D confusion-diffusion pattern for image encryption. J King Saud Univ - Comput Inf Sci 2023;35:101790. https://doi.org/10.1016/j.jksuci.2023.101790.

[24] Zhao M, Li L, Yuan Z. A multi-image encryption scheme based on a new n-dimensional chaotic model and eight-base DNA. Chaos, Solitons & Fractals 2024;186:115332. https://doi.org/10.1016/j.chaos.2024.115332.

[25] Rahul B, Kuppusamy K, Senthilrajan A. Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function. Optik (Stuttg) 2023;289:171253. https://doi.org/10.1016/j.ijleo.2023.171253.

[26] Zhang W, Xu J, Zhao B. DNA image encryption algorithm based on serrated spiral scrambling and cross bit plane. J King Saud Univ - Comput Inf Sci 2023;35:101858. https://doi.org/10.1016/j.jksuci.2023.101858.

[27] Zhao J, Wang S, Zhang L. Block Image Encryption Algorithm Based on Novel Chaos and DNA Encoding. Information 2023;14:150. https://doi.org/10.3390/info14030150.

[28] Alawida M. A novel DNA tree-based chaotic image encryption algorithm. J Inf Secur Appl 2024;83:103791. https://doi.org/10.1016/j.jisa.2024.103791.

[29] Almasoud AS, Alabduallah B, Alqahtani H, Aljameel SS, Alotaibi SS, Mohamed A. Chaotic image encryption algorithm with improved bonobo optimizer and DNA coding for enhanced security. Heliyon 2024;10:e25257. https://doi.org/10.1016/j.heliyon.2024.e25257.

[30] Wang S, Peng Q, Du B. Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Opt Laser Technol 2022;148:107753. https://doi.org/10.1016/j.optlastec.2021.107753.

[31] Liang Q, Zhu C. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. Opt Laser Technol 2023;160:109033. https://doi.org/10.1016/j.optlastec.2022.109033.

[32] Winarno E, Hadikurniawati W, Nugroho K, Lusiana V. Integrating Quadratic Polynomial and Symbolic Chaotic Map-Based Feistel Network to Improve Image Encryption Performance. IEEE Access 2024;12:106720–34. https://doi.org/10.1109/ACCESS.2024.3436558.

[33] Yan X, Hu Q, Teng L, Su Y. Unmanned ship image encryption method based on a new four-wing three-dimensional chaotic system and compressed sensing. Chaos, Solitons & Fractals 2024;185:115146. https://doi.org/10.1016/j.chaos.2024.115146.

[34] Stallings W. Cryptography and network security: principles and practice. 7th ed. Pearson India; 2017.

[35] JarJar A. Improvement of Feistel method and the new encryption scheme. Optik (Stuttg) 2018;157:1319–24. https://doi.org/10.1016/j.ijleo.2017.12.065.

[36] Mousavi M, Sadeghiyan B. A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box. Multimed Tools Appl 2021;80:13157–77. https://doi.org/10.1007/s11042-020-10440-4.

[37] Feng W, Qin Z, Zhang J, Ahmad M. Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel Network and Dynamic DNA Encoding. IEEE Access 2021;9:145459–70. https://doi.org/10.1109/ACCESS.2021.3123571.

[38] Gao J, Xie T. DNA computing in cryptography. Adv. Comput., vol. 129. 1st ed., Elsevier Inc.; 2023, p. 83–128. https://doi.org/10.1016/bs.adcom.2022.08.002.

[39] Elmenyawi MA, Abdel Aziem NM, Bahaa-Eldin AM. Efficient and Secure Color Image Encryption System with Enhanced Speed and Robustness Based on Binary Tree. Egypt Informatics J 2024;27:100487. https://doi.org/10.1016/j.eij.2024.100487.

[40] Berezin C-T, Peccoud S, Kar DM, Peccoud J. Cryptographic approaches to authenticating synthetic DNA sequences. Trends Biotechnol 2024;42:1002–16. https://doi.org/10.1016/j.tibtech.2024.02.002.

[41] Elamir MM, Mabrouk MS, Marzouk SY. Secure framework for IoT technology based on RSA and DNA cryptography. Egypt J Med Hum Genet 2022;23:116. https://doi.org/10.1186/s43042-022-00326-5.

[42] Mansoor S, Parah SA. HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. Multimed Tools Appl 2023;82:28769–96. https://doi.org/10.1007/s11042-023-14542-7.

[43] Pavithran P, Mathew S, Namasudra S, Srivastava G. A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems. Comput Commun 2022;188:1–12. https://doi.org/10.1016/j.comcom.2022.02.008.

[44] Li H, Yu S, Feng W, Chen Y, Zhang J, Qin Z, et al. Exploiting Dynamic Vector-Level Operations and a 2D-Enhanced Logistic Modular Map for Efficient Chaotic Image Encryption. Entropy 2023;25:1147. https://doi.org/10.3390/e25081147.

[45] Cao C, Sun K, Liu W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. Signal Processing 2018;143:122–33. https://doi.org/10.1016/j.sigpro.2017.08.020.

[46] Lai Q, Hu G, Erkan U, Toktas A. A novel pixel-split image encryption scheme based on 2D Salomon map. Expert Syst Appl 2023;213:118845. https://doi.org/10.1016/j.eswa.2022.118845.

[47] Lai Q, Hua H, Zhao X-W, Erkan U, Toktas A. Image encryption using fission diffusion process and a new hyperchaotic map. Chaos, Solitons & Fractals 2023;175:114022. https://doi.org/10.1016/j.chaos.2023.114022.

[48] Wang M, Fu X, Teng L, Yan X, Xia Z, Liu P. A new 2D-HELS hyperchaotic map and its application on image encryption using RNA operation and dynamic confusion. Chaos, Solitons and Fractals 2024;183:114959. https://doi.org/10.1016/j.chaos.2024.114959.

[49] USC Viterbi School of Engineering. SIPI Image Database n.d. http://sipi.usc.edu/database/ (accessed March 27, 2019).

[50] Raghuvanshi A, Budhia M, Patro KAK, Acharya B. FSR-SPD: an efficient chaotic multi-image encryption system based on flip-shift-rotate synchronous-permutation-diffusion operation. Multimed Tools Appl 2023. https://doi.org/10.1007/s11042-023-17700-z.

FeistelX Network-Based Image Encryption Leveraging Hyperchaotic Fusion and Extended DNA Coding

ORIGINALITY REPORT

20%	8%	20%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Qiumei Xiao, Wenxin Yu. "A random decomposition method for chaotic sequences to improve the security of image encryption", Physica Scripta, 2025 Publication	<1%
2	Tong Niu, Yi Liu, Lin Gao. "A Novel Multi Remote Sensing Image Encryption Scheme Exploiting Modified Zigzag Transformation and S-Box", Physica Scripta, 2024 Publication	<1%
3	Yang Yang, Degang Yang. "Block-based color image encryption algorithm by a novel memristor chaotic system and new RNA computation", Physica Scripta, 2024 Publication	<1%
4	Yongsheng Hu, Han Wu, Luoyu Zhou. "Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion", Alexandria Engineering Journal, 2023 Publication	<1%

5	Mehmet Demirtaş, Sabri Altunkaya. "A novel chirp-based 2D hyperchaotic map for enhanced image encryption", Physica Scripta, 2024 Publication	<1%
6	Qianqian Shi, Shaocheng Qu, Xinlei An, Xiaona Du. "A novel coupled functional neuron model and its application in medical image encryption", Nonlinear Dynamics, 2024 Publication	<1%
7	Sirui Ding, Hairong Lin, Xiaoheng Deng, Wei Yao, Jie Jin. "A hidden multiwing memristive neural network and its application in remote sensing data security", Expert Systems with Applications, 2025 Publication	<1%
8	Yan Wan, Liqun Zhou, Jiapeng Han. "Global polynomial synchronization of proportional delay memristive neural networks with uncertain parameters and its application to image encryption", Engineering Applications of Artificial Intelligence, 2025 Publication	<1%
9	Zahra rafieian bahabadi, Ali Nodehi, Rasul Enayatifar. "A novel approach to fast image encryption: Josephus Ring, DNA sequence,	<1%

and chaotic function", Multimedia Tools and Applications, 2025
Publication

---

10 Wassim Alexan, Yen-Lin Chen, Lip Yee Por, Mohamed Gabr. "Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption", Symmetry, 2023 <1%
Publication

---

11 Mingxu Wang, Xianping Fu, Lin Teng, Xiaopeng Yan, Zhiqiu Xia, Pengbo Liu. "A new 2D-HELS hyperchaotic map and its application on image encryption using RNA operation and dynamic confusion", Chaos, Solitons & Fractals, 2024 <1%
Publication

---

12 Nehal Abd El-Salam Mohamed, Hala El-Sayed, Aliaa Youssif. "Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)", Fractal and Fractional, 2023 <1%
Publication

---

13 reunir.unir.net <1%
Internet Source

---

14 Ernesto Moya-Albor, Andrés Romero-Arellano, Jorge Brieva, Sandra L. Gomez-Coronel. "Color Image Encryption Algorithm Based on a <1%

Chaotic Model Using the Modular Discrete Derivative and Langton's Ant", Mathematics, 2023
Publication

15	Jiehua Sun, Xiaoqiang Zhang, Chuxia Chen. "Image encryption algorithm based on V-shaped scanning and matrix multiplication", Physica Scripta, 2025 Publication	<1 %
16	Pramod Pavithran, Sheena Mathew, Suyel Namasudra, Gautam Srivastava. "A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems", Computer Communications, 2022 Publication	<1 %
17	discovery.researcher.life Internet Source	<1 %
18	publikasi.dinus.ac.id Internet Source	<1 %
19	www.frontiersin.org Internet Source	<1 %
20	Alfan Wijaya, Nur Ahmad, Laila Hanum, Elda Melwita, Aldes Lesbani. "Spirogyra sp. Macro-Algae-Supported NiCr-LDH Adsorbent for Enhanced Remazol Red Dye Removal", Results in Surfaces and Interfaces, 2025	<1 %

Publication

21	dlibrary.univ-boumerdes.dz:8080 Internet Source	<1%
22	Ebrahim Zarei Zefreh. "PSDCLS: Parallel simultaneous diffusion–confusion image cryptosystem based on Latin square", Journal of Information Security and Applications, 2024 Publication	<1%
23	Qiang Lai, Hanqiang Hua, Xiao-Wen Zhao, Uğur Erkan, Abdurrahim Toktas. "Image encryption using fission diffusion process and a new hyperchaotic map", Chaos, Solitons & Fractals, 2023 Publication	<1%
24	Amey S Deshpande, Varsha Daftardar-Gejji. "Enhancing the security of image communication with a new hyper-chaotic system", Physica Scripta, 2024 Publication	<1%
25	Jianghong Xiang, Shubei Liang, Liangang Qi, Yu Zhong. "Image encryption based on four-dimensional multi-parameter robust chaotic system and dynamic spiral block transformation", Physica Scripta, 2025 Publication	<1%

26	S. Aashiq Banu, Adel Ismail Al-Alawi, M. Padmaa, P. Shanmuga Priya, V. Thanikaiselvan, Rengarajan Amirtharajan. "Healthcare with datacare—a triangular DNA security", Multimedia Tools and Applications, 2023 Publication	<1%
27	Xiuli Chai, Haiyang Wu, Zhihua Gan, Yushu Zhang, Yiran Chen. "Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy", Signal Processing, 2020 Publication	<1%
28	assets.researchsquare.com Internet Source	<1%
29	Lin Teng, Yang Liu, Yafei Wang. "A multi-medical image encryption algorithm based on ROI and DNA coding", Physica Scripta, 2024 Publication	<1%
30	Vivek Verma, Sanjeev Kumar, Narbda Rani. "Novel image encryption algorithm using hybrid 3D-ICPCM and hessenberg decomposition", Nonlinear Dynamics, 2024 Publication	<1%
31	Xu, Rudan, Lina Chen, Yuanyuan Sun, and Xiaopeng Hu. "Image compression and	<1%

encryption scheme using fractal dictionary and Julia set", IET Image Processing, 2015.
Publication

32	coek.info Internet Source	<1%
33	vdocuments.site Internet Source	<1%
34	Abdolah Amirany, Kian Jafari, Mohammad Hossein Moaiyeri. "Highly reliable bio-inspired spintronic/CNTFET multi-bit per cell nonvolatile memory", AEU - International Journal of Electronics and Communications, 2023 Publication	<1%
35	De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Rahmawati Zulfiningrum. "Medical image cryptosystem using dynamic josephus sequence and chaotic-hash scrambling", Journal of King Saud University - Computer and Information Sciences, 2022 Publication	<1%
36	Mohammed Ibrahim M, Venkatesan R, Musheer Ahmad. "A Hybrid Approach of Substitution and Permutation techniques for Modern Image-Cryptosystem", Physica Scripta, 2024 Publication	<1%

37	Hemalatha Mahalingam, Padmapriya Velupillai Meikandan, Karuppuswamy Thenmozhi, Kawthar Mostafa Moria et al. "Neural Attractor-Based Adaptive Key Generator with DNA-Coded Security and Privacy Framework for Multimedia Data in Cloud Environments", Mathematics, 2023 Publication	<1%
38	Kartikey Pandey, Deepmala Sharma. "Novel image encryption algorithm utilizing hybrid chaotic maps and Elliptic Curve Cryptography with genetic algorithm", Journal of Information Security and Applications, 2025 Publication	<1%
39	Omer Kocak, Uğur Erkan, Ismail Babaoglu. "Design and practical implementation of a novel hyperchaotic system generator based on Apéry's constant", Integration, 2025 Publication	<1%
40	Submitted to Universitas Dian Nuswantoro Student Paper	<1%
41	arxiv.org Internet Source	<1%
42	orbit-lab.org Internet Source	<1%

43	Atul Kumar, Mohit Dua. "Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption", Multimedia Tools and Applications, 2021 Publication	<1%
44	Erdal Güvenoğlu. "An image encryption algorithm based on multi-layered chaotic maps and its security analysis", Connection Science, 2024 Publication	<1%
45	Submitted to Universiti Teknologi Malaysia Student Paper	<1%
46	cards.algoreducation.com Internet Source	<1%
47	De Rosal Ignatius Moses Setiadi, T. Sutojo, Supriadi Rustad, Muhamad Akrom et al. "Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption", Computers, Materials & Continua, 2025 Publication	<1%
48	Pai Liu, Shihua Zhou, Wei Qi Yan. "A 3D Cuboid Image Encryption Algorithm Based on Controlled Alternate Quantum Walk of Message Coding", Mathematics, 2022 Publication	<1%

49	Submitted to University of Glasgow Student Paper	<1%
50	patents.google.com Internet Source	<1%
51	qu.edu.iq Internet Source	<1%
52	Dong-dai Liu, Wei Zhang, Hai Yu, Zhi-liang Zhu. "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion", Signal Processing, 2018 Publication	<1%
53	Fang Yin, Ao Li, Chunyan Lv, Rui Wu, Suo Gao. "A new image encryption algorithm with feedback key mechanism using two-dimensional dual discrete quadratic chaotic map", Nonlinear Dynamics, 2024 Publication	<1%
54	Jiming Zheng, Tianyu Bao. "An Image Encryption Algorithm Using Cascade Chaotic Map and S-Box", Entropy, 2022 Publication	<1%
55	Raquel García-Bertrand, Luis Baringo, Álvaro García-Cerezo. "Introduction to probability theory", Elsevier BV, 2023 Publication	<1%

56	Shanooja M. A., Anil Kumar M. N.. "A Technique for Image Encryption Using the Modular Multiplicative Inverse Property of Mersenne Primes", Symmetry, 2025 Publication	<1%
57	Zeric Tabekoueng Njitacke, Louai A. Maghrabi, Musheer Ahmad, Turki Althaqafi. "Efficient Bit-Plane Based Medical Image Cryptosystem Using Novel and Robust Sine-Cosine Chaotic Map", Computers, Materials & Continua, 2025 Publication	<1%
58	www.iieta.org Internet Source	<1%
59	Bhaskar Panna, Sumit Kumar, Rajib Kumar Jha. "Image Encryption Based on Block-wise Fractional Fourier Transform with Wavelet Transform", IETE Technical Review, 2018 Publication	<1%
60	Cong Ding, Ru Xue. "Signal-sensing dynamic S-box image encryption with 2D Griewank–sin map", Nonlinear Dynamics, 2023 Publication	<1%
61	K. Abhimanyu Kumar Patro, Bibhudendra Acharya, Vijay Nath. "Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps", Microsystem Technologies, 2019	<1%

Publication

62	Mingjie Zhao, Lixiang Li, Zheng Yuan. " A multi-image encryption scheme based on a new -dimensional chaotic model and eight-base DNA ", Chaos, Solitons & Fractals, 2024 Publication	<1%
63	Mohit Dua, Rahul Bhogal. "Medical image encryption using novel sine-tangent chaotic map", e-Prime - Advances in Electrical Engineering, Electronics and Energy, 2024 Publication	<1%
64	Monu Singh, Naman Baranwal, K.N. Singh, A.K. Singh, Huiyu Zhou. "Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression", Journal of Information Security and Applications, 2023 Publication	<1%
65	Zhihua Gan, Xiuli Chai, Miaohui Zhang, Yang Lu. "A double color image encryption scheme based on three-dimensional brownian motion", Multimedia Tools and Applications, 2018 Publication	<1%
66	jeas.springeropen.com Internet Source	<1%

67	Akshat Tiwari, Prachi Diwan, Tarun Dhar Diwan, Mahdal Miroslav, S. P. Samal. "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication", Scientific Reports, 2025 Publication	<1%
68	Ali Shakiba. "A novel randomized one-dimensional chaotic Chebyshev mapping for chosen plaintext attack secure image encryption with a novel chaotic breadth first traversal", Multimedia Tools and Applications, 2019 Publication	<1%
69	Hassan M. Elkamchouchi, Ali E. Takieldeen, Mahmoud A. Shawky, I. M. Fouda, M. M. Khalil, A. A. Elkomy, A. Kh, Abd Elrasol. "A New Image Encryption Algorithm Combining the Meaning of Location with Output Feedback Mode", 2018 13th APCA International Conference on Control and Soft Computing (CONTROLO), 2018 Publication	<1%
70	Igor V. Anikin, Khaled Alnajjar. "Pseudo-random number generator based on fuzzy logic", 2016 International Siberian Conference	<1%

on Control and Communications (SIBCON), 2016
Publication

71 Marcin Lawnik, Lazaros Moysis, Murilo S. Baptista, Christos Volos. "Discrete one-dimensional piecewise chaotic systems without fixed points", Nonlinear Dynamics, 2024 <1%
Publication

72 Qin Liu, Ye Liang, Fu Liu, Xiulun Yang, Xiangfeng Meng. "Optical image encryption based on singular value decomposition ghost imaging and fractional chaotic mapping", Optics and Lasers in Engineering, 2025 <1%
Publication

73 Seyedeh Bahareh Zakaria, Keivan Navi. "Image encryption and decryption using exclusive-OR based on ternary value logic", Computers and Electrical Engineering, 2022 <1%
Publication

74 Usman Shahid, Shamsa Kanwal, Mahwish Bano, Saba Inam, Manal Elzain Mohamed Abdalla, Zaffar Ahmed Shaikh. "Blockchain driven medical image encryption employing chaotic tent map in cloud computing", Scientific Reports, 2025 <1%
Publication

75	Yexia Yao, Xuemei Xu, Zhaohui Jiang. "A New Chaotic Color Image Encryption Algorithm Based on Memristor Model and Random Hybrid Transforms", Applied Sciences, 2025 Publication	<1%
76	Yongming Zhang, Ruoyu Zhao, Yushu Zhang, Rushi Lan, Xiuli Chai. "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system", Journal of King Saud University - Computer and Information Sciences, 2022 Publication	<1%
77	as-proceeding.com Internet Source	<1%
78	ideas.repec.org Internet Source	<1%
79	impa.usc.edu Internet Source	<1%
80	www.qeios.com Internet Source	<1%
81	Amnah Firdous, Aqeel ur Rehman, Malik M. Saad Missen. "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2", Multimedia Tools and Applications, 2019 Publication	<1%

82	Atul Kumar, Mohit Dua. "A novel chaos map based medical image encryption scheme", The Imaging Science Journal, 2022 Publication	<1 %
83	Behnia, S., A. Akhavan, A. Akhshani, and A. Samsudin. "Image encryption based on the Jacobian elliptic maps", Journal of Systems and Software, 2013. Publication	<1 %
84	Bharti Ahuja, Rajesh Doriya, Sharad Salunke, Md. Farukh Hashmi, Aditya Gupta. "Advanced 5D logistic and DNA encoding for medical images", The Imaging Science Journal, 2023 Publication	<1 %
85	Chunhua Wang, Dong Tang, Hairong Lin, Fei Yu, Yichuang Sun. "High-dimensional memristive neural network and its application in commercial data encryption communication", Expert Systems with Applications, 2024 Publication	<1 %
86	Edy Winarno, Kristiawan Nugroho, Prajanto Wahyu Adi, De Rosal Ignatius Moses Setiadi. "Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System", IEEE Access, 2023 Publication	<1 %

87	Fanqi Meng, Zhenglan Gu. "A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System", Fractal and Fractional, 2023 Publication	<1%
88	Jyotsna Kumari Bharti, P Balasubramaniam, K Murugesan. "Image encryption algorithm based on matrix projective combination-combination synchronization of an 11-dimensional time delayed hyperchaotic system", Physica Scripta, 2024 Publication	<1%
89	Kadda Benyahia, Abdelkader Khobzaoui, Samir Benbakreti. "Hybrid image encryption: leveraging DNA sequencing and Lorenz chaotic dynamics for enhanced security", Cluster Computing, 2025 Publication	<1%
90	Linqing Huang, Shuting Cai, Mingqing Xiao, Xiaoming Xiong. "A Simple Chaotic Map-Based Image Encryption System Using Both Plaintext Related Permutation and Diffusion", Entropy, 2018 Publication	<1%
91	Moatsum Alawida. "A novel DNA tree-based chaotic image encryption algorithm", Journal	<1%

of Information Security and Applications, 2024
Publication

92 Mohamed Gabr, Yousef Korayem, Yen-Lin Chen, Por Lip Yee, Chin Soon Ku, Wassim Alexan. " —Rescale, Rotate, and Randomize: A Novel Image Cryptosystem Utilizing Chaotic and Hyper-Chaotic Systems ", IEEE Access, 2023 <1%
Publication

93 Noura Khalil, Amany Sarhan, Mahmoud A.M. Alshewimy. "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps", Optics & Laser Technology, 2021 <1%
Publication

94 P. Mathivanan, Ponnambalam Maran. "Color image encryption based on novel kolam scrambling and modified 2D logistic cascade map (2D LCM)", The Journal of Supercomputing, 2023 <1%
Publication

95 Puneet Kumar Pal, Dhirendra Kumar. "The coupled Kaplan–Yorke-Logistic map for the image encryption applications", Computers and Electrical Engineering, 2024 <1%
Publication

96	Qiuyu Zhang, Jitian Han, Yutong Ye. "Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding", IET Image Processing, 2019 Publication	<1%
97	Raman Yadav, Sachin, Phool Singh. "Multidomain asymmetric image encryption using phase-only CGH, QZS method and Umbrella map", Journal of Optics, 2024 Publication	<1%
98	Shengtao Geng, Danlei Guo, Xuncai Zhang, Yanfeng Wang, Ying Niu. "Image encryption scheme based on thorp shuffle and pseudo dequeue", Scientific Reports, 2025 Publication	<1%
99	Shuang Zhao, Joon Huang Chuah, Anis Salwa Mohd Khairuddin, Chengjie Chen. "Single inertial neuron with forced bipolar pulse: chaotic dynamics, circuit implementation, and color image encryption", Physica Scripta, 2024 Publication	<1%
100	Tarun Kumar, Suyel Namasudra. "Introduction to DNA computing", Elsevier BV, 2022 Publication	<1%
101	Yibo Huang, Ling Wang, Zhiyong Li, Qiuyu Zhang. "A new 3D robust chaotic mapping	<1%

and its application to speech encryption", Chaos, Solitons & Fractals, 2024
Publication

102	Zhenlong Man, Jianmeng Liu, Fan Zhang, Xiangfu Meng. "Research on cloud dynamic public key information security based on elliptic curve and primitive Pythagoras", Alexandria Engineering Journal, 2025 Publication	<1 %
103	www.researchgate.net Internet Source	<1 %
104	www.rsc.org Internet Source	<1 %
105	"Intelligent Systems and Pattern Recognition", Springer Science and Business Media LLC, 2025 Publication	<1 %
106	Ahmet Samil Demirkol, Muhammet Emin Sahin, Baris Karakaya, Hasan Ulutas, Alon Ascoli, Ronald Tetzlaff. "Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding", Chaos, Solitons & Fractals, 2024 Publication	<1 %
107	Bharti Ahuja, Rajesh Doriya. "GLDS: high dimensional Gauss-Logistic DNA System with	<1 %

Triad Hybrid Chaos for image encryption", Multimedia Tools and Applications, 2024
Publication

---

108 Chen Yang, Ping Pan, Qun Ding. "Image Encryption Scheme Based on Mixed Chaotic Bernoulli Measurement Matrix Block Compressive Sensing", Entropy, 2022 <1%
Publication

---

109 Hira Nazir, Imran Sarwar Bajwa, Saima Abdullah, Rafaqut Kazmi, Muhammad Sami ullah. "A Color Image Encryption Scheme combining Hyperchaos and Genetic Codes", IEEE Access, 2022 <1%
Publication

---

110 Jiangang Zuo, Meng Wang, Jie Zhang. "Design of multi-scroll chaotic attractor based on a novel multi-segmented memristor and its application in medical image encryption", Microelectronic Engineering, 2024 <1%
Publication

---

111 Juan Wang, Boyong Gao, Xingchuang Xiong, Zilong Liu, Chenbo Pei. "Multi-Objective Region Encryption Algorithm Based on Adaptive Mechanism", Electronics, 2024 <1%
Publication

---

112 Lingfei Wang, Zhibin Pan, Ruoxin Zhu. "A novel reversible data hiding scheme using <1%

SMVQ prediction index and multi-layer embedding", Multimedia Tools and Applications, 2017
Publication

113 Maram Kumar, Deepak. Ch. "Enhancing image security through a fusion of chaotic map and multi-level scrambling techniques", Signal, Image and Video Processing, 2025 <1%
Publication

114 Muhammad Umair Safdar, Tariq Shah, Asif Ali. "An effective encryption approach using a combination of a non-chain ring and a four-dimensional chaotic map", Cognitive Neurodynamics, 2025 <1%
Publication

115 Mukesh Rawat, Anil Singh Bafila, Sunil Kumar, Manish Kumar, Amit Pundir, Sanjeev Singh. "A new encryption model for multimedia content using two dimensional Brownian motion and coupled map lattice", Multimedia Tools and Applications, 2023 <1%
Publication

116 Ruoyu Meng, Xiaoqiang Zhang, Anni Xu. "Image encryption algorithm based on a l dimensional chaotic map and double-base DNA coding", Physica Scripta, 2024 <1%
Publication

117 Talha Umar, Mohammad Nadeem, Faisal Anwer. "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage", Expert Systems with Applications, 2024 <1%
Publication

118 Wei Feng, Jiaxin Yang, Xiangyu Zhao, Zhentao Qin, Jing Zhang, Zhengguo Zhu, Heping Wen, Kun Qian. "A Novel Multi-Channel Image Encryption Algorithm Leveraging Pixel Reorganization and Hyperchaotic Maps", Mathematics, 2024 <1%
Publication

119 Xuncai Zhang, Guanhe Liu, Jiali Di. "An image encryption scheme based on the four-dimensional chaotic system and the mealy finite state machine", Physica Scripta, 2024 <1%
Publication

120 Yaoqun Xu, Jiaoyang Liu, Zelong You, Tianqi Zhang. "A Novel Color Image Encryption Algorithm Based on Hybrid Two-Dimensional Hyperchaos and Genetic Recombination", Mathematics, 2024 <1%
Publication

121 Yibo Zhao, Ruoyu Meng, Yi Zhang, Qing Yang. "Image encryption algorithm based on a new <1%

chaotic system with Rubik's Cube transform and Brownian motion model", Optik, 2022
Publication

122	Z. B. Madouri, N. Hadj Said, A. Ali Pacha. "A new pseudorandom number generator based on chaos in digital filters for image encryption", Journal of Optics, 2024 Publication	<1%
123	Zhenlong Man. "Biometric information security based on double chaotic rotating diffusion", Chaos, Solitons & Fractals, 2023 Publication	<1%
124	iieta.org Internet Source	<1%
125	jmhg.springeropen.com Internet Source	<1%
126	ray.yorksj.ac.uk Internet Source	<1%
127	www.e3s-conferences.org Internet Source	<1%
128	www2.mdpi.com Internet Source	<1%
129	Biniyam Ayele Belete, Demissie Jobir Gelmecha, Ram Sewak Singh. "Online sequential Extreme learning Machine (OSELM)	<1%

based denoising of encrypted image", Expert Systems with Applications, 2025
Publication

130 Guidong Zhang, Weikang Ding, Lian Li. "Image Encryption Algorithm Based on Tent Delay-Sine Cascade with Logistic Map", Symmetry, 2020 <1%
Publication

131 Lingzhi Zhou, Han Xia, Wenming Lyu, Gesong Huang, Hongjing Chen, Hangyu Zhou, Zejie Zhang, zhou man. "Image protection scheme for bridge management systems based on quantum coupling function", Physica Scripta, 2025 <1%
Publication

132 Maryam Mousavi, Babak Sadeghiyan. "A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box", Multimedia Tools and Applications, 2021 <1%
Publication

133 J.R. Anisha, Y.P. Arul Teen. "An adaptive approach for securing patient data in intellectual disability care with 8D Hyperchaotic DNA encryption and IWT", Biomedical Signal Processing and Control, 2025 <1%
Publication

134	Manish Kumar, Aneesh Sreevallabh Chivukula, Gunjan Barua. "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain", Scientific Reports, 2025 Publication	<1%
135	PU Wang, Xiaojun Liu, Jing Xu, Chenhao Lu. "A novel image encryption method based on the cycle replacement", Physica Scripta, 2024 Publication	<1%
136	Qin Liang, Congxu Zhu. "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding", Optics & Laser Technology, 2023 Publication	<1%
137	Siva Janakiraman, Vinoth Raj R, R. Sivaraman, A. Sridevi, Har Narayan Upadhyay, Rengarajan Amirtharajan. "Integrity verified lightweight ciphering for secure medical image sharing between embedded SoCs", Scientific Reports, 2025 Publication	<1%
138	Xuncai Zhang, Mengrui Liu, Ying Niu. "Facial image encryption scheme based on improved 4-D hyperchaotic system", The Journal of Supercomputing, 2025 Publication	<1%

139	Yang Yang, Lidan Wang, Shukai Duan, Li Luo. "Dynamical analysis and image encryption application of a novel memristive hyperchaotic system", Optics & Laser Technology, 2021 Publication	<1%
140	Zhen Li, Shuang Zhang, Weijie Tan, Xianming Wu. "Enhanced secure color image encryption using a novel hyperchaotic 2D-ETCS model and cross-permutation", Nonlinear Dynamics, 2025 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		