symmetry

MDPI

Article

An Image Encryption Method Based on a Two-Dimensional Cross-Coupled Chaotic System

Caiwen Chen [1], Tianxiu Lu [1,*] and Boxu Yan [2]

[1] School of Mathematics and Statistics, Sichuan University of Science and Engineering, Zigong 643000, China; 323070108102@stu.suse.edu.cn
[2] School of Automation and Information Engineering, Sichuan University of Science and Engineering, Zigong 643000, China; 324081104103@stu.suse.edu.cn
* Correspondence: lubeeltx@suse.edu.cn; Tel.: +86-13408138464

Abstract

Chaotic systems have demonstrated significant potential in the field of image encryption due to their extreme sensitivity to initial conditions, inherent unpredictability, and pseudo-random behavior. However, existing chaos-based encryption schemes still face several limitations, including narrow chaotic regions, discontinuous chaotic ranges, uneven trajectory distributions, and fixed pixel processing sequences. These issues substantially hinder the security and efficiency of such algorithms. To address these challenges, this paper proposes a novel hyperchaotic map, termed the two-dimensional cross-coupled chaotic map (2D-CFCM), derived from a newly designed 2D cross-coupled chaotic system. The proposed 2D-CFCM exhibits enhanced randomness, greater sensitivity to initial values, a broader chaotic region, and a more uniform trajectory distribution, thereby offering stronger security guarantees for image encryption applications. Based on the 2D-CFCM, an innovative image encryption method was further developed, incorporating efficient scrambling and forward and reverse random multidirectional diffusion operations with symmetrical properties. Through simulation tests on images of varying sizes and resolutions, including color images, the results demonstrate the strong security performance of the proposed method. This method has several remarkable features, including an extremely large key space (greater than 2^{912}), extremely high key sensitivity, nearly ideal entropy value (greater than 7.997), extremely low pixel correlation (less than 0.04), and excellent resistance to differential attacks (with the average values of NPCR and UACI being 99.6050% and 33.4643%, respectively). Compared to existing encryption algorithms, the proposed method provides significantly enhanced security.

Keywords: chaotic system; chaotic performance evaluation; Zigzag transformation; multidirectional diffusion; security analysis

check for updates

Academic Editors: Xiangliang Xu, Guodong Li and Tianxian Zhang

Received: 26 June 2025
Revised: 16 July 2025
Accepted: 23 July 2025
Published: 2 August 2025

Citation: Chen, C.; Lu, T.; Yan, B. An Image Encryption Method Based on a Two-Dimensional Cross-Coupled Chaotic System. *Symmetry* **2025**, *17*, 1221. https://doi.org/10.3390/sym17081221

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the rapid growth of digital communication technologies and the increasing reliance on cloud storage and online data transfer, protecting sensitive data has become a major concern. Images, in particular, are vulnerable to breaches and attacks due to their ability to contain personal, confidential, or national security-related information. As a result, image encryption has become essential for safeguarding images during storage and transmission [1–4]. In the domain of image encryption for large datasets, traditional algorithms such as the Data Encryption Standard (DES) [5], Advanced Encryption Standard

(AES) [6], and Rivest–Shamir–Adleman (RSA) system [7] have been largely replaced by newer methods. A variety of innovative image encryption methods, using DNA coding [8], RNA coding [9,10], neural networks [11,12], cellular automata [13], Fourier transform [14], compressed sensing [15,16], chaos theory [17], or others [18,19], have emerged. Notably, encryption systems based on chaos theory have demonstrated significant advantages in enhancing the overall performance of cryptographic algorithms.

The effectiveness of chaotic image encryption algorithms largely relies on the specific attributes of the chaotic system employed. Owing to the sensitivity to initial conditions, ergodic properties, and intrinsic stochasticity, chaotic systems can significantly enhance encryption performance [20,21]. Consequently, chaotic systems have found widespread applications across various scientific disciplines, including cryptography, secure communications, information technology, mathematics, biology, medicine, economics, engineering, and physics [17,22–28]. Depending on their complexity, chaotic systems are typically divided into single-variable (one-dimensional) and multi-variable (high-dimensional) categories. One-dimensional discrete chaotic systems, characterized by their simplicity, fewer control parameters, and relatively quick generation of chaotic sequences, offer advantages in terms of efficiency. However, limited key space and lower pseudo-randomness make them more susceptible to attacks. In contrast, high-dimensional chaotic systems possess a more extensive key space and more robust chaotic behavior, providing enhanced security. Nevertheless, high-dimensional chaotic systems come with increased computational burden and higher implementation costs.

The two-dimensional (2D) chaotic system combines the simplicity of one-dimensional systems with the complexity of higher-dimensional systems, providing strong performance while maintaining efficiency. In recent years, the use of various 2D chaotic systems for image encryption has been growing. For example, Wu [24] used a 2D logical map with a complex basin structure and attractor. Hua [25] introduced a new 2D sine logistic modulated map (2D-SLMM). Zhu [26] presented a 2D chaotic map based on sine modulation and logistic coupling, called the logical modulated sine coupling logistic map (LSMCL). In addition to developing new chaotic systems and encryption algorithms, it is equally crucial to consider the role of cryptanalysis in evaluating the robustness of these methods. Recent studies have conducted in-depth cryptanalysis of various image encryption schemes [27,28]. These analyses not only revealed the potential weaknesses but also proposed significant improvement measures to enhance the security of the algorithm.

In this study, a new 2D chaotic system with cross-coupling is introduced to enhance system performance. Furthermore, a novel hyperchaotic system (2D-CFCM) was developed by combining Chebyshev, Fuch, sine, and cosine mappings. Analysis of phase diagrams, fractal diagrams (also known as bifurcation diagrams), Lyapunov exponents, and information entropy reveals that the proposed system demonstrates more extensive chaotic behaviors and increased complexity, significantly improving both the security and efficiency of encryption methods. An effective image encryption algorithm is proposed, which utilizes chaotic matrices and an enhanced Zigzag transformation. The algorithm incorporates both forward and reverse random multidirectional diffusion. The chaotic matrix-based permutation simultaneously scrambles pixel positions across both rows and columns, significantly boosting the randomness of the scrambling process and minimizing pixel correlation. The forward and reverse random multidirectional diffusion process selects diffusion directions from multiple orientations in both forward and reverse directions, thus increasing diffusion randomness and enhancing encryption security. To accommodate color image encryption, the approach was extended to process the R, G, and B components individually. The experimental results demonstrate that the proposed algorithm

ensures strong security, as confirmed by key space, information entropy, pixel correlation, and histogram analyses.

The key contributions of this work are outlined as follows:

(1) A new 2D cross-coupled chaotic system is proposed, capable of generating multiple chaotic maps. Specifically, a hyperchaotic system was developed by combining Chebyshev mapping, the Fuch map, sine mapping, and cosine mapping.

(2) The analysis of bifurcation diagrams, phase diagrams, Lyapunov exponents, and permutation entropy reveals that the proposed system exhibits a larger key space, enhanced ergodicity, and increased unpredictability, leading to more complex chaotic dynamics.

(3) An efficient image encryption scheme is introduced, which utilizes a chaotic matrix in conjunction with a Zigzag transformation for effective permutation and forward and reverse random multidirectional diffusion operations with symmetrical significance. The chaotic matrix-based permutation disrupts pixel positions by simultaneously scrambling both rows and columns in a random order. The symmetric forward and backward random multi-directional diffusion is achieved by conducting two rounds of random diffusion in multiple directions.

(4) A comprehensive evaluation of the encryption algorithm's performance is conducted, covering aspects such as key space, histogram analysis, variance, entropy, and correlation coefficient.

The organization of this paper is as follows. Section 2 presents the novel two-dimensional hyperchaotic map, 2D-CFCM. Section 3 discusses the dynamical behavior of the map with comparative performance analysis. Section 4 describes the design of the image encryption algorithm based on the proposed chaotic system. Section 5 provides simulation results and evaluates this security performance of the proposed method. Finally, Section 6 concludes the study.

2. Definition of 2D-CFCM

The chaotic properties of chaotic systems are crucial in encryption communication. Some classical chaotic mappings exhibit limited attractor distribution, low ergodicity, and insufficient unpredictability of chaotic sequences, leading to security vulnerabilities. In response to these drawbacks, this study introduces a newly developed two-dimensional cross-coupled chaotic system, which introduces two inputs and a cross-coupling mechanism to construct a more complex hyperchaotic map, as illustrated in Figure 1.

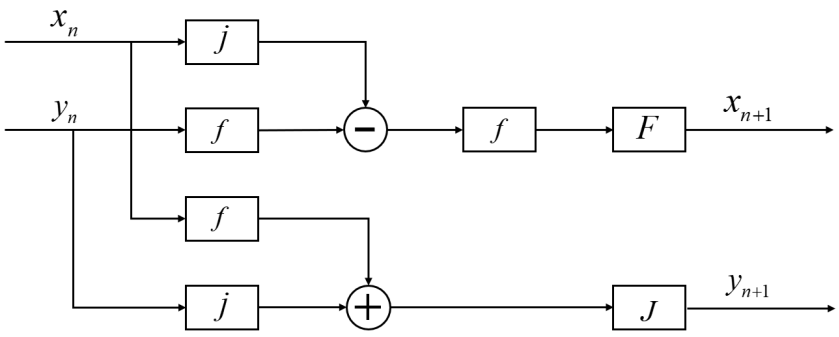


Figure 1. Structure diagram of 2D-CFCM.

As shown in Figure 1, the system consists of two independent variables, x_n and y_n, as inputs, and two dependent variables, x_{n+1} and y_{n+1}, as outputs. F and J represent one-dimensional chaotic maps. The operations $\oplus$ and $\ominus$ correspond to addition and subtraction applied to the signals, respectively. To improve the unpredictability and pseudorandomness

of the two-dimensional chaotic map, functions f and j are introduced to modulate the system, leading to the two-dimensional cross-coupled chaotic system. The system is defined as follows.

$$\begin{cases} x_{n+1} = F(f(f(y_n) - j(x_n))), \\ y_{n+1} = J(f(x_n) + j(y_n)). \end{cases} \tag{1}$$

In the cross-coupling system, the function f is defined as the sine function, while j is selected as the cosine function. The chaotic maps F and J are represented by the Chebyshev map and the Fuch map, respectively. Both the Chebyshev and Fuch maps are well-established chaotic functions, and their respective formulations are presented in Equations (2) and (3).

$$x_{n+1} = \cos\left(\alpha \cos^{-1}(x_n)\right). \tag{2}$$

$$y_{n+1} = \cos(1/y_n^2). \tag{3}$$

A novel, two-dimensional Chebyshev–Fuchs coupled map (2D-CFCM) is obtained through subtle modifications based on Equations (2) and (3).

$$\begin{cases} x_{n+1} = \cos(\alpha \cdot \cos^{-1}(\sin(\sin y_n - \cos x_n))), \\ y_{n+1} = \beta \cdot \cos(9/(\sin x_n + \cos y_n)^2). \end{cases} \tag{4}$$

α, β are control parameters and α, $\beta \in [1, +\infty)$.

3. Chaotic Property Evaluation of 2D-CFCM

To analyze the chaotic properties of 2D-CFCM, such as ergodicity, complexity, and unpredictability, we employed various analytical techniques, including phase portraits, bifurcation diagrams, Lyapunov exponents, and permutation entropy. Additionally, we compared the characteristics of 2D-CFCM with those of traditional one-dimensional chaotic maps (e.g., logistic map, sine map, and ICMIC) and two-dimensional chaotic maps (e.g., 2D-SIMM, 2D-LSMCL, 2D-logistic map, and 2D-SLMM).

3.1. Phase Diagram

The phase diagram serves as an essential analytical tool for visualizing and characterizing the dynamical behaviors of chaotic systems. The phase trajectories of chaotic motion typically form non-closed curves, a characteristic that is clearly exhibited in phase plane plots. Systems displaying prominent chaotic behavior often have attractors that cover a considerable area in the phase diagram, revealing intricate and complex structures. In order to ensure the comparability of the experiments and the optimal performance of the system, the initial values of all systems in this study were set as $(x_0, y_0) = (0.1, 0.1)$. To balance the optimal performance and practical feasibility of 2D-CFCM, the system parameters were set as $\alpha = 100$ and $\beta = 100$, resulting in the phase diagram shown in Figure 2a. Figure 2b–d are the phase diagrams of 2D-LSMCL ($\alpha = 0.75$, $\beta = 3$), 2D-SLMM ($\alpha = 1$, $\beta = 3$), and 2D-Logistic (r = 1.19) obtained based on the selection of the optimal parameters from the existing literature. Compared with this, the trajectory of 2D-CFCM covers the entire phase plane. Therefore, 2D-CFCM exhibits superior ergodicity and a broader chaotic distribution.

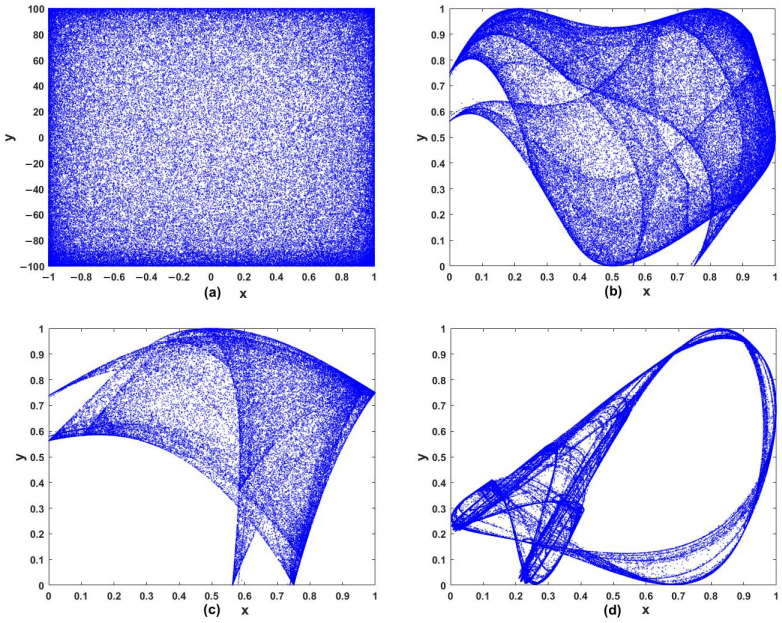


Figure 2. Attractor phase diagram. (**a**) 2D-CFCM; (**b**) 2D-LSMCL; (**c**) 2D-SLMM; (**d**) 2D-logisitc.

3.2. Bifurcation Diagram

The bifurcation diagram is an essential analytical tool for analyzing and understanding the various dynamical behavior of chaotic systems. It demonstrates how a system's motion evolves with varying control parameters and investigates its stability, periodic behavior, and whether it reaches the chaotic state [29]. Figure 3 presents the bifurcation diagram of the 2D-CFCM, where (a) illustrates the bifurcation diagram of x as it depends on system parameters α and β, with both parameters varying within the range (0, 100). (b) shows the bifurcation diagram of y as it depends on α and β, also within the range (0, 100). As observed in Figure 3, both bifurcation diagrams of the 2D-CFCM system exhibit chaotic behavior across broad range of parameter values, with no periodic states emerging. This indicates that the chaotic regime of the 2D-CFCM system is extensive.

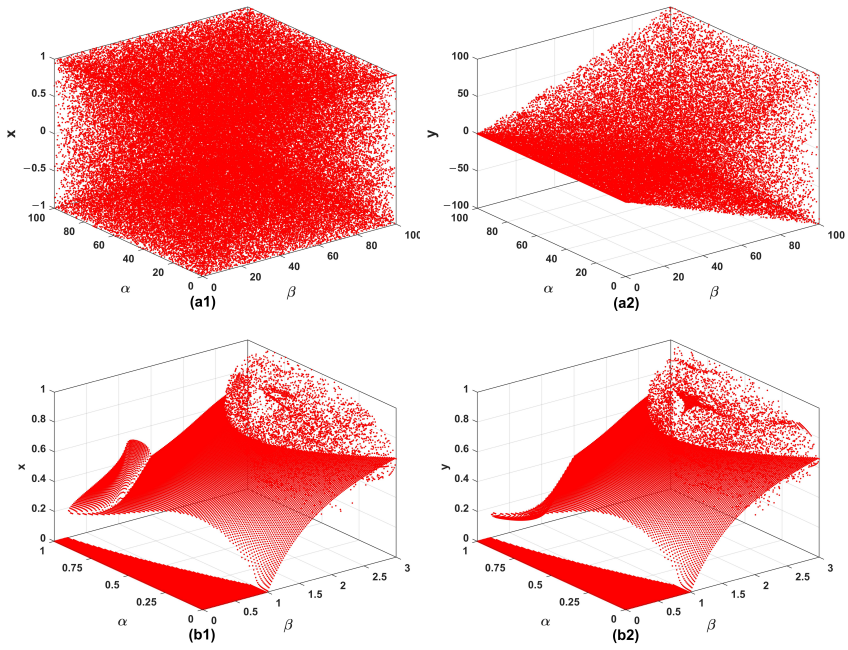


Figure 3. *Cont.*

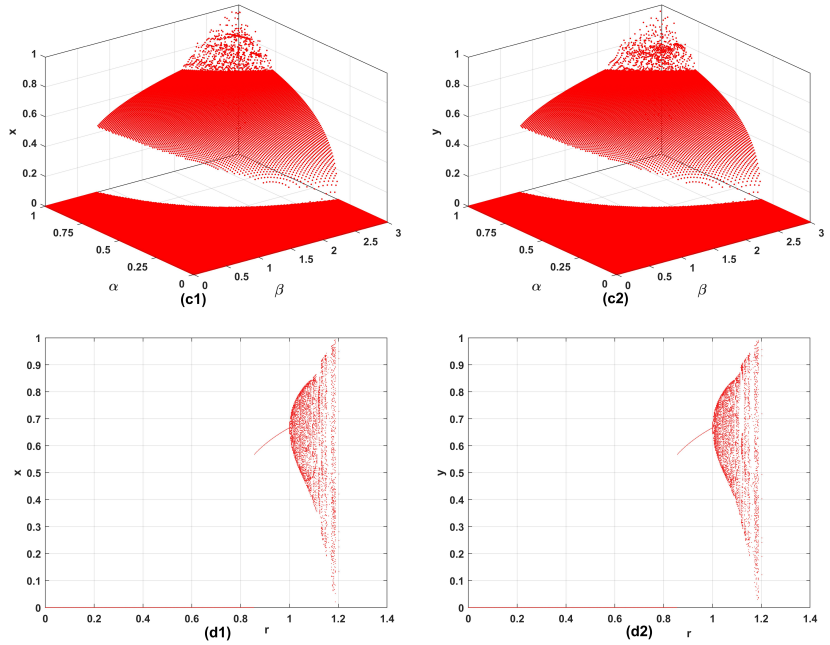


Figure 3. Bifurcation diagram of system variables x and y. (**a1**,**a2**) 2D-CFCM; (**b1**,**b2**) 2D-LSMCL; (**c1**,**c2**) 2D-SLMM; (**d1**,**d2**) 2D-Logisitc.

3.3. Lyapunov Exponent

The Lyapunov exponent (LE) is a key measure for determining the chaotic nature of a dynamical system and assessing its chaotic behavior. It quantifies how the system's trajectory responds to variations in initial conditions over time. A positive LE indicates sensitivity to initial conditions, where even small perturbations lead to rapid divergence [30]. Multiple positive LE signify a hyperchaotic state in the system. The calculation method for the LE of a two-dimensional chaotic system is described as follows. $f(x,y) = (f_1(x,y), f_2(x,y))$, i.e., for any $i \in \mathbb{N}$,

$$\begin{cases} x_{i+1} = f_1(x_i, y_i) = \cos(\alpha \cdot \cos^{-1}(\sin(\sin y_n - \cos x_n))), \\ y_{i+1} = f_2(x_i, y_i) = \beta \cdot \cos(9/(\sin x_n + \cos y_n)^2), \end{cases} \tag{5}$$

$$J(x_i, y_i) = \begin{pmatrix} \frac{\partial f_1(x,y)}{\partial x} & \frac{\partial f_1(x,y)}{\partial y} \\ \frac{\partial f_2(x,y)}{\partial x} & \frac{\partial f_2(x,y)}{\partial y} \end{pmatrix}, \tag{6}$$

where $f(x,y)$ represents the two-dimensional chaotic map. $J(x_i, y_i)$ denotes the Jacobian matrix of $f(x,y)$.

Assuming the Jacobian matrix J has eigenvalues $\lambda_1(J)$ and $\lambda_2(J)$, the LE can be computed using the following approach.

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |\lambda_i(J)|. \tag{7}$$

Figure 4 displays the LE for 2D-CFCM. Panel (a) shows the variation of the first Lyapunov exponent (LE_1) as a function of the system parameters α and β, while panel (b) presents the second Lyapunov exponent (LE_2) for the same set of parameters. It is evident that when $\alpha > 1$ and $\beta > 1$, both Lyapunov exponents are positive; this implies a hyperchaotic state for the system. With increasing α and β, the system's Lyapunov exponents (LEs) also increase, suggesting an enhancement in the chaotic behavior as the system parameters grow. Additionally, the system exhibits a heightened sensitivity to initial

conditions, suggesting the presence of complex dynamical behavior; thus, it is appropriate for cryptographic applications.

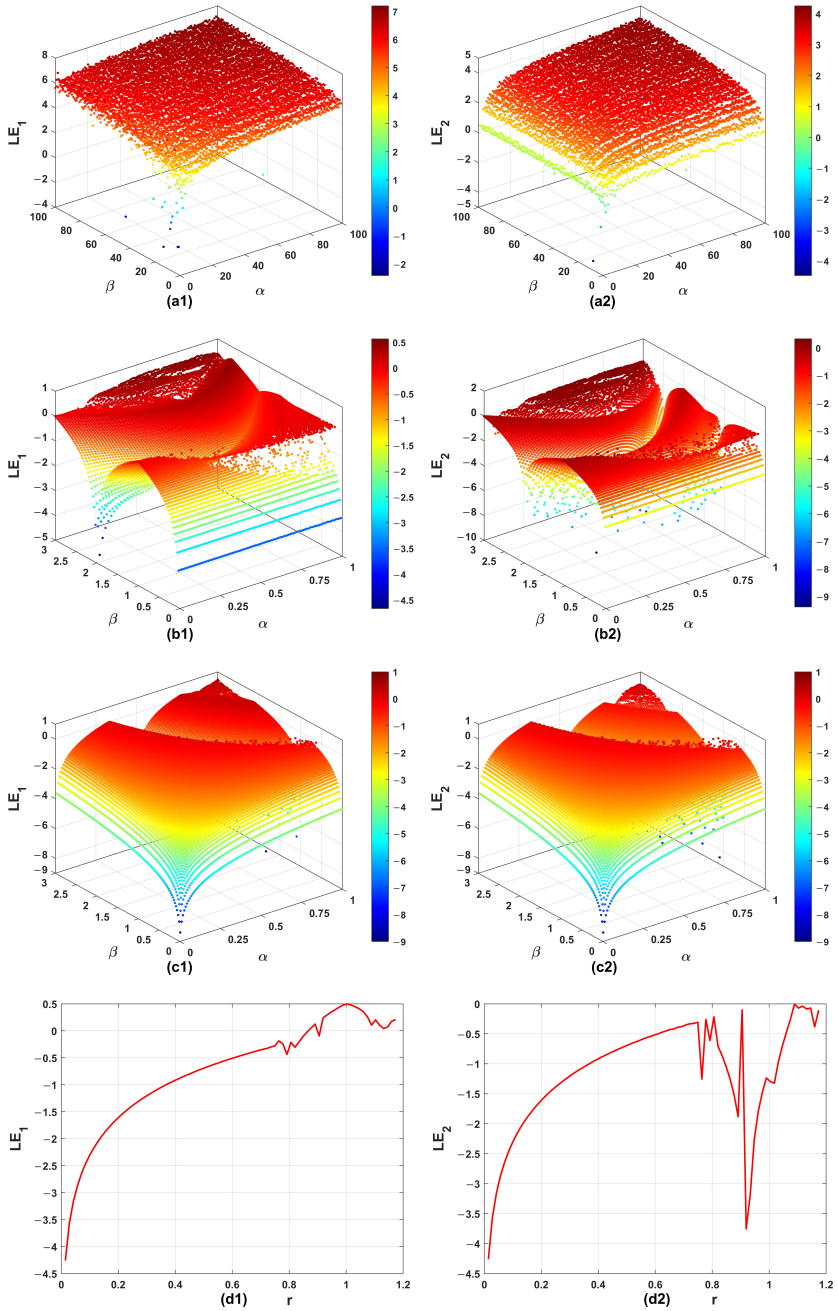


Figure 4. Lyapunov exponents of the system. (**a1**,**a2**) 2D-CFCM; (**b1**,**b2**) 2D-LSMCL; (**c1**,**c2**) 2D-SLMM; (**d1**,**d2**) 2D-Logisitc.

3.4. Complexity

The complexity measure of chaotic systems serves as a critical indicator for assessing the degree of resemblance between the system-generated chaotic sequences and purely random sequences. Due to the inherent uncertainty and nonlinearity of chaotic systems, the sequences they generate often exhibit characteristics similar to those of random sequences. The complexity of chaotic sequences significantly affects their performance in encryption tasks. The higher the value of complexity, the more the statistical properties of the chaotic sequence resemble those of a random sequence and the higher the cryptographic

security. There are many methods used to analyze the complexity. In this section, we will use replacement entropy (PE) to evaluate the complexity situation of 2D-CFCM.

Figure 5 shows the replacement entropy (PE) complexity plots of the mapped 2D-CFCM with respect to the control parameters α and β, respectively. In Figure 6a, the PE complexity of the 2D-CFCM chaotic system is compared with the PE complexity of several classical 1D chaotic systems, such as logistic maps, sinusoidal maps, and ICMIC. Figure 6b shows the PE complexity comparison of 2D-CFCM with three 2D chaotic systems: 2D-SLMM, 2D-logistic map, and 2D-LSMCL.The results show that 2D-CFCM generates chaotic sequences with a complexity value close to 1, which indicates that it has a good complexity and unpredictability. This suggests that it is well suited for generating more secure image encryption key sequences.

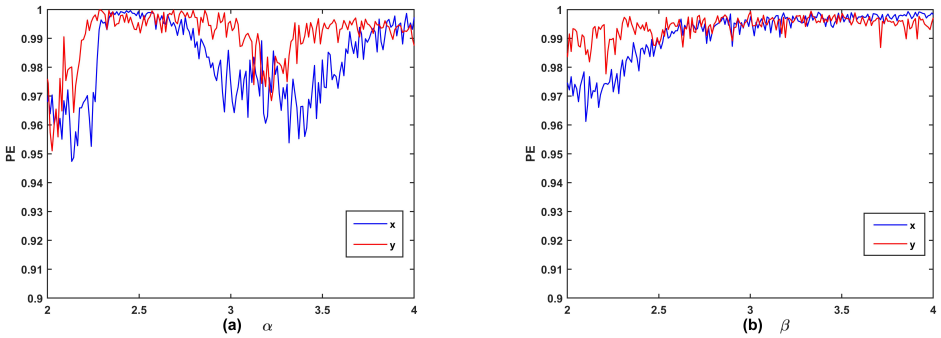


Figure 5. (**a**) Complexity graph of 2D-CFCM with respect to α. (**b**) Complexity graph of 2D-CFCM with respect to β.

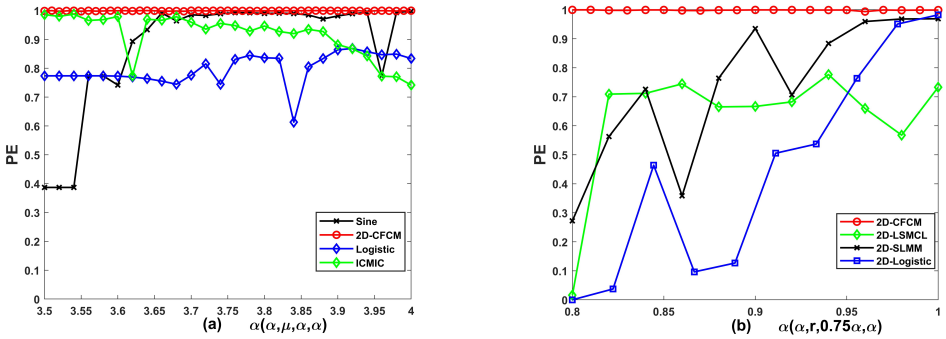


Figure 6. Permutation entropy analysis of various maps is presented. (**a**) includes 2D-CFCM, logistic map, sine map, and ICMIC; (**b**) comprises 2D-CFCM, 2D-SLMM, 2D-LSMCL, and 2D-logistic.

4. Image Encryption Method

This section primarily introduces the preparatory work and the proposed encryption method. The aforementioned two-dimensional chaotic system, 2D-CFCM, possesses an extensive chaotic range, strong unpredictability, and complex chaotic characteristics, which offers a robust basis for the development of secure encryption schemes. Based on 2D-CFCM, a new image encryption method is introduced in this section. The comprehensive flowchart outlining the algorithm is depicted in Figure 7. The algorithm consists of three stages: (1) generating keys related to the plane image; (2) performing scrambling operations based on the chaotic matrix and Zigzag transformation; (3) implementing forward and backward random multidirectional diffusion operations.

4.1. Generating Keys

The hash algorithm exhibits an extremely high sensitivity to input variations, where even a minor change results in a drastically different output, thus effectively resisting

plaintext attacks. Furthermore, the result of the hash algorithm is non-reversible, meaning that the original input cannot be reconstructed from the output, ensuring strong one-way functionality and security [31,32]. Consequently, the cryptographic algorithm proposed in this paper utilizes a hash algorithm to generate keys, thus improving system security.

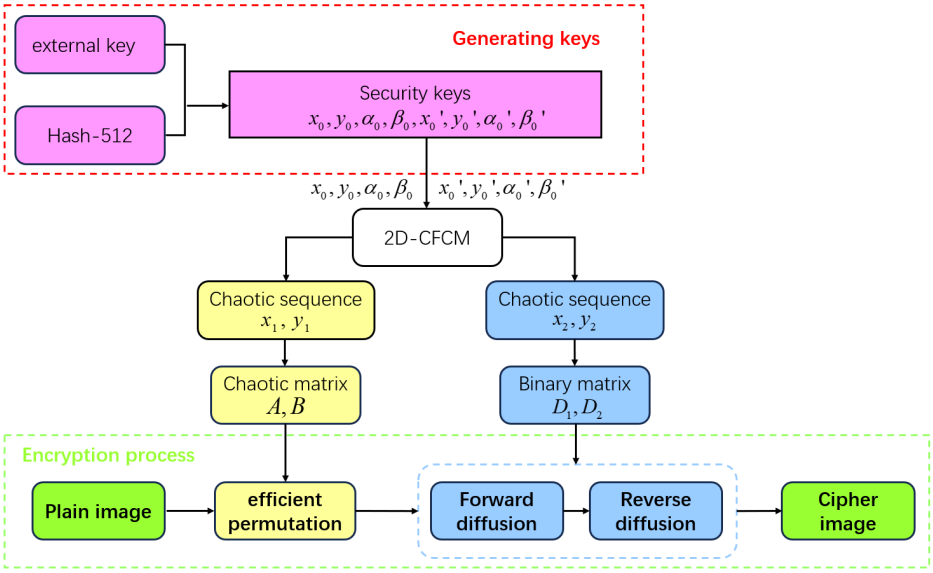


Figure 7. Flowchart of the encryption algorithm.

The 512 bit hash output, denoted as *Hash*, is generated using the SHA-512 algorithm. This hash is subsequently segmented into 64 groups of 8 bits each, represented as $h_1, h_2, \ldots, h_{63}, h_{64}$. The SHA-512 hash function can generate a unique subkey derived from the original image, thereby ensuring that distinct images produce different encryption keys. The detailed procedure of the SHA-512 algorithm is outlined as follows: $Hash = h_1, h_2, \ldots, h_{63}, h_{64}$.

By combining $h_1, h_2, \ldots, h_{63}, h_{64}$, 16 hash combinations $H_1, H_2, \ldots, H_{16}$ are obtained, which are derived from the equations outlined below.

$$\begin{cases} H_1 = min(h_1, h_2, \ldots, h_{15}, h_{16}), \\ H_2 = max(h_1, h_2, \ldots, h_{15}, h_{16}), \\ H_3 = h_1 + h_2 + \ldots + h_{15} + h_{16}, \\ H_4 = h_1 \oplus h_2 \oplus \ldots \oplus h_{15} \oplus h_{16}, \\ H_5 = min(h_{17}, h_{18}, \ldots, h_{31}, h_{32}), \\ H_6 = max(h_{17}, h_{18}, \ldots, h_{31}, h_{32}), \\ H_7 = h_{17} + h_{18} + \ldots + h_{31} + h_{32}, \\ H_8 = h_{17} \oplus h_{18} \oplus \ldots \oplus h_{31} \oplus h_{32}, \\ H_9 = min(h_{33}, h_{34}, \ldots, h_{47}, h_{48}), \\ H_{10} = max(h_{33}, h_{34}, \ldots, h_{47}, h_{48}), \\ H_{11} = h_{33} + h_{34} + \ldots + h_{47} + h_{48}, \\ H_{12} = h_{33} \oplus h_{34} \oplus \ldots \oplus h_{47} \oplus h_{48}, \\ H_{13} = min(h_{49}, h_{50}, \ldots, h_{63}, h_{64}), \\ H_{14} = max(h_{49}, h_{50}, \ldots, h_{63}, h_{64}), \\ H_{15} = h_{49} + h_{50} + \ldots + h_{63} + h_{64}, \\ H_{16} = h_{49} \oplus h_{50} \oplus \ldots \oplus h_{63} \oplus h_{64}. \end{cases} \tag{8}$$

The intermediate keys $R_1, R_2, \ldots, R_8$ are calculated by $H_1, H_2, \ldots, H_{16}$ and the external keys $t_1, t_2, \ldots, t_7, t_8 (t_i \in [0,1])$, which are described as

$$\begin{cases} R_1 = (t_1 \times t_3 + t_7) + \frac{1}{2\times 512} \times \frac{H_1}{H_2}, \\ R_2 = (t_2 + t_6 \times t_7 + t_8) + t_7 \times \frac{H_4}{H_3}, \\ R_3 = (t_1 + t_3 + t_5) \times \frac{H_8}{H_7}, \\ R_4 = (t_4 \times t_7) \times \left(\frac{H_5}{H_6} - H_5\right), \\ R_5 = (t_1 \times t_7 + t_5) - \frac{1}{2\times 512} \times \frac{H_9}{H_{10}}, \\ R_6 = (t_2 \times t_3 + t_6) - \frac{1}{2\times 512} \times \frac{H_{11}}{H_{12}}, \\ R_7 = (t_1 \times t_7 + t_2) + t_4 \times \frac{H_{13}}{H_{14}}, \\ R_8 = (t_2 \times t_3 + t_8) + \frac{1}{3\times 512} \times \frac{H_{15}}{H_{16}}. \end{cases} \tag{9}$$

Further keys (x_0, y_0, α_0, β_0) and (x'_0, y'_0, α'_0, β'_0) of the 2D-CFCM chaotic map are generated according to the following equations:

$$\begin{cases} \alpha_0 = mod\left(\left|(R_1 \times R_2 + R_5) \times 10^{16}\right|, 10\right), \\ \beta_0 = mod\left(\left|(R_3 \times R_4 + R_6) \times 10^{16}\right|, 10\right), \\ x_0 = mod(|R_1 + R_2|, 1), \\ y_0 = mod(|R_3 + R_4|, \beta_0), \end{cases} \tag{10}$$

and

$$\begin{cases} \alpha'_0 = mod\left(\left|(R_5 \times R_6 + R_7) \times 10^{16}\right|, 10\right), \\ \beta'_0 = mod\left(\left|(R_7 \times R_8 + R_8) \times 10^{16}\right|, 10\right), \\ x'_0 = mod(|R_5 + R_6|, 1), \\ y'_0 = mod(|R_7 + R_8|, \beta'_0). \end{cases} \tag{11}$$

Since the key is inherently associated with the plaintext image, even a single bit alteration in the plaintext causes a substantially different key to be generated. Therefore, the key generation algorithm exhibits a high level of security.

4.2. Chaotic Efficient Permutation

Many current image encryption methods use fixed pixel arrangements, whether in rows or columns, which may leave predictable patterns that can be exploited by attackers, and the construction of chaotic matrices is simple, thereby endangering the security of the encryption [33,34]. To improve both security and randomness, a novel image encryption algorithm that combines chaotic matrices with a Zigzag transformation is introduced. This approach randomizes the pixel positions using a secret order, enhancing the encryption's complexity. Additionally, the algorithm modifies pixel locations in both the horizontal and vertical directions simultaneously. Following the permutation, the pixels are relocated within the image, greatly diminishing their correlation. A comprehensive explanation of this chaotic permutation process is provided below.

Figure 8 shows the generation of the row matrix a_1, the column matrix b_1, and the coordinate matrices a_2 and b_2. The corresponding coordinates of the rows with the same color are changed. The elements of each row of the a_1 matrix are combined with the corresponding elements of each row of n to form the coordinates and then a modified Zigzag transformation is performed to obtain the coordinate matrix a_2. The modified Zigzag transformation is shown in Figure 9. For example, the elements of the first row of a_1 in horizontal coordinates are combined with the first element of n in column coordinates to obtain the first row of the coordinate matrix a_2: (4, 3), (2, 3), (3, 3), (5, 3), (1, 3). The elements

of the first column of the matrix b_1 are combined with the corresponding elements of the first column of n to form the coordinates, and the coordinate matrix b_2 is obtained. For example, the horizontal coordinates of the first column element of b_1 are combined with the column coordinates of each column element of m to obtain the first column of the coordinate matrix b_2: (3, 4), (2, 4), (1, 4), (5, 4), (4, 4).

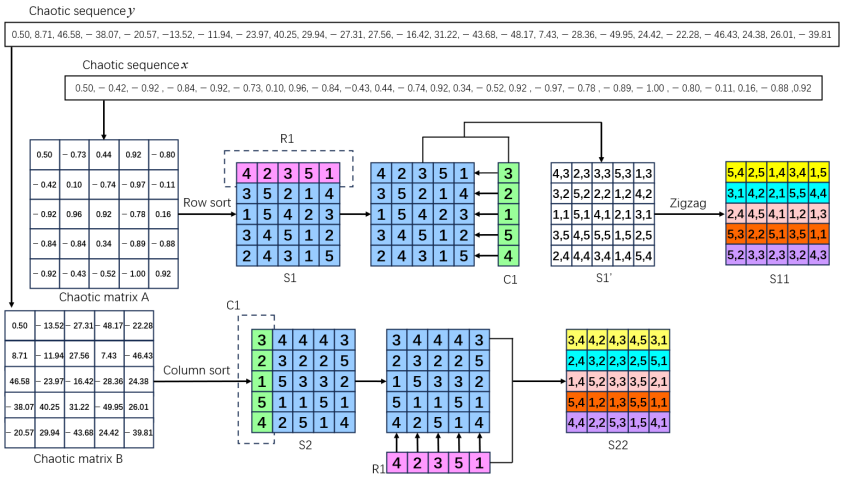


Figure 8. The generation of the position index matrices.

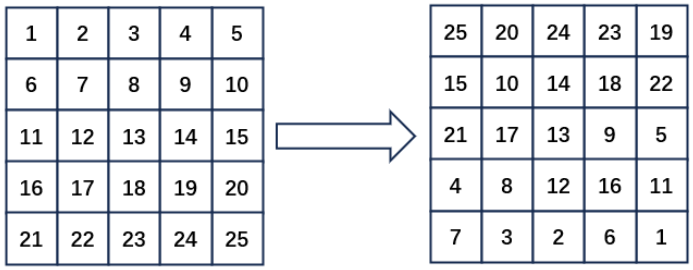


Figure 9. An example of an I-Zigzag transform.

As shown in Figure 10, the pixel positions in the image P are numbered sequentially from 1 to 25. After one disarrangement operation proposed in this paper, a chaotic matrix T is obtained. Each pixel in the image is completely rearranged depending on the coordinate matrices a_2 and b_2. Different colors are chosen to make the scrambling effect more intuitive. Without knowing the coordinate matrices, it becomes extremely challenging for an attacker to decrypt the image, which greatly improves the security of the encryption scheme.

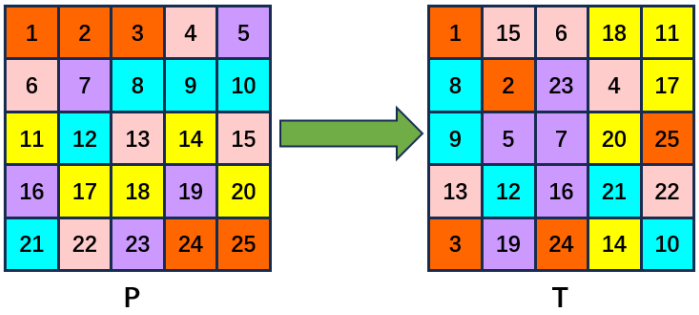


Figure 10. An example of an ordinary image T operated by scrambling.

The detailed procedure of the image scrambling operation is described as follows.

Step 1. Select the pixels corresponding to all the coordinates in the first row of b_2 from the image P and move these corresponding pixels to different positions corresponding

to all the coordinates corresponding to the first row of a_2. For example, T(5, 4) = P(3, 4), T(2, 5) = P(4, 2), T(1, 4) = P(4, 3), T(3, 4) = P(4, 5), and T(1, 5) = P(3,1), as shown in Figure 11a.

Step 2. Select the pixels corresponding to all the coordinates in the second row of b_2 from the image P. Move these corresponding pixels to different positions corresponding to all the coordinates corresponding to the second row of a_2. For example, T(3, 1) = P(2, 4), T(4, 2) = P(3, 2), T(2, 1) = P(2, 3), T(5, 5) = P(2, 5), and T(4, 4) = P(5, 1), as shown in Figure 11b.

Step 3. Select the pixels corresponding to all the coordinates in the third row of b_2 from the image P and move these corresponding pixels to different positions corresponding to all the coordinates corresponding to the third row of a_2. For example, T(2, 4) = P(1, 4), T(4, 5) = P(5, 2), T(4, 1) = P(3, 3), T(1, 2) = P(3, 5), and T(1, 3) = P(2, 1), as shown in Figure 11c.

Step 4. Select the pixels corresponding to all the coordinates in the fourth row of b_2 from the image P. Move these corresponding pixels to different positions corresponding to all the coordinates corresponding to the fourth row of a_2. For example, T(5, 3) = P(5, 4), T(2, 2) = P(1, 2), T(5, 1) = P(1, 3), T(3, 5) = P(5, 5), and T(1, 1) = P(1, 1), as shown in Figure 11d.

Step 5. Select the pixels corresponding to all the coordinates in the fifth row of b_2 from the image P. Move these corresponding pixels to different positions corresponding to all the coordinates corresponding to the fifth row of a_2. For example, T(5, 2) = P(4, 4), T(3, 3) = P(2, 2), T(2, 3) = P(5, 3), T(3, 2) = P(1, 5), and T(4, 3) = P(4, 1), as shown in Figure 11e.

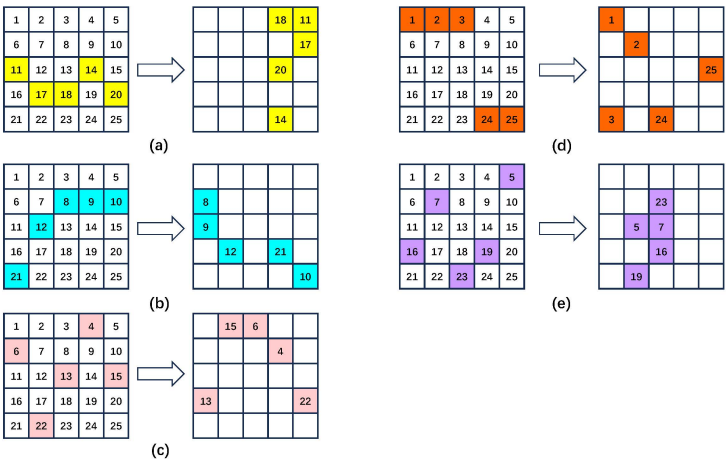


Figure 11. Anexample of the scrambling process of a numerical matrix. (**a**) the first row; (**b**) the second row; (**c**) the third row; (**d**) the fourth row; (**e**) the fifth row.

The permutation process used in the encryption stage is inherently reversible. During decryption, the same initial keys and parameters of the 2D cross-coupled chaotic map (2D-CFCM) are employed to regenerate the identical chaotic sequences. These sequences are then used to reconstruct the original permutation index. Based on this index, an inverse permutation operation is performed on the encrypted image, whereby the scrambled pixels are remapped to their original positions, thus restoring the original spatial structure of the image. This inverse permutation procedure is highly sensitive to the correctness of the secret keys. Even a minute deviation in the key values will result in an incorrect chaotic sequence, ultimately causing the decryption to fail. This high key sensitivity ensures the security and confidentiality of the encrypted image data.

4.3. Forward and Reverse Random Multidirectional Diffusion

The core objective of diffusion is to propagate the effect of a pixel's change to other pixel locations, thereby enhancing the encryption system's sensitivity to variations in the plaintext. An ideal encryption algorithm should demonstrate strong diffusion properties, ensuring that minor modifications to the plaintext image induce widespread alterations

in the ciphertext image. Currently, most diffusion methods adopt a fixed pixel processing order, where each pixel is only influenced by its preceding pixel. This approach somewhat weakens the encryption effectiveness. To address this issue, we propose a forward and backward random multi-directional diffusion method with symmetrical characteristics. This method selects the diffusion direction based on different chaotic matrices. It is achieved through two rounds of random diffusion in multiple directions. The forward diffusion and the backward diffusion are symmetrically related in structure and mechanism. This diffusion algorithm can modify pixels in each direction at each position, thereby improving the performance of this diffusion method. A detailed description of the forward and reverse random multidirectional diffusion process is provided below.

Assume that the dimension of the matrix T is $M \times N$. The initial values $x'_0, y'_0, \alpha'_0, \beta'_0$ are obtained from Equation (11). Two chaotic sequences, $\{x'_p\}$ and $\{y'_q\}$, each of length $M \times N$, are generated according to Equation (4). Then, the matrices B_1 and B_2 are constructed by the following Equations (12) and (13):

$$\begin{aligned} X' &= \mathrm{mod}(\mathrm{floor}(x'_p \times 10^{25}), 256), \\ Y' &= \mathrm{mod}(\mathrm{floor}(y'_q \times 10^{25}), 256). \end{aligned} \tag{12}$$

$$\begin{aligned} B_1 &= \mathrm{reshape}(X', [M, N]), \\ B_2 &= \mathrm{reshape}(Y', [M, N]). \end{aligned} \tag{13}$$

where 'floor' represents rounding down and 'reshape' represents reshaping.

The iterative equation for the forward random multidirectional diffusion process is as follows:

$$R(p,q) = \begin{cases} \mathrm{mod}(T(1,1) \oplus B_1(1,1), 256) & (p = 1, q = 1); \\ \mathrm{mod}(T(1,q) \oplus B_1(1,q) \oplus R(1,q-1), 256) & (p = 1, 2 \le q \le N); \\ \mathrm{mod}(T(p,1) \oplus B_1(p,1) \oplus R(p-1,1), 256) & (2 \le p \le M, q = 1); \\ \mathrm{mod}\begin{pmatrix} T(p,q) \oplus B_1(p,q) \oplus R(p-1,q-1) \\ \oplus R(p,q-1) \oplus R(p-1,q) \end{pmatrix}, 256 & (2 \le p \le M, 2 \le q \le N). \end{cases} \tag{14}$$

where T is the input variable of forward diffusion, R is the output variable of forward diffusion, B_1 is the key used for forward diffusion, and symbol $\oplus$ denotes the bit-level XOR operation.

The schematic diagram of forward stochastic multidirectional diffusion is shown in Figure 12. Different colors represent the different equations used in the encryption process, and the arrows indicate that the pixels at this coordinate are related to the pixels at other coordinates. Therefore, the decryption equation for forward stochastic multidirectional diffusion can be obtained by the following computational procedure.

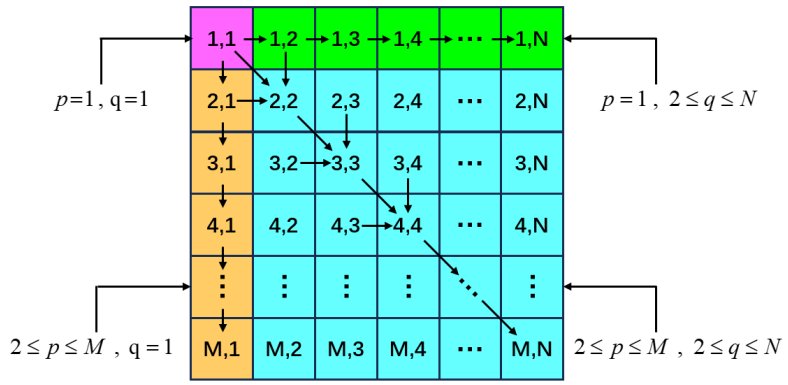


Figure 12. Diagram of forward random multidirectional diffusion.

Step 1. Remove the 'mod' operation in the forward random multinomial diffusion equation.

$$R(p,q) = \begin{cases} \mathrm{mod}(T(1,1) \oplus B_1(1,1), 256) & (p=1, q=1); \\ \mathrm{mod}(T(1,q) \oplus B_1(1,q) \oplus R(1,q-1), 256) & (p=1, 2 \le q \le N); \\ \mathrm{mod}(T(p,1) \oplus B_1(p,1) \oplus R(p-1,1), 256) & (2 \le p \le M, q=1); \\ \mathrm{mod}\begin{pmatrix} T(p,q) \oplus B_1(p,q) \oplus R(p-1,q-1) \\ \oplus R(p,q-1) \oplus R(p-1,q) \end{pmatrix}, 256 & (2 \le p \le M, 2 \le q \le N). \end{cases} \tag{15}$$

$$= \begin{cases} T(1,1) \oplus B_1(1,1) + 256n_{1,1} & (p=1, q=1); \\ T(1,q) \oplus B_1(1,q) \oplus R(1,q-1) + 256n_{1,q} & (p=1, 2 \le q \le N); \\ T(p,1) \oplus B_1(p,1) \oplus R(p-1,1) + 256n_{p,1} & (2 \le p \le M, q=1); \\ \begin{pmatrix} T(p,q) \oplus B_1(p,q) \oplus R(p-1,q-1) \\ \oplus R(p,q-1) \oplus R(p-1,q) + 256n_{p,q} \end{pmatrix} & (2 \le p \le M, 2 \le q \le N). \end{cases} \tag{16}$$

Step 2. Calculate the diffusion input matrix $T(p,q)$.

$$T(p,q) = \begin{cases} R(1,1) \oplus B_1(1,1) + 256n_{1,1} & (p=1, q=1); \\ R(1,q) \oplus B_1(1,q) \oplus R(1,q-1) + 256n_{1,q} & (p=1, 2 \le q \le N); \\ R(p,1) \oplus B_1(p,1) \oplus R(p-1,1) + 256n_{p,1} & (2 \le p \le M, q=1); \\ \begin{pmatrix} R(p,q) \oplus B_1(p,q) \oplus R(p-1,q-1) \\ \oplus R(p,q-1) \oplus S(p-1,q) + 256n_{p,q} \end{pmatrix} & (2 \le p \le M, 2 \le q \le N). \end{cases} \tag{17}$$

$$= \begin{cases} \mathrm{mod}(R(1,1) \oplus B_1(1,1), 256) & (p=1, q=1); \\ \mathrm{mod}(R(1,q) \oplus B_1(1,q) \oplus R(1,q-1), 256) & (p=1, 2 \le q \le N); \\ \mathrm{mod}(R(p,1) \oplus B_1(p,1) \oplus R(p-1,1), 256) & (2 \le p \le M, q=1); \\ \mathrm{mod}\begin{pmatrix} R(p,q) \oplus B_1(p,q) \oplus R(p-1,q-1) \\ \oplus R(p,q-1) \oplus R(p-1,q) \end{pmatrix}, 256 & (2 \le p \le M, 2 \le q \le N). \end{cases} \tag{18}$$

The reverse random multinomial diffusion operation is described as follows:

$$C(p,q) = \begin{cases} \mathrm{mod}(R(M,N) \oplus B_2(M,N), 256) & (p=M, q=N); \\ \mathrm{mod}(R(M,q) \oplus B_2(M,q) \oplus C(M,q+1), 256) & (p=M, 1 \le q \le N-1); \\ \mathrm{mod}(R(p,N) \oplus B_2(p,N) \oplus C(p+1,N), 256) & (1 \le p \le M-1, q=N); \\ \mathrm{mod}\begin{pmatrix} R(p,q) \oplus B_2(p,q) \oplus C(p+1,q+1) \\ \oplus C(p+1,q) \oplus C(p,q+1) \end{pmatrix}, 256 & (1 \le p \le M-1, 1 \le q \le N-1). \end{cases} \tag{19}$$

where R is the input variable of the reverse diffusion, C is the output variable of the reverse diffusion, B_2 is the reverse diffusion key, and symbol $\oplus$ denotes the bit-level XOR operation.

The schematic diagram of reverse random multidirectional diffusion is shown in Figure 13. The meanings of the colors and arrows are the same as those in Figure 12. Similar to the decryption process of forward stochastic multidirectional diffusion, the decryption equation of reverse stochastic multidirectional diffusion can also be described by the following equation.

Step 1. Remove the 'mod' operation in the reverse random multinomial diffusion equation.

Step 2. Calculate the diffusion input matrix $R(p,q)$.

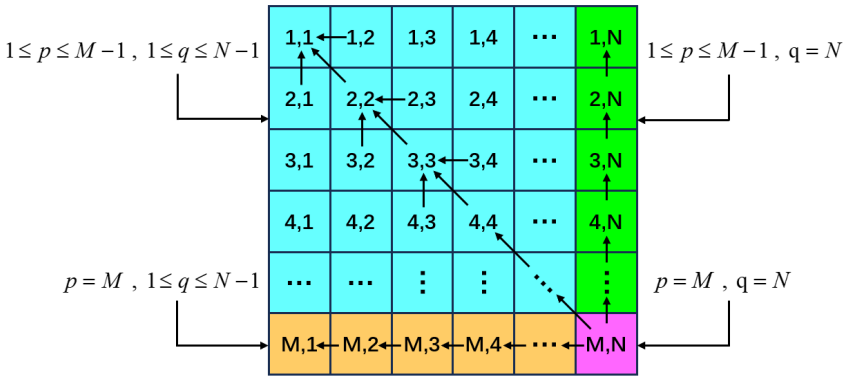


Figure 13. Diagram of reverse random multidirectional diffusion.

$$R(p,q) = \begin{cases} \mathrm{mod}(C(M,N) \oplus B_2(M,N), 256) & (p = M, q = N); \\ \mathrm{mod}(C(M,q) \oplus B_2(M,q) \oplus C(M,q+1), 256) & (p = M, 1 \le q \le N-1); \\ \mathrm{mod}(C(p,N) \oplus B_2(p,N) \oplus C(p+1,N), 256) & (1 \le p \le M-1, q = N); \\ \mathrm{mod}\begin{pmatrix} C(p,q) \oplus B_2(p,q) \oplus C(p+1,q+1) \\ \oplus C(p+1,q) \oplus C(p,q+1) \end{pmatrix}, 256 & (1 \le p \le M-1, 1 \le q \le N-1). \end{cases} \tag{20}$$

5. Simulation Results and Performance Analysis

This section comprehensively evaluates the encryption performance and security of the proposed algorithm through various testing methods applied to color images of different sizes. These simulation experiments were all conducted on MATLAB 2020b on a compatible Windows-10-operating-system computer (with 8.00 GB of memory and an Intel(R) Core(TM) i5-7300HQ CPU @ 2.50 GHz). All the experimental images were sourced from three renowned benchmark databases: https://sipi.usc.edu/database/ (accessed on 22 July 2025) USC-SIPI, https://www.imageprocessingplace.com/root_files_V3/image_databases.htm (accessed on 22 July 2025) IPP, and https://www.cs.cmu.edu/~cil/v-images.html (accessed on 22 July 2025) CVIT. The test images selected included a 256 × 256 Lena image, a 512 × 512 Aircraft image, a 512 × 512 Sailboat image, a 1024 × 1024 Satellite map image, and a 768 × 512 Butterfly image. The simulation results, as illustrated in Figure 14, demonstrate that the encrypted images effectively conceal the plaintext information. In addition to performing encryption tests on these images, a comprehensive security analysis of the encryption method was performed, including key space analysis, entropy, histogram analysis, chi-squared test, and correlation analysis. Through this comprehensive analysis, it was demonstrated that the proposed encryption method delivers effective security performance when applied to color images across a range of different sizes and resolutions.

5.1. Key Space Analysis

Brute-force attacks involve systematically attempting to crack a cryptographic key by exhaustively trying all possible combinations of passwords or passphrases until the correct one is found. Over time, images encrypted with shorter keys become more vulnerable to such attacks, while longer keys provide stronger protection, making short-term decryption nearly impossible. Evaluating the size of the key space is crucial for assessing the strength of encryption systems against brute-force attacks. A key space larger than 2^{100} is typically regarded as robust enough to resist such attacks [35].

The keys used in this scheme are $t_1, t_2, \ldots, t_7, t_8$, along with SHA-512. Assuming the precision accuracy to be 10^{-16}, the key total space of the eight input keys can be approximated as $10^{16\times 8} = 10^{128}$, which is greater than $10^{120} \approx 2^{10\times 40}$. In contrast, the key space is generated during the key creation stage using 2^{512}. As such, the total key space is greater than 2^{912}, which is significantly greater than 2^{100}, thus meeting the required security

level. A comparison of the key space of this scheme with that of several previous schemes is presented in Table 1. As shown, compared with the reference method, this scheme has a better key space, thereby providing a stronger capability to withstand brute-force attacks.

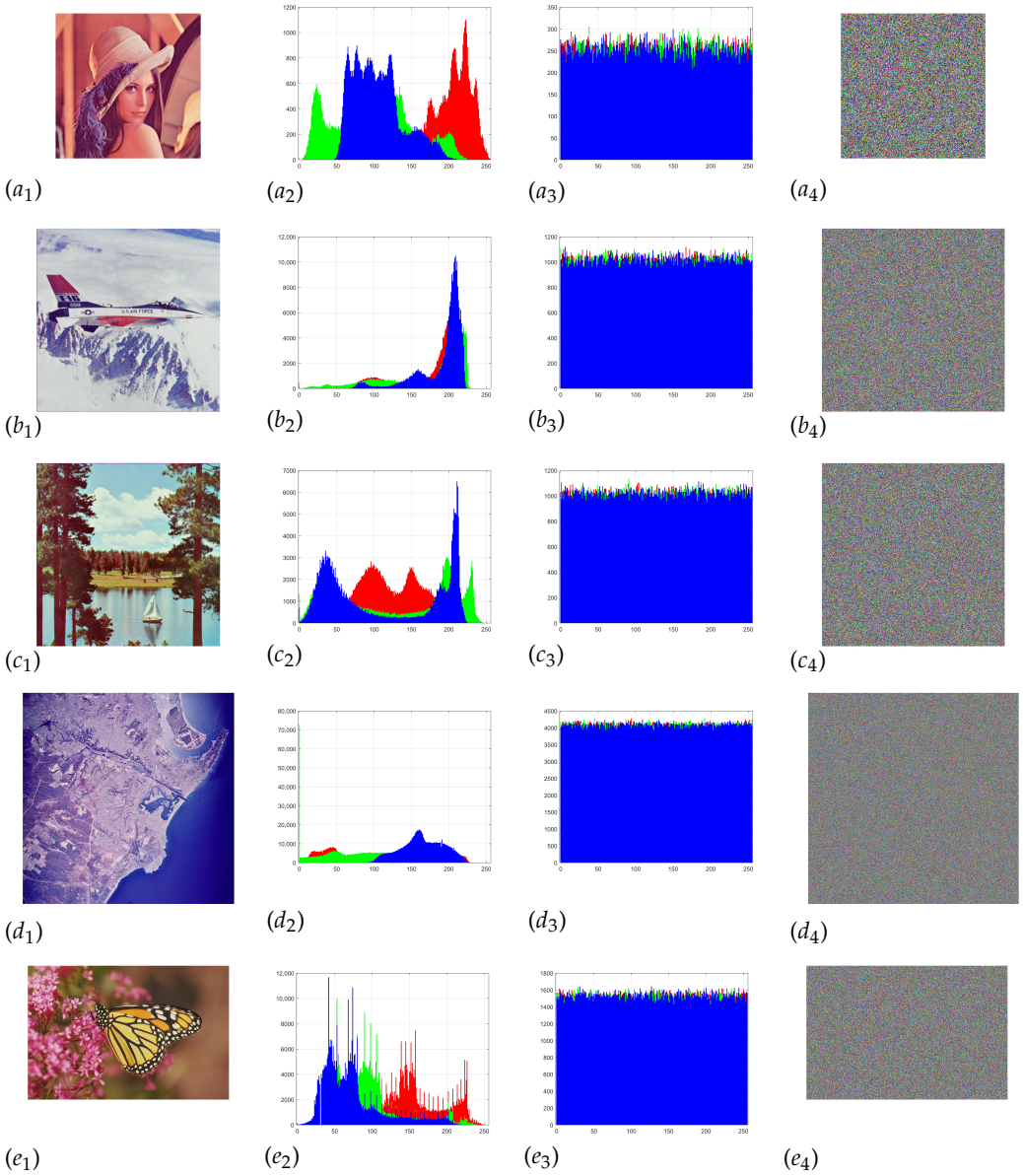


Figure 14. Encryption effect diagrams of color images. (a_1–a_4) Lena (256 × 256 × 3); (b_1–b_4) aircraft (512 × 512 × 3); (c_1–c_4) sailboat (512 × 512 × 3); (d_1–d_4) satellite map (1024 × 1024 × 3); (e_1–e_4) butterfly (768 × 512 × 3).

Table 1. Key space comparison.

Scheme	Key Space	Scheme	Key Space	Scheme	Key Space
Ref. [36]	2^{209}	Ref. [37]	10^{64}	Ref. [38]	2^{128}
Ref. [39]	2^{260}	Ref. [40]	2^{512}	Ref. [41]	2^{168}
Ref. [42]	2^{398}	Ref. [43]	2^{512}	Proposed	$>2^{912}$

5.2. Histogram Analysis

Histograms are commonly used to statistically evaluate image encryption algorithms. They graphically show the distribution of pixel intensities across grayscale levels, re-

flecting the image's grayscale characteristics. A plaintext image typically has distinct statistical patterns, while an ideally encrypted image disrupts these patterns, resulting in a uniform grayscale distribution in the ciphertext, effectively concealing the original image's information.

Experimental evaluations on standard test images with different resolutions (e.g., Lena, airplane, sailboat, satellite, and butterfly) showed that the image encryption method in this study significantly destroyed the original grayscale distribution. As shown in Figure 14, where red, green, and blue correspond to the R, G, and B channels respectively, the histogram distribution of the image after encryption was very homogeneous, indicating an equal frequency of gray levels. This uniformity indicated that the image content was completely obfuscated and, therefore, statistical analysis could not extract meaningful information. Thus, the algorithm exhibits strong resistance to statistical attacks.

5.3. Variance and Chi-Square Analysis

An uneven pixel value distribution in an image typically indicates the presence of important structural or feature details. This distribution characteristic can enable an attacker to obtain relevant data. In contrast, when the pixel values exhibit a uniform distribution, the statistical nature of the original image can be effectively hidden, thus enhancing the resistance of this encryption algorithm to statistical attacks. The variance var(X) and the Chi-square χ^2 tests for a grayscale image can be calculated using Equations (21) and (22), respectively.

$$var(X) = \frac{1}{n^2} \sum_{i=0}^{n} \sum_{j=1}^{n} \frac{1}{2} (x_i - x_j)^2, \tag{21}$$

$$\chi^2 = \sum_{i=0}^{255} \frac{(n_i - n/256)^2}{n/256}, \tag{22}$$

where $X = \{x_1, x_2, \ldots, x_{256}\}$ represents the vector of tonal values in the histogram. x_i and x_j indicate the pixel counts for gray levels i and j, respectively. Let n_i denote the frequency of tonal value i and n the total pixel count. Thus, the expected frequency for each tonal value is $n/256$. A significance level of $\alpha = 0.05$ is typically used. If chi-square score $\chi^2_{0.05}(255) = 293.248$, this suggests that the pixel distribution is exceptionally uniform [44]. To achieve greater uniformity, the variance should be made as small as possible. The variance and χ^2 test results for the original and encrypted images under the histogram analysis in Figure 14 are presented in Table 2.

Table 2. Analysis of variance and χ^2 test results for the images.

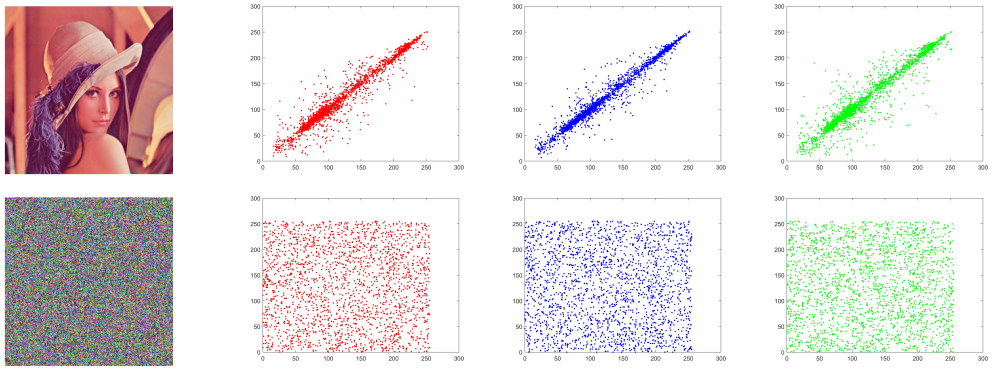
Images	P/E	Size	Variance	Chi-Square
Lena	Plain	256×256	1.9329×10^5	6.4430×10^4
	Encrypted	256×256	666.9725	221.4557
Aircraft	Plain	512×512	2.7718×10^7	2.3098×10^6
	Encrypted	512×512	2714.8	225.3457
Sailboat	Plain	512×512	2.6723×10^6	2.2269×10^5
	Encrypted	512×512	2955.1	245.2995
Satellite	Plain	1024×1024	6.8016×10^7	1.4170×10^6
	Encrypted	1024×1024	11,434	237.2786
Butterfly	Plain	768×512	1.4687×10^7	8.1595×10^5
	Encrypted	768×512	4145.3	229.3971

5.4. Correlation Analysis

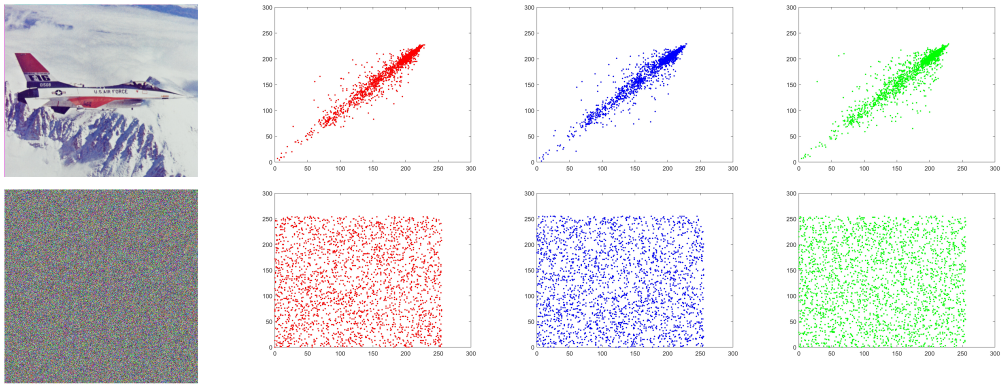
In plaintext images, pixels usually exhibit strong correlations among themselves. Therefore, efficient image encryption algorithms should greatly reduce inter-pixel correlation through effective substitution operations. To quantify the correlation between pixels, the correlation coefficient r_{xy} between pixels can be computed using Equation (23).

$$r_{xy} = \frac{E[x - E(x)][y - E(y)]}{\sqrt{var(x)\sqrt{var(y)}}}, \tag{23}$$

where $E(x) = \frac{1}{N}\Sigma_{i=1}^{N} x_i$, $var(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x)]^2$, x_i, and y_i denote the hue value of the i pairs of neighboring pixels and N denotes the number of pixel samples. In this study, 3000 pixel samples were analyzed by extracting them from encrypted images. The original and encrypted images of Lena, airplane, sailboat, satellite, and butterfly were analyzed along with their correlation coefficients in horizontal, vertical, and diagonal directions for R, G, and B channels. Figure 15 shows the correlations in the three directions of the experimental pictures, where the horizontal, vertical, and diagonal correspond to red, blue, and green respectively and Table 3 presents the corresponding correlation numbers. The results show that while the original images showed significant pixel correlation, the encrypted images showed negligible correlation between neighboring pixels. The reduction of the correlation coefficient tended to zero, which proves that the proposed encryption method effectively improves the randomness and security of encryption and further confirms the efficiency of the algorithm.

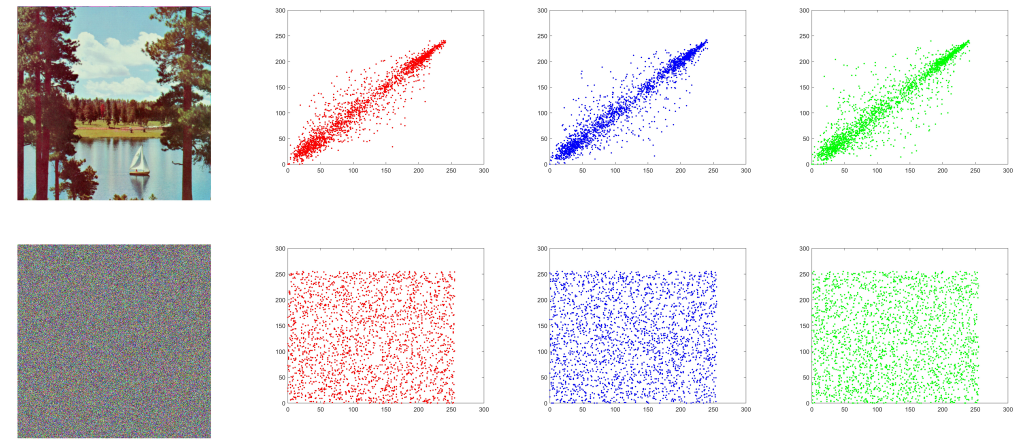


(**a**) Lena

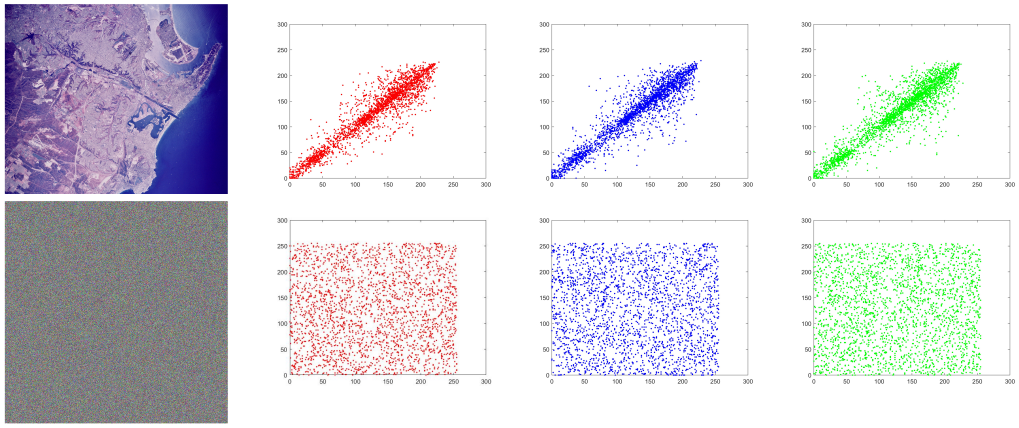


(**b**) Aircraft

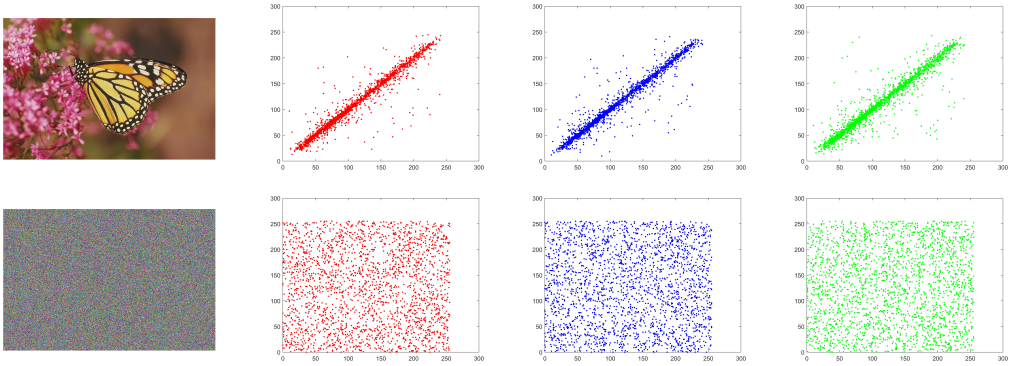
Figure 15. *Cont.*



(**c**) Sailboat



(**d**) Satellite



(**e**) Butterfly

Figure 15. The first row of each group of images is for plain images and the second row is for encrypted images.

Table 3. The correlation coefficient of adjacent pixels in the image.

Images	Channels	Plaintext Image			Ciphertext Image		
		H	**V**	**D**	**H**	**V**	**D**
Lena	R	0.9403	0.9742	0.9255	0.0127	−0.0252	0.0022
	G	0.9500	0.9669	0.9279	−0.0238	0.0003	0.0066
	B	0.9431	0.9634	0.9203	−0.0080	−0.0130	−0.0020
Aircraft	R	0.9686	0.9733	0.9447	−0.0107	0.0033	0.0008
	G	0.9646	0.9722	0.9458	0.0392	−0.0076	0.0086
	B	0.9591	0.9570	0.9274	−0.0369	0.0096	−0.0092

Table 3. *Cont.*

Images	Channels	Plaintext Image			Ciphertext Image		
		H	V	D	H	V	D
Sailboat	R	0.9632	0.9594	0.9483	−0.0113	0.0069	0.0001
	G	0.9716	0.9689	0.9586	0.0295	−0.0111	−0.0093
	B	0.9748	0.9719	0.9560	−0.0006	−0.0015	0.0044
Satellite	R	0.9560	0.9192	0.9027	0.0004	−0.0102	0.0248
	G	0.9208	0.9242	0.9038	−0.0001	−0.0005	0.0256
	B	0.8902	0.9128	0.8902	−0.0228	0.0034	0.0017
Butterfly	R	0.9721	0.9612	0.9535	0.0207	−0.0263	0.0023
	G	0.9411	0.9478	0.9091	0.0061	0.0193	−0.0093
	B	0.9590	0.9470	0.9455	−0.0062	0.0030	0.0311

5.5. Information Entropy Analysis

Information entropy is a fundamental measure of uncertainty and randomness in image data. Higher entropy values indicate greater unpredictability in an image's content. An entropy value near eight typically signifies that the encrypted image exhibits enhanced security and randomness [45]. As a crucial tool for evaluating ciphertext properties, information entropy is widely applied to assess the performance of encryption algorithms and the resilience of encryption schemes. By using formula (24), entropy can be quantified, providing a clear standard for evaluating the security of an encryption system.

$$H(x) = \sum_{i=0}^{2^n-1} p(x_i) log_2 \frac{1}{p(x_i)}. \tag{24}$$

Let x represent the information source, with the probability of x_i denoted as $p(x_i)$. The total number of possible states is 2^n. For color images with 256 grayscale levels, Table 4 lists the entropy values of R, G, and B channels of plaintext and ciphertext images according to the encryption method proposed in this paper and compares them with the entropy values obtained by other encryption techniques. The results show that the entropy values of the R, G, and B channels of the ciphertext image are almost equal to the ideal value eight.

Table 4. Information entropy analysis.

Images	Size	Plaintext Image			Ciphertext Image		
		R	G	B	R	G	B
Lena	256 × 256 × 3	7.2353	7.5683	6.9176	7.9974	7.9976	7.9972
Aircraft	512 × 512 × 3	6.7178	6.799	6.2138	7.9994	7.9993	7.9994
Sailboat	512 × 512 × 3	7.3124	7.6461	7.2137	7.9993	7.9994	7.9993
Satellite	1024 × 1024 × 3	7.7229	7.5289	6.8318	7.9998	7.9998	7.9998
Butterfly	768 × 512 × 3	7.4042	7.0843	6.9801	7.9996	7.9995	7.9996
Ref. [34]	512 × 512 × 3	–	–	–	7.9971	7.9975	7.9974
Ref. [36]	512 × 512 × 3	–	–	–	7.9912	7.9913	7.9914
Ref. [38]	512 × 512 × 3	–	–	–	7.9974	7.9974	7.9974

5.6. Differential Attack Analysis

In the field of image encryption, differential analysis is commonly employed to assess the robustness of encryption algorithms against differential attacks. This approach involves introducing slight perturbations to the input image and then observing how these small changes propagate within the ciphertext, thereby evaluating whether the encryption algorithm possesses strong security. Ideally, a secure image encryption system should exhibit high plaintext sensitivity, meaning that even a single pixel change in the input image should lead to a significant alteration in the overall structure of the ciphertext.

To quantify the performance of encryption algorithms under such conditions, two key metrics are commonly introduced: the Number of Pixels Change Rate (NPCR) and

Unified Average Changing Intensity (UACI). NPCR measures the proportion of pixel position changes between two ciphertext images before and after encryption, reflecting the extent to which local disturbances are diffused in the ciphertext. UACI, on the other hand, captures the average intensity differences between two ciphertext images, indicating the response of the encryption output to perturbations at the numerical level. Together, these two metrics allow for a comprehensive assessment of an algorithm's resistance to differential attacks from both the spatial distribution and intensity change perspectives. Therefore, NPCR and UACI have become essential standards for evaluating the security of image encryption algorithms and are widely used in the verification of modern encryption schemes. The calculation formulas for NPCR and UACI are defined in Equations (25)–(27).

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%, \tag{25}$$

$$D(i,j) = \begin{cases} 1, T_1(i,j) \neq T_2(i,j) \\ 0, T_1(i,j) = T_2(i,j) \end{cases}, \tag{26}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|T_1(i,j) - T_2(i,j)|}{255}\right] \times 100\%, \tag{27}$$

where $T_1(i,j)$ and $T_2(i,j)$ respectively represent the pixel values at the same coordinate positions in the encrypted images obtained by the encryption algorithm from the original images that have slight differences. M and N indicate the number of rows and columns of the ciphertext image, respectively. The NPCR and UACI results for images of various sizes used in the experiments are presented in Table 5. Notably, the experimental results are in close proximity to the ideal NPCR value of 99.6094% and the ideal UACI value of 33.4635%. The comparative analysis shows that the performance of our algorithm in terms of NPCR and UACI is basically closer to the theoretical ideal values. This indicates that our algorithm exhibits stronger resistance to differential attacks.

Table 5. Results of NPCR and UACI performance.

Images	NPCR(%)			UACI(%)		
	R	**G**	**B**	**R**	**G**	**B**
Lena	99.6156	99.5965	99.5978	33.4829	33.4759	33.4573
Aircraft	99.6046	99.6107	99.6116	33.3912	33.4616	33.4250
Sailboat	99.5964	99.6064	99.6075	33.4997	33.4976	33.4578
Satellite	99.6076	99.5987	99.5989	33.4419	33.5068	33.5038
Butterfly	99.5921	99.6242	99.6056	33.4480	33.4497	33.4656
Ref. [46]	99.5461	99.7066	99.6070	35.9229	36.6366	36.2376
Ref. [47]	99.5925	99.6294	99.6140	33.4226	33.4344	33.4698
Ref. [48]	99.6048	99.6010	99.5987	33.4481	33.4886	33.5094

6. Conclusions and Outlook

This paper introduced a novel hyperchaotic system developed from a two-dimensional cross-coupled chaotic system. By combining Chebyshev mapping, Fuch mapping, and nonlinear functions $sin(x)$ and $cos(x)$, a two-dimensional Chebyshev–Fuch coupled map (2D-CFCM) was established. The proposed chaotic system exhibits significant chaotic behavior, highlighted by enhanced phase diagrams, bifurcation diagrams, Lyapunov exponents, and complexity. The resulting chaotic sequences demonstrate a greater degree of randomness, and the chaotic parameter space is notably expanded. In order to check the performance of the 2D chaotic system, an image encryption scheme based on 2D-CFCM was introduced. The algorithm derives a key from the original image using the SHA-512

function and then applies both obfuscation and diffusion via a chaotic matrix coupled with the I-Zigzag transformation, achieving multi-directional randomness. Simulation outcomes show that the encryption method performs exceptionally well, provides a large key space, and exhibits significant sensitivity to key alterations. However, the encryption method's efficiency, especially for larger images, requires further optimization. Future research could explore the integration of this encryption method with emerging technologies like quantum computing and machine learning to enable more advanced encryption solutions. Additionally, testing the algorithm's applicability in real-world scenarios, such as cloud storage and digital media transmission, would demonstrate its practical potential.

Author Contributions: Conceptualization, C.C.; validation, C.C. and T.L.; formal analysis, B.Y.; investigation, C.C. and B.Y.; writing original draft, C.C.; writing review and editing, C.C. and T.L.; supervision, T.L.; funding acquisition, T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Scientiffc Research and Innovation Team Program of SUSE (no. SUSE652B002), the Scientic Research Project of Sichuan University of Science and Engineering (no. 2025RCZ023), and the Graduate Student Innovation Fundings (no. Y2024334).

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: Many thanks to experts and editors for their valuable suggestions.

Conflicts of Interest: The authors declare that they have no conflicts of interest.

References

1. Khan, M.; Jamal, S.S.; Hazzazi, M.M. An efficient image encryption scheme based on double affine substitution box and chaotic system. *Integration* **2021**, *81*, 108–122. [CrossRef]
2. Wang, X.; Chen, S.; Zhang, Y. A chaotic image encryption algorithm based on random dynamic mixing. *Opt. Laser Technol.* **2021**, *138*, 106837. [CrossRef]
3. Zhou, S.; Wang, X.; Zhang, Y. Novel image encryption scheme based on chaotic signals with finite-precision error. *Inf. Sci.* **2023**, *621*, 782–798. [CrossRef]
4. Golalipour, K. A novel permutation-diffusion technique for image encryption based on the imperialist competitive algorithm. *Multimed. Tools Appl.* **2023**, *82*, 725–746. [CrossRef]
5. Coppersmith, D. The Data Encryption Standard (DES) and its strength against attacks. *IBM J. Res. Dev.* **1994**, *38*, 243–250. [CrossRef]
6. Toughi, S.; Fathi, M.H.; Sekhavat, Y.A. An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal Process.* **2017**, *141*, 217–227. [CrossRef]
7. Gong, L.; Qiu, K.; Deng, C. An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Opt. Lasers Eng.* **2019**, *121*, 169–180. [CrossRef]
8. Wu, X.; Kurths, J.; Kan, H. A robust and lossless DNA encryption scheme for color images. *Multimed. Tools Appl.* **2018**, *77*, 12349–12376. [CrossRef]
9. Mahmud, M.; Lee, M.; Choi, J.Y. Evolutionary-based image encryption using RNA codons truth table. *Opt. Laser Technol.* **2020**, *121*, 105818. [CrossRef]
10. Cun, Q.; Tong, X.; Wang, Z. A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing. *Vis. Comput.* **2023**, *39*, 6589–6608. [CrossRef]
11. Feng, W.; Zhang, K.; Zhang, J. Integrating fractional-order Hopfield neural network with differentiated encryption: Achieving high-performance privacy protection for medical images. *Fractal Fract.* **2025**, *9*, 426. [CrossRef]
12. Yu, F.; Zhang, S.; Su, D. Dynamic analysis and implementation of FPGA for a new 4D fractional-order memristive Hopfield neural network. *Fractal Fract.* **2025**, *9*, 115. [CrossRef]
13. Darani, A.Y.; Yengejeh, Y.K.; Pakmanesh, H. Image encryption algorithm based on a new 3D chaotic system using cellular automata. *Chaos Solit. Fractals* **2024**, *179*, 114396. [CrossRef]
14. Zhang, D.; Liao, X.; Yang, B. A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform. *Multimed. Tools Appl.* **2018**, *77*, 2191–2208. [CrossRef]

15. Gan, Z.; Xiong, B.; Pang, Z. A visually secure image encryption scheme using newly designed 1D sinusoidal chaotic map and P-tensor product compressive sensing. *Nonlinear Dyn.* **2024**, *112*, 2979–3001. [CrossRef]
16. Wang, C.; Song, L. An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios. *Inf. Sci.* **2023**, *642*, 119166. [CrossRef]
17. Zhang, Z.; Tang, J.; Ni, H. Image adaptive encryption algorithm using a novel 2D chaotic system. *Nonlinear Dyn.* **2023**, *111*, 10629–10652. [CrossRef]
18. Luo, Y.; Lin, J.; Liu, J. A robust image encryption algorithm based on Chua's circuit and compressive sensing. *Signal Process.* **2019**, *161*, 227–247. [CrossRef]
19. Feng, W.; Zhang, J.; Chen, Y. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst. Appl.* **2024**, *246*, 123190. [CrossRef]
20. Luo, J.; Xu, X.; Ding, Y. Application of a memristor-based oscillator to weak signal detection. *Eur. Phys. J. Plus* **2018**, *133*, 239. [CrossRef]
21. Yang, F.; Mou, J.; Ma, C. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Opt. Lasers Eng.* **2020**, *129*, 106031. [CrossRef]
22. Lu, T.; Anwar, W.; Tang, X. Distributional chaoticity of C_0-semigroup on a Frechet space. *Symmetry* **2019**, *11*, 345. [CrossRef]
23. Mohamadi, H.E.; Lahlou, L.; Kara, N. A versatile chaotic cryptosystem with a novel substitution-permutation scheme for internet-of-drones photography. *Nonlinear Dyn.* **2024**, *112*, 4977–5012. [CrossRef]
24. Akraam, M.; Rashid, T.; Zafar, S. A novel and secure image encryption scheme based on two-dimensional logistic and Arnold cat map. *Clust. Comput.* **2024**, *27*, 2029–2048. [CrossRef]
25. Hua, Z.; Zhou, Y.; Pun, C.M. 2D sine logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
26. Zhu, H.; Zhao, Y.; Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [CrossRef]
27. Feng, W.; Qin, Z.; Zhang, J. Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding. *IEEE Access* **2021**, *9*, 145459–145470. [CrossRef]
28. Feng, W.; He, Y.; Li, H. Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. *IEEE Access* **2019**, *7*, 12584–12597. [CrossRef]
29. Wang, X.; Guan, N. 2D sine-logistic-tent-coupling map for image encryption. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 13399–13419. [CrossRef]
30. Yang, Z.; Cao, Y.; Ji, Y. Securing color image by using bit-level modified integer nonlinear coupled chaos model in Fresnel diffraction domains. *Opt. Lasers Eng.* **2022**, *152*, 106969. [CrossRef]
31. Hua, Z.; Zhu, Z.; Yi, S. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **2021**, *546*, 1063–1083. [CrossRef]
32. Huang, X.; Dong, Y.; Zhu, H. Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image. *Alex. Eng. J.* **2022**, *61*, 7637–7647. [CrossRef]
33. Hua, Z.; Yi, S.; Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **2018**, *144*, 134–144. [CrossRef]
34. Herbadji, D.; Derouiche, N.; Belmeguenai, A . A new colour image encryption approach using a combination of two 1D chaotic map. *Int. J. Electron. Secur. Digit. Forensics* **2020**, *12*, 337–356. [CrossRef]
35. Liu, Z.; Liu, J.Y.; Zhang, L.Y. Performance of the 2D coupled map lattice model and its application in image encryption. *Complexity* **2022**, *2022*, 5193618. [CrossRef]
36. Zhang, Z.; Tang, J.; Zhang, F. Color image encryption using 2D sine-cosine coupling map. *IEEE Access* **2022**, *10*, 67669–67685. [CrossRef]
37. Xuejing, K.; Zihui, G. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Process.* **2020**, *80*, 115670. [CrossRef]
38. Rezaei, B.; Ghanbari, H.; Enayatifar, R. An image encryption approach using tuned Henon chaotic map and evolutionary algorithm. *Nonlinear Dyn.* **2023**, *111*, 9629–9647. [CrossRef]
39. Li, L.; Luo, Y.; Qiu, S. Image encryption using chaotic map and cellular automata. *Multimed. Tools Appl.* **2022**, *81*, 40755–40773. [CrossRef]
40. Demirtaş, M. A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. *Optik* **2022**, *265*, 169430. [CrossRef]
41. Zhang, Y.Q.; He, Y.; Li, P. A new color image encryption scheme based on 2DNLCML system and genetic operations. *Opt. Lasers Eng.* **2020**, *128*, 106040. [CrossRef]
42. Erkan, U.; Toktas, A.; Enginoğlu, S. An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimed. Tools Appl.* **2022**, *81*, 7365–7391. [CrossRef]
43. Li, L. A novel chaotic map application in image encryption algorithm. *Expert Syst. Appl.* **2024**, *252* , 124316. [CrossRef]

44. Zhang, X.; Zhao, Z.; Wang, J. Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Process.* **2014**, *29*, 902–913. [CrossRef]
45. Dong, Y.; Zhao, G.; Ma, Y. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. *Inf. Sci.* **2022**, *593*, 121–154. [CrossRef]
46. Ahmad, I.; Shin, S. A novel hybrid image encryption compression scheme by combining chaos theory and number theory. *Signal Process.* **2021**, *98*, 116418. [CrossRef]
47. Yildirim, M. Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. *Chaos Solit. Fractals* **2022**, *155*, 111631. [CrossRef]
48. Liu, X.; Tong, X.; Wang, Z. Uniform non-degeneracy discrete chaotic system and its application in image encryption. *Nonlinear Dyn.* **2022**, *108*, 653–682. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.