Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 34(7): 4577–4610.
DOI: 10.3934/era.2026202
Received: 17 March 2026
Revised: 05 May 2026
Accepted: 07 May 2026
Published: 28 May 2026

Research article

Color image encryption based on a square-term enhanced 4D chaotic system

Ping Gao[1,2], Tianxiu Lu[1,*] and Jiahua Dong[1]

[1] College of Mathematics and Statistics, Sichuan University of Science and Engineering, Zigong 643000, China

[2] Brewing Science and Technology Key Laboratory of Sichuan Province, Zigong 643000, China

* **Correspondence:** Email: lubeeltx@163.com.

Abstract: Chaotic systems confer distinct advantages for image encryption due to their remarkable responsiveness to initial parameters, inherent unpredictability, and characteristics of pseudo-randomness. However, many existing chaos-based image encryption schemes still suffer from limitations such as narrow chaotic parameter intervals, insufficient trajectory uniformity, and inadequate diffusion depth, which may weaken the randomness of generated sequences and reduce encryption robustness. To address these issues, a square-term enhanced four-dimensional chaotic system was constructed, and a color image encryption scheme integrating hierarchical scrambling and symmetric bidirectional diffusion was developed. Dynamic analyses, including phase portraits, bifurcation diagrams, maximum Lyapunov exponents, time-series distribution, and complexity evaluation, indicate that the proposed system exhibits a broad chaotic interval, strong initial-value sensitivity, and improved trajectory uniformity. It can well-adapt to the image encryption requirements of different categories. Simulation experiments conducted using a variety of test images indicate that the encryption scheme offers an adequately large key space, with pixel correlation measured at less than 0.03, information entropy exceeding 7.9974, and robust resistance to differential attacks. The computed mean values for number of pixels change rate (NPCR) and unified average changing intensity (UACI) were found to be 99.6073% and 33.4626%, respectively, demonstrating a strong alignment with the optimal benchmarks. The algorithm achieves competitive performance in terms of efficiency and security, can effectively resist common attacks, and is suitable for the secure transmission and storage of sensitive images.

Keywords: four-dimensional chaotic system; dynamic analysis; two-level scrambling; multidirectional random diffusion; image encryption

1. Introduction

Amidst the swift advancement of digital communication technologies, digital imagery has emerged as the primary means for conveying information [1]. However, unapproved access to image content can result in violations of individual privacy and pose risks to both commercial confidentiality and national security [2, 3]. Consequently, the field of image encryption has emerged as an essential focus of research in today's information security landscape. In large-scale data image encryption scenarios, traditional standards like the advanced encryption standard (AES) and the data encryption standard (DES) exhibit low efficiency, leading to their gradual replacement by emerging encryption methods [4]. Emerging image encryption methods include DNA coding [5–8], cellular automata [9], RNA coding [10], neural networks [11–13], S-box techniques [14, 15], compressed sensing [16–18], chaotic systems [19, 20], the fractional Fourier transform [21], and compliance matrix methods [22]. Similar to the idea of dynamically balancing access efficiency and update overhead in data replication in distributed systems, image encryption also requires a balance between security and computational efficiency [23].

Chaos-based systems possess a substantial capability to improve encryption techniques due to their sensitivity to initial conditions, unpredictable dynamics, and intrinsic randomness [24, 25]. As such, they hold promising application potential across multiple domains, including image cryptography, secure communications, and interdisciplinary fields like economics and physics [26–30]. The majority of initial investigations were grounded in one-dimensional and two-dimensional chaotic systems. While they offer benefits such as a straightforward structure and ease of implementation, they also present limitations, including a restricted key space, and a lack of dynamic diversity. When confronted with brute force and statistical attacks, the level of security is inadequate. Conversely, high-dimensional chaotic systems augment the quantity of state variables while enhancing the nonlinear coupling interactions among them. They show more complex dynamic behavior, richer parameter space, and stronger anti-cracking ability, thus offering some viable approaches to boost encryption scheme security.

Recently, a wide array of chaotic systems in high-dimensional space have been thoroughly explored and utilized for image encryption purposes. Adaptive unequal protection and fuzzy logic control have been widely used in wireless multimedia transmission to achieve dynamic service quality assurance, which provides important inspiration for the adaptive design of image encryption [31]. Liang et al. [32] proposed a newly developed image encryption method that utilizes a unique four-wing hyperchaotic system combined with dynamic DNA coding, effectively addressing the limitations of previous techniques that depend on static DNA rules and keys independent of plaintext. Chen et al. [33] introduced a symmetric encryption approach for images that leverages a three-dimensional chaotic cat mapping, effectively tackling the challenges faced by traditional encryption algorithms in managing extensive volumes of highly redundant image data. Mehdi [34] developed an image encryption strategy utilizing an innovative four-dimensional hyperchaotic system, enhancing the resilience of the encryption mechanism against a range of possible attacks. Wu et al. [35] put forward an innovative 5D fractional-order complex chaotic system, alongside a dynamic Arnold scrambling technique. By tying the scrambling parameters to the pixel information of each image channel, this approach enhances the algorithm's sensitivity to plaintext content. Panwar et al. [36] proposed a six-dimensional hyperchaotic system with four positive Lyapunov exponents

(LEs), delivering complex dynamics and secure chaotic sequences for encryption. Tong et al. [37] developed an improved five-dimensional chaotic system, which achieved efficient encryption and improved security through 10 rounds of iteration. Gong et al. [38] proposed a four-dimensional dissipative chaotic system based on a continuous Hopfield neural network, which has excellent dynamic characteristics. Through the image compression algorithm of chaotic encryption, the pixel position is efficiently scrambled to enhance the diffusion effect. In addition to conventional full-image encryption schemes, recent studies have also explored several extended application scenarios of image encryption. For example, Song et al. [39] proposed a batch image encryption method based on cross-image permutation and diffusion, which supports the efficient protection of multiple images with different sizes in a unified framework. Liu et al. [40] introduced a semantically enhanced selective image encryption scheme with parallel computing, where sensitive regions are detected and encrypted in a targeted manner to improve efficiency and practicality. Meanwhile, Yu et al. [41] developed discrete cascaded memristive neuron maps and applied the generated hyperchaotic sequences to color image encryption. These studies indicate that recent image encryption research has gradually expanded from traditional whole-image protection to more flexible and task-oriented encryption frameworks. Nevertheless, for chaos-based full-image encryption schemes, it remains important to design an encryption framework that simultaneously maintains strong security, clear algorithmic structure, and high sensitivity to plaintext changes.

Although many existing high-dimensional chaotic systems have been applied to image encryption, some of them still exhibit limited chaotic parameter ranges, uneven trajectory distributions, or insufficient dynamic complexity. These drawbacks may reduce the randomness and uniformity of the generated chaotic sequence, thereby weakening the effectiveness of scrambling and diffusion operations. Therefore, constructing new chaotic systems with richer nonlinear coupling and improved dynamic behavior is still of great significance for secure image encryption applications.

This study proposes an innovative four-dimensional chaotic system characterized by the introduction of a squared nonlinear term, which can enhance the coupling between state variables, enrich the dynamic characteristics of the system, and potentially improve the complexity and distribution characteristics of the generated chaotic sequence. By examining the phase diagram, complexity measure, and bifurcation diagram, it is evident that the proposed system exhibits more extensive chaotic behavior and higher complexity. Adopting two-stage scrambling and multi-directional random diffusion to enhances the randomness of the encryption process and minimizes pixel correlation to the greatest extent possible. The experimental results show that the developed algorithm has robust security features, which can be demonstrated by evaluating key space, histogram characteristics, pixel correlation, information entropy, and its robustness to differential attacks.

In conclusion, the main contributions of this study are presented below.

(i) A novel four-dimensional chaotic system has been developed, which is capable of producing chaotic sequences characterized by a high degree of randomness and a uniform distribution.

(ii) The four-dimensional system's performance is assessed using bifurcation diagrams, LEs, time series distribution, and so on. Results demonstrate a wide chaotic interval, excellent randomness, and superior chaotic performance.

(iii) A color image encryption framework driven by the proposed chaotic system is developed. Instead of relying on a single permutation or a conventional one-way diffusion process, the scheme

combines hierarchical two-stage scrambling with symmetric bidirectional diffusion to enhance pixel-position randomness, diffusion depth, and overall resistance to statistical and differential attacks.

The organization of this manuscript is outlined as follows. Section 2 presents a full examination of the creation and evaluation of the novel four-dimensional chaotic system. Section 3 elaborates on the scrambling and diffusion mechanisms integrated into the proposed encryption scheme. Section 4 encompasses the simulation experiments and the security evaluations related to the proposed approach. Finally, Section 5 summarizes the core conclusions drawn from this research.

2. A four-dimensional chaotic system

In the exploration of complex dynamical systems, this study integrates established chaos theory and methodologies based on the concept of nonlinear interactions in multidimensional space to establish relationships among variables. In order to overcome the constraints observed in current chaos maps, which include restricted chaotic ranges and uneven distributions of trajectories, we introduce an innovative four-dimensional chaotic system that includes quadratic terms, as delineated in Eq (2.1).

$$\begin{cases} \dot{x} = a(x+z) - yz, \\ \dot{y} = x^2 - by, \\ \dot{z} = c(x-z), \\ \dot{w} = c(y-w), \end{cases} \tag{2.1}$$

where $a = 10$, $b = 5.5$, $c = 17.5$, and (x, y, z, w) denote the state variables. To clarify the dynamical role of the introduced square term, we analyze its influence on the equilibrium structure and local linearization of system (2.1). The equilibrium points are determined by

$$\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0.$$

By solving these algebraic equations, the equilibrium points are obtained as

$$\begin{cases} E_0 = (0, 0, 0, 0), \\ E_1 = (\sqrt{2ab}, 2a, \sqrt{2ab}, 2a), \\ E_2 = (-\sqrt{2ab}, 2a, -\sqrt{2ab}, 2a). \end{cases}$$

The introduction of the square term changes the nonlinear feedback structure of the system and consequently modifies the distribution and local stability of the equilibrium points. Compared with the original system, the modified system exhibits a richer equilibrium structure, which implies that trajectories are affected by more complex local attraction-repulsion interactions in phase space. Such changes are beneficial for enhancing stretching and folding behaviors, increasing phase-space complexity, and improving sensitivity to initial conditions. Therefore, the square term does not merely increase the algebraic nonlinearity of the model, but also contributes to more complex dynamical evolution, which is desirable for chaotic sequence generation in image encryption.

The Jacobian matrix and the Lyapunov exponents are used below to further characterize the local and global dynamical behavior of system (2.1). The calculation method for LEs is as follows. Let $\dot{X} =$

$F(X)$, where $X = (x, y, z, w)^T$ and $F(X) = (F_1, F_2, F_3, F_4)^T$. The Jacobian matrix $J(X)$ of system (2.1), which describes the local linearization around the state X, is given by Eq (2.2).

$$J(x,y,z,w) = \begin{pmatrix} \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} & \frac{\partial F_1}{\partial z} & \frac{\partial F_1}{\partial w} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} & \frac{\partial F_2}{\partial z} & \frac{\partial F_2}{\partial w} \\ \frac{\partial F_3}{\partial x} & \frac{\partial F_3}{\partial y} & \frac{\partial F_3}{\partial z} & \frac{\partial F_3}{\partial w} \\ \frac{\partial F_4}{\partial x} & \frac{\partial F_4}{\partial y} & \frac{\partial F_4}{\partial z} & \frac{\partial F_4}{\partial w} \end{pmatrix} = \begin{pmatrix} a & -z & a-y & 0 \\ 2x & -b & 0 & 0 \\ c & 0 & -c & 0 \\ 0 & c & 0 & -c \end{pmatrix}. \tag{2.2}$$

It can be seen from Eq (2.2) that the entry $\partial\dot{y}/\partial x = 2x$ is explicitly state-dependent. This feature distinguishes the proposed system from models with only constant or weakly varying linear gains, and confirms that the square term directly affects the local expansion/contraction mechanism of the flow field.

Suppose that the Jacobian matrix J has eigenvalues $\lambda_1(J)$, $\lambda_2(J)$, $\lambda_3(J)$, and $\lambda_4(J)$. Then, the Lyapunov exponents can be calculated according to Eq (2.3).

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|\lambda_i(J)|. \tag{2.3}$$

Let n be sufficiently large to make the LEs of system (2.1) converge, and the LEs of the system are $LE_1 = 1.39$, $LE_2 = 0$, $LE_3 = -14.51$, $LE_4 = -17.6$, respectively. Among the four LEs of system (2.1), one of them is positive and satisfies the law of $(+, 0, -, -)$, which verifies that system (2.1) is a chaotic system. Combined with the above equilibrium and Jacobian analyses, this result indicates that the introduced square term does not merely add nonlinearity formally, but substantively alters the local instability structure and the global evolution pattern of the system.

In addition, the geometric complexity of the attractor can be further quantified by the Kaplan-Yorke dimension. The Kaplan-Yorke dimension is defined as

$$D_{KY} = j + \frac{\sum_{i=1}^{j} LE_i}{|LE_{j+1}|},$$

where j is the largest integer satisfying $\sum_{i=1}^{j} LE_i \geq 0$ and $\sum_{i=1}^{j+1} LE_i < 0$. For system (2.1), since $LE_1 + LE_2 = 1.39 > 0$ and $LE_1 + LE_2 + LE_3 < 0$, one has $j = 2$. Therefore,

$$D_{KY} = 2 + \frac{LE_1 + LE_2}{|LE_3|} = 2 + \frac{1.39 + 0}{14.51} \approx 2.096.$$

The obtained fractional dimension indicates that the attractor of system (2.1) possesses a non-integer geometric structure and considerable dynamical complexity. For further quantitative evaluation, the Kaplan-Yorke dimension of the proposed system was compared with that of a representative recent 4D chaotic system reported in the literature. Wang et al. [42] reported that the Kaplan-York dimension of the proposed 4D chaotic system is 2.052, while the value of system (2.1) is slightly higher. This same-class comparison suggests that the proposed attractor has competitive geometric complexity. It should be noted that some recent 4D hyperchaotic systems may exhibit larger Kaplan-Yorke dimensions because they belong to a different dynamical regime with multiple positive Lyapunov exponents. Therefore, the comparison here is intended as a quantitative reference within the category of recent 4D chaotic systems.

Although the chaotic characteristics of system (2.1) have been verified, mere chaos is insufficient for its application in scenarios such as image encryption. The effectiveness of chaotic performance has a direct impact on the randomness and uniformity of the sequences produced, which in turn exerts a pivotal influence on the encryption security and resilience against diverse attack methods. Therefore, a rigorous analysis of the core dynamical properties of this system is imperative for its practical application. In the subsequent research, the dissipativity, invariance, phase diagram, bifurcation diagram, maximum LE, time series, and complexity of system (2.1) will be examined. These analyses aim to comprehensively assess whether the system meets the stringent high-performance chaos criteria required for image encryption.

2.1. Dissipativity and invariance

Dissipativity is the basis for chaotic systems to generate complex and stable chaotic behaviors, which guarantees the pseudo-randomness of sequences. Invariance ensures that the chaotic system can still maintain the core chaotic characteristics under interference. It guarantees the stability and repeatability of sequence generation.

It is not difficult to find that

$$\nabla F = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = a - b - 2c < 0. \tag{2.4}$$

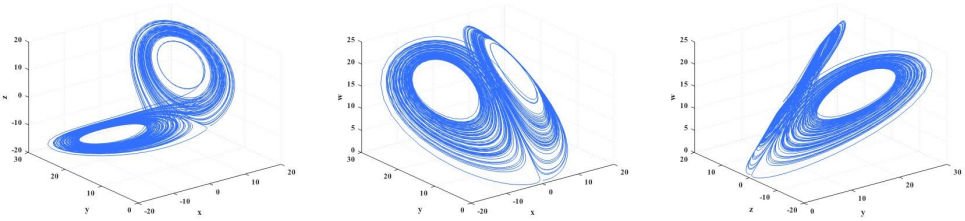
When $a < b + 2c$, the system is dissipative and the volume element $V(t)$ in the phase space satisfies $V(t) = V_0 e^{(a-b-2c)t}$. When $t \to \infty$,

$$\lim_{t\to\infty} V(t) = V_0 \lim_{t\to\infty} e^{(a-b-2c)t} = 0. \tag{2.5}$$

In the end, all trajectories are restricted to a subset of zero volume, and the continuous motion approaches an attractor. Moreover, changing the variables (x, y, z, w) to $(-x, y, -z, w)$, system (2.1) remains invariant.

2.2. Phase diagram

As the fundamental visual analysis tool for representing the behavior of chaotic systems, the distinctive value of phase diagrams lies in their ability to intuitively illustrate the system's motion dynamics. The trajectory representation of chaotic dynamics exhibits distinctive open characteristics, which is prominently illustrated in the phase plane diagram. For systems with significant chaotic characteristics, there are often attractors with wide coverage in the phase diagram. The trajectory distribution of these attractors is intertwined, which profoundly reveals the complex and orderly dynamic structure inside the system. The following Figure 1 is a three-dimensional axial phase diagram of system (2.1).

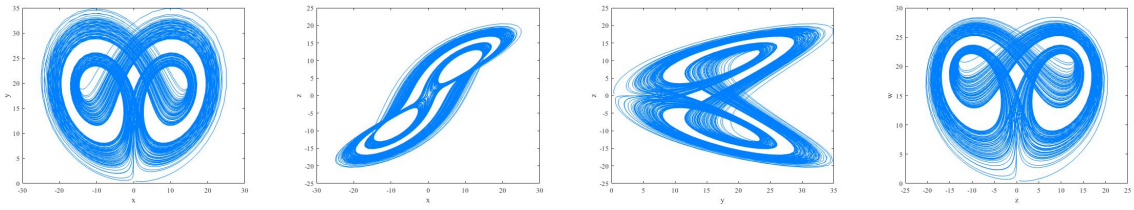


(a) (b) (c)

Figure 1. Three-dimensional axial phase diagrams of system (2.1): (a) *xyz* phase diagram, (b) *xyw* phase diagram, and (c) *yz*w phase diagram.

The three-dimensional phase diagrams discussed above all exhibit characteristic complex trajectory patterns, which directly confirm the chaotic nature of the proposed system. In a bounded space, the trajectories exhibit persistent entanglement and folding without any observable repeating patterns or divergent dispersion. This phenomenon indicates that the system demonstrates a high degree of sensitivity to variations in initial conditions.

The following Figure 2 is a two-dimensional axial phase diagram of system (2.1). The two-dimensional phase diagram further reveals the chaotic nature of the system from the combined dimension of different variables. The trajectory distribution of each phase diagram shows the characteristics of high nonlinearity and strong randomness. The system has been validated to exhibit outstanding chaotic behavior.



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

Figure 2. Two-dimensional axial phase diagrams of system (2.1): (a) *xy* phase diagram, (b) *xz* phase diagram, (c) *yz* phase diagram, and (d) *zw* phase diagram.

2.3. Bifurcation diagram

The bifurcation diagram functions as a crucial tool for analyzing chaotic systems, providing a clear visualization of how the dynamic behavior of a system changes in response to variations in parameters. It effectively delineates the chaotic parameter range to the system and offers a foundation for the encryption algorithm to select parameters characterized by high randomness and sensitivity. Simultaneously, assessing the intricacies of the bifurcation diagram allows for a rapid evaluation of the system's dynamic richness, facilitating the identification of chaotic systems with robust anti-attack capabilities. To investigate the dynamic behavior of system (2.1), a numerical simulation was conducted to generate and analyze its bifurcation diagram, which is presented in Figure 3.

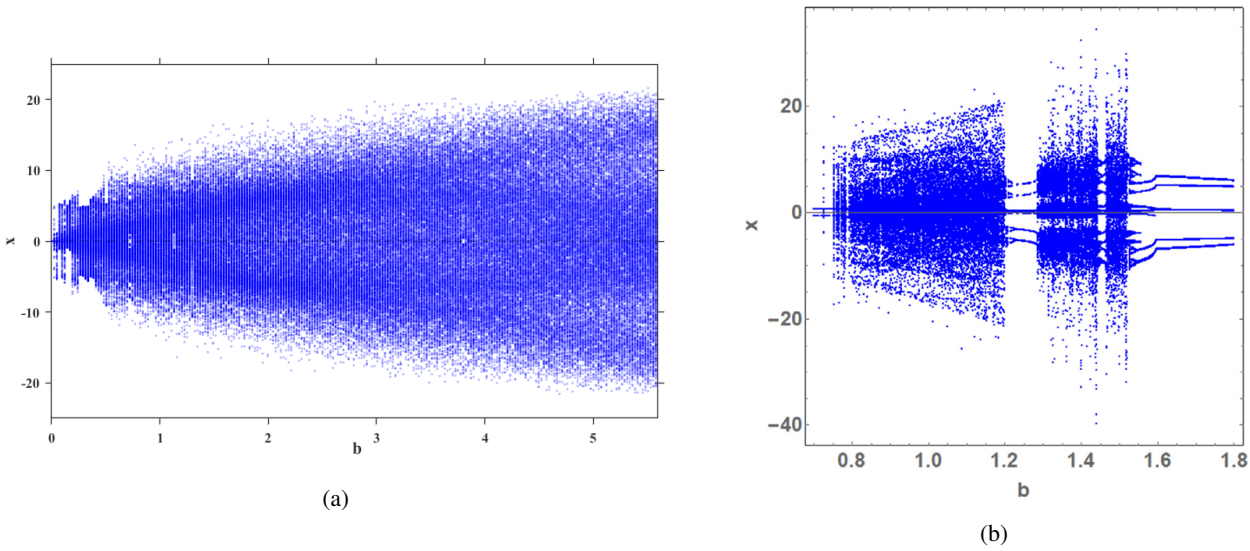


Figure 3. Bifurcation diagrams for comparison: (a) the proposed system and (b) the system in [43].

Observing the bifurcation diagram, the chaotic region is wide and continuous, covering a broad range of state values. This indicates that the system remains in a chaotic state over a relatively wide parameter interval, and the chaotic persistence is strong. Moreover, only a few narrow periodic windows can be observed, suggesting that the system possesses rich and disordered nonlinear dynamics. The bifurcation diagram reveals that the proposed system has a wide and continuous chaotic interval with few periodic windows. In contrast, the 4D system from Elsadany et al. [43] displays more periodic windows and chaotic discontinuities. Thus, our system shows better chaos robustness under parameter variations.

2.4. Maximum Lyapunov exponent

The exponential divergence speed of the system trajectory is quantified, which determines the randomness and unpredictability of the chaotic sequence. The maximum Lyapunov exponent (MLE) is a fundamental quantitative metric employed to assess the behavior of a system, with a positive value serving as a definitive indicator of its chaotic characteristics. Higher MLE values correspond to greater complexity in encrypted key streams. Figure 4 presents the system's maximum Lyapunov exponent, and it can be found that the system exhibits excellent chaotic performance. Figure 4 demonstrates that the MLE remains consistently positive over an extended time interval, with notable peaks in certain regions indicating elevated index values. It means that the system state shows a trend of rapid separation over time, and has a strong sensitivity to initial conditions.

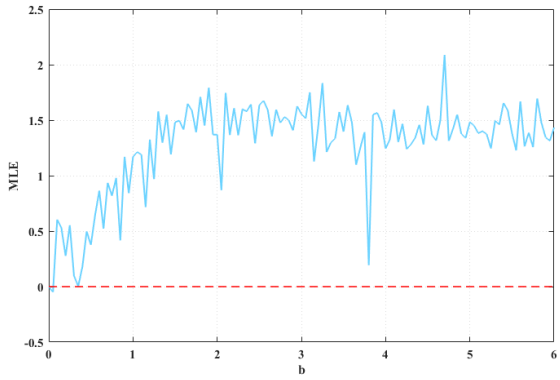


Figure 4. Maximum Lyapunov exponent.

The maximum Lyapunov exponent remains positive over most of the corresponding parameter range, which further confirms the existence of sustained chaotic dynamics.

2.5. Time series

The distribution of a chaotic time series is an intuitive basis for evaluating chaotic performance. Its irregular, non-periodic patterns embody the system's pseudo-random properties. It can reveal the value coverage and uniformity of chaotic sequences. The more dispersed the distribution is, the more local aggregation of sequences can be avoided, and the diversity of key streams can be guaranteed.

Analysis of Figure 5 reveals strong chaotic performance in system (2.1). The four variable curves show continuous and irregular large-scale oscillations on the time axis. Furthermore, the extensive amplitude range combined with the absence of periodic repetition illustrates the system's pronounced sensitivity to initial conditions. The curves are interspersed and entangled with each other, reflecting the strong nonlinear coupling between variables, which further strengthens the complexity of chaotic motion.

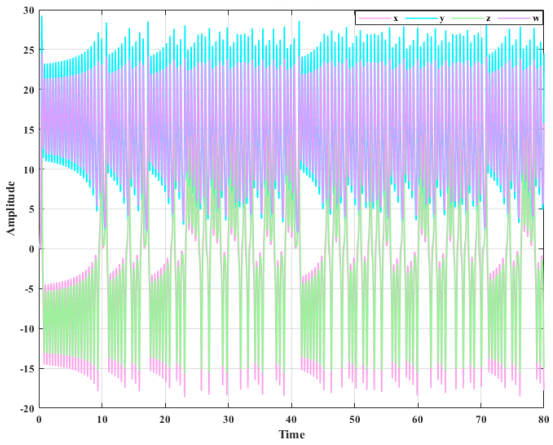
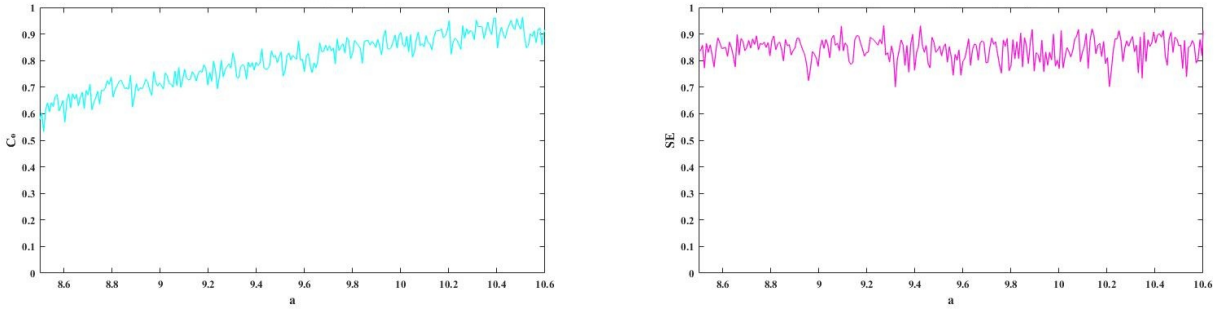


Figure 5. Time series distribution diagram.

2.6. Complexity analysis

Complexity is the core dimension to measure the performance of chaos, which directly determines the behavior richness and unpredictability of chaotic systems. The higher the complexity, the more difficult the system is to be modeled or cracked. High complexity systems can generate more irregular sequences, effectively improve the randomness of the key stream, and enhance the anti-statistical attack ability of the algorithm.

From the two complexity curves in Figure 6, the structural complexity and spectral entropy complexity maintain a high level within a certain parameter range. This indicates the system has rich dynamic behavior, complex structure, and high disorder. Although there is a brief decline, it can rebound quickly, reflecting the robustness of chaotic characteristics. The high and stable complexity distribution reflects the strong unpredictability and diversity of system states over time, which is a quantitative confirmation of the complex dynamic behavior of chaotic systems.



(a) (b)

Figure 6. Complexity analysis of system (2.1): (a) C_0 structural complexity, and (b) spectral entropy complexity.

The complexity analysis indicates that the proposed system produces sequences with high irregularity and strong pseudo-random characteristics, which are desirable for image encryption.

3. Image encryption algorithm

This section encompasses a thorough examination of the foundational principles and key design elements of the image encryption scheme. The aforementioned system (2.1) exhibits several notable advantages, including a broad chaotic range, significant unpredictability, and intricate chaotic dynamics. This lays a robust groundwork for the advancement of high-security encryption methodologies. Leveraging chaotic systems, an innovative image encryption approach has been introduced. The overall process is illustrated in Figure 7, which encompasses three core stages. (1) The external secret key is used to initialize the chaotic system and generate the chaotic sequences required for encryption. (2) The plaintext image is processed by multi-level scrambling operations to destroy pixel position correlation. (3) Forward and reverse diffusion are performed to modify pixel values and enhance resistance to statistical and differential attacks.

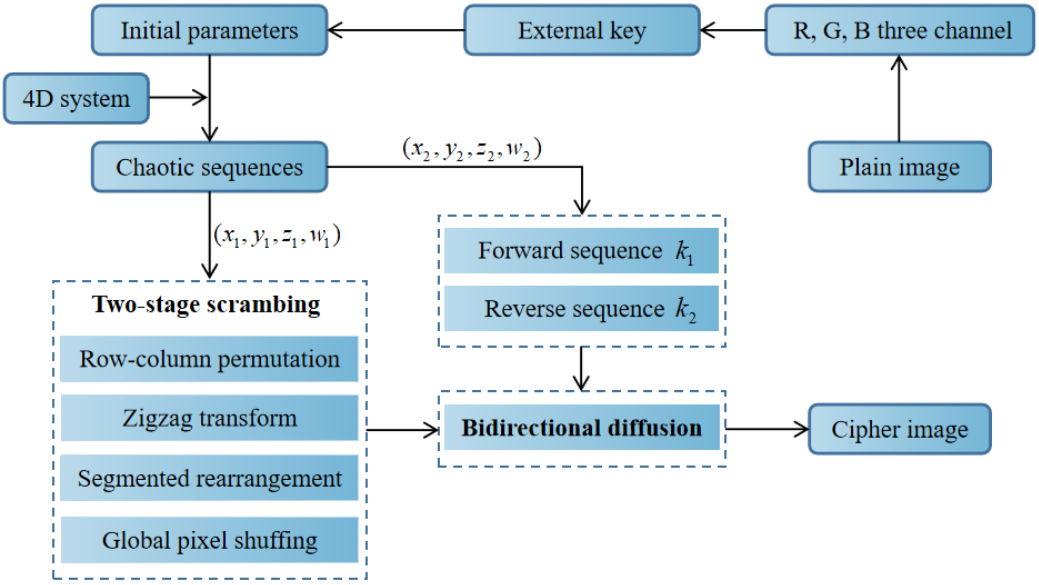


Figure 7. Framework of the proposed color image encryption scheme.

3.1. Key initialization

The key initialization mechanism of this scheme is based on external keys. The external key is used to deterministically generate the initial state and control parameters of the proposed four-dimensional chaotic system, so that the same chaotic sequence can be reproduced during encryption and decryption processes. Specifically, user-defined external keys are first converted into binary sequences and then divided into several sub blocks. These sub blocks are further normalized and mapped to initial conditions (x_0, y_0, z_0, w_0) and corresponding control parameters within predefined intervals. In this way, the generated chaotic trajectory is completely determined by the external key, ensuring the reversibility and practical feasibility of the encryption scheme. In order to improve the sensitivity of the scheme to plaintext changes, the SHA-512 hash value of the plaintext image is introduced as an auxiliary perturbation factor during the encryption process. Due to the avalanche effect of SHA-512, small modifications in plaintext images will cause significant changes in the generated perturbations, thereby improving plaintext sensitivity. The factor that relies on plaintext is not the key itself, nor does it affect the reversibility of the decryption process. After determining the initial state and parameters, the four-dimensional chaotic system is iterated to generate chaotic sequences for scrambling and diffusion. Since the initialization process is driven by an external key in a deterministic manner, the same key can regenerate the same chaotic sequence, providing a foundation for accurate decryption.

3.2. Chaotic two-stage scrambling

The purpose of scrambling is to destroy the spatial correlation among plaintext pixels. Driven by chaotic sequences, the proposed two-stage scrambling strategy combines row-column permutation, zigzag transformation, segmented rearrangement, and global shuffling to enhance pixel-position randomness and prepare for the subsequent diffusion process. The detailed procedure for the chaotic

two-stage scrambling is outlined as follows.

Step 1. Chaotic row-column exchange of the original image pixel matrix. The pixel matrix of the original image is subjected to chaotic row and column exchange. The four-dimensional chaotic sequence, derived from the four-dimensional chaotic system, entails the selection of the initial N elements and the final N elements of the x-dimension sequence, which are then organized in ascending order. Initially, the pixel matrix of the original image undergoes a transformation in the row dimension, followed by a subsequent transformation in the column dimension. This operation preliminarily breaks the local spatial structure of the image and weakens the direct adjacency relationship among neighboring pixels.

Step 2. Zigzag transformation. The pixel matrix, after undergoing chaotic row and column permutation, is subjected to a zigzag transformation and subsequently flattened into a one-dimensional array, denoted as a. The zigzag transformation further converts the two-dimensional spatial arrangement into a one-dimensional sequence, which facilitates subsequent nonlocal rearrangement.

Step 3. Segmented rearrangement. The elements of the second and fourth segments of the four-dimensional chaotic sequence y are selected in ascending order. Then the elements of the first and third segments in the sequence z are arranged in ascending order. The flattened one-dimensional array a is divided into four groups from beginning to end, and the generated four indexes are used to rearrange it four times to obtain a new one-dimensional array b. The segmented rearrangement enhances the disruption of local continuity by performing multiple index-driven permutations on different parts of the sequence.

Step 4. Global shuffling. The w-dimensional sequence in the four-dimensional chaotic sequence is sorted according to numerical ascending order, and the obtained index is globally shuffled on the array b to obtain the scrambled array c. The global shuffling operation further improves the global mixing effect and makes the pixel positions more difficult to trace.

Step 5. Inverse zigzag transformation. The one-dimensional array c undergoes an inverse zigzag transformation to derive the final scrambled matrix.

Through the above hierarchical operations, both local adjacency and global positional regularity of the plaintext image are effectively destroyed, providing a suitable basis for the subsequent diffusion stage, and a quantitative comparison between the single-level scrambling counterpart and the proposed two-stage scrambling scheme is provided in Section 4.1.

The scrambling process for the 4×4 original image is depicted in Figure 8.

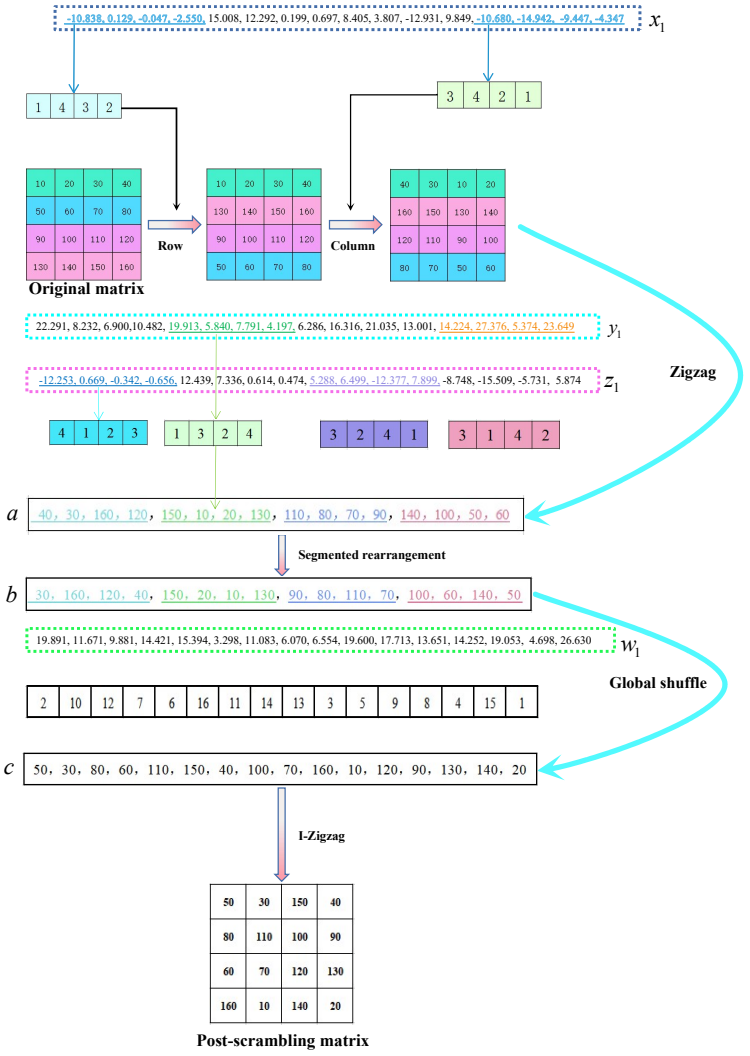


Figure 8. Scrambling process.

3.3. Diffusion process

Diffusion is implemented by adjusting image pixel values, essentially serving as a key step to encrypt image data and enhance security. The core idea is that it can spread the change of a pixel to other pixels, so that any pixel can affect the surrounding, or even farther away pixels after modification. Through this operation, the original content of the image becomes uncertain, and it also makes it more difficult for the attacker to crack. Diffusion usually uses a modulo operation, XOR, to ensure that the result is always within the effective gray value range. This additionally complicates the statistical connection between plaintext and ciphertext, thereby hindering attackers from deducing the original information from the ciphertext.

The forward diffusion and backward diffusion exhibit symmetrical features in both their structural design and operational mechanisms. This diffusion algorithm facilitates multi-directional synchronous adjustments for each pixel. As a result, it effectively enhances both the coverage and the depth of

influence during the diffusion process, thereby augmenting the overall efficacy of the algorithm. The subsequent sections elaborate on the comprehensive methodology for both the forward and reverse processes of random multi-directional diffusion.

Let the single-channel scrambled image matrix be $X \in \mathbb{Z}^{H\times W}$, where H is the image height and W is the width. The forward diffusion factor matrix generated by system (2.1) is K_1, the reverse diffusion factor is K_2, the forward diffusion output matrix is Y, the reverse diffusion output matrix is Z, the one-dimensional sequence is k_1, k_2, $\tilde{Y}$, $\tilde{Z}$, and the final diffusion output matrix is C.

The iterative equations that define the forward random multi-directional diffusion process are provided by Eq (3.1).

$$\boldsymbol{Y}(m,n) = \begin{cases} (\boldsymbol{X}(m,n) \oplus \boldsymbol{K}_1(m,n)) \bmod 256, & m = 0,\ n = 0; \\ (\boldsymbol{X}(m,n) \oplus \boldsymbol{K}_1(m,n) \oplus \boldsymbol{Y}(m,n-1)) \bmod 256, & m = 0,\ 1 \le n \le W-1; \\ (\boldsymbol{X}(m,n) \oplus \boldsymbol{K}_1(m,n) \oplus \boldsymbol{Y}(m-1,n)) \bmod 256, & 1 \le m \le H-1,\ n = 0; \\ (\boldsymbol{X}(m,n) \oplus \boldsymbol{K}_1(m,n) \oplus \boldsymbol{Y}(m-1,n-1) & 1 \le m \le H-1,\ 1 \le n \le W-1. \\ \quad \oplus \boldsymbol{Y}(m,n-1) \oplus \boldsymbol{Y}(m-1,n)) \bmod 256, & \end{cases} \tag{3.1}$$

The iterative equations characterizing the backward random multi-directional diffusion process are delineated as Eq (3.2).

$$\boldsymbol{Z}(m,n) = \begin{cases} (\boldsymbol{Y}(m,n) \oplus \boldsymbol{K}_2(m,n)) \bmod 256, & m = H-1,\ n = W-1; \\ (\boldsymbol{Y}(m,n) \oplus \boldsymbol{K}_2(m,n) \oplus \boldsymbol{Z}(m,n+1)) \bmod 256, & m = H-1,\ 0 \le n \le W-2; \\ (\boldsymbol{Y}(m,n) \oplus \boldsymbol{K}_2(m,n) \oplus \boldsymbol{Z}(m+1,n)) \bmod 256, & 0 \le m \le H-2,\ n = W-1; \\ (\boldsymbol{Y}(m,n) \oplus \boldsymbol{K}_2(m,n) \oplus \boldsymbol{Z}(m+1,n+1) & 0 \le m \le H-2,\ 0 \le n \le W-2. \\ \quad \oplus \boldsymbol{Z}(m,n+1) \oplus \boldsymbol{Z}(m+1,n)) \bmod 256, & \end{cases} \tag{3.2}$$

The following are the specific steps of chaotic forward diffusion.

Step 1. Generate diffusion sequences. Using the generated second chaotic sequence, first select any two variable chaotic sequences. Then it is divided into four segments according to the same length. The first and third segments of one are selected, and the second and fourth segments of the other are selected to form a one-dimensional chaotic sequence.

Step 2. Quantize the sequence. Quantize the new two-dimensional chaotic sequence to obtain a one-dimensional array k_1 with a value of $[0, 255]$. k_1 is a one-dimensional array of matrix K_1 expanded by rows. The specific quantitative equation is shown in Eq (3.3).

$$k_1 = \bmod\left(\text{floor}\left[\left(\sin(\pi k_{1i}) \cdot \cos(2\pi k_{1i}) + \frac{(k_{1i})^3}{3}\right) \times 10^3\right], 256\right), i = 0, 1, \ldots, L-1. \tag{3.3}$$

Step 3. Execute forward diffusion. The matrix X obtained by the scrambling process is expanded into a one-dimensional array according to the zigzag change. Then the one-dimensional array and k_1 are iterated according to the forward diffusion equation. The forward diffusion image sequence Y_1 is obtained.

The main difference between chaotic reverse diffusion and forward diffusion is actually the opposite direction. The detailed procedures are outlined below.

Step 1. Generate the reverse diffusion sequence. Among the four-dimensional chaotic sequences used in the diffusion process, the remaining two one-dimensional sequences are selected to generate a new one-dimensional chaotic sequence in the same way.

Step 2. Chaotic sequence quantization. By quantifying the new chaotic one-dimensional sequence, a one-dimensional array k_2 with a value of $[0, 255]$ is obtained. k_2 is a one-dimensional array of row-wise expansions of matrix K_2, with the quantization equation defined as Eq (3.4).

$$k_2 = \mathrm{mod}\left(\mathrm{floor}\left[\left(\sin(\pi k_{2i}) \cdot \cos(2\pi k_{2i}) + \frac{(k_{2i})^3}{3}\right) \times 10^3\right], 256\right), i = 0, 1, \ldots, L-1. \tag{3.4}$$

To justify the adopted nonlinear quantization strategy, a brief comparative analysis with two commonly used quantization methods is provided below.

To evaluate whether the adopted quantization formulas in Eqs (3.3) and (3.4) provide better randomness for the diffusion factors, a comparative experiment was conducted using the same raw chaotic sequence. For fairness, all compared methods were implemented under the same initial condition, the same chaotic source, and the same sequence length.

In addition to the proposed nonlinear quantization strategy, two commonly used quantization methods were considered. The first is a simple modulo-based mapping, defined as

$$k_i^{(1)} = \mathrm{mod}\left(\left\lfloor |s_i| \times 10^{14} \right\rfloor, 256\right),$$

where s_i denotes the raw chaotic sequence. The second is a linear scaling method, defined as

$$k_i^{(2)} = \left\lfloor 255 \cdot \frac{s_i - s_{\min}}{s_{\max} - s_{\min} + \varepsilon} \right\rfloor,$$

where $s_{\min}$ and $s_{\max}$ are the minimum and maximum values of the sequence, respectively, and ε is a small positive constant.

Three indicators were employed for evaluation, namely, information entropy, adjacent-element correlation, and the chi-square statistic of the histogram distribution. The comparison results are listed in Table 1. It can be observed that the proposed quantization strategy yields entropy values closer to the ideal value, lower adjacent-element correlation, and better histogram uniformity than the other two methods. This indicates that the adopted nonlinear quantization method provides better randomness and is more suitable for constructing diffusion factors in the proposed encryption framework.

Table 1. Comparison of different chaotic-sequence quantization methods.

Quantization method	Entropy	Pixel correlation	Chi-square
Simple modulo mapping	7.9988	0.0753	1745.58
Linear scaling	7.7698	0.0988	1203.84
Proposed nonlinear quantization	7.9998	0.0006	236.14

Step 3. Diffusion iteration and matrix conversion. The sequence $\tilde{Y}$ obtained by forward diffusion and the sequence k_2 obtained by quantization are iterated according to the iterative equation to obtain the sequence $\tilde{Z}$. This $\tilde{Z}$ is then converted into a matrix according to the row priority, and the diffused image C is obtained.

The entire diffusion process of the original image, taking a 4×4 matrix as an example, is illustrated in Figure 9.

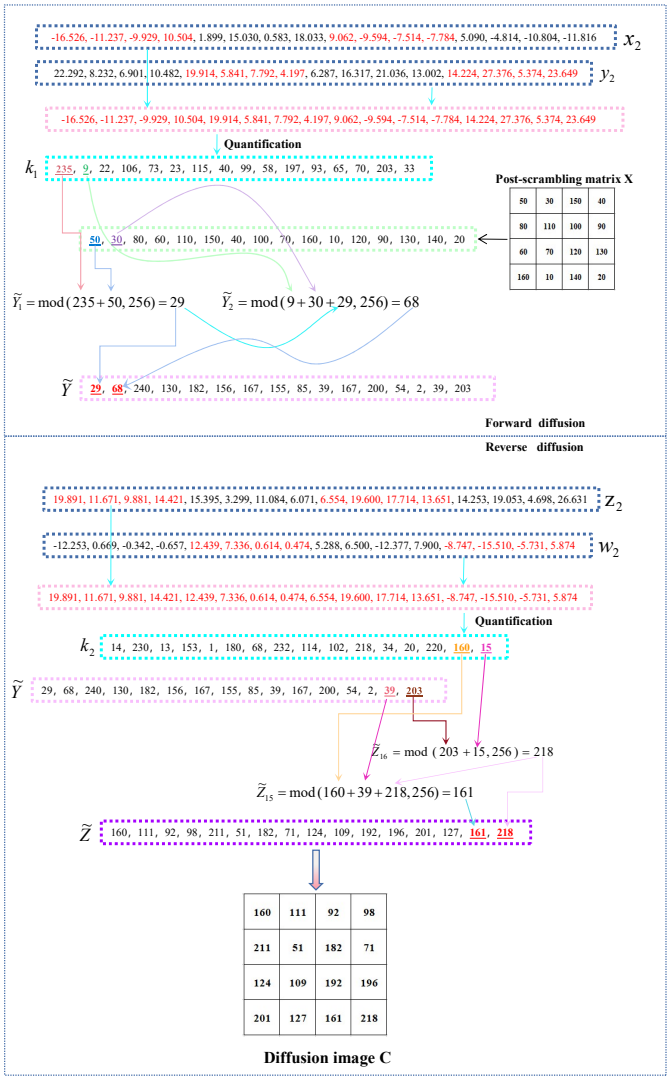


Figure 9. Diffusion process.

The proposed image encryption scheme is fully reversible. During decryption, the same external secret key is used to regenerate the initial states and chaotic sequences required by the encryption process. The inverse reverse-diffusion operation is first performed, followed by the inverse forward-diffusion operation. Then, inverse global shuffling, inverse segmented rearrangement, inverse zigzag transformation, and inverse chaotic row-column exchange are applied successively. Since all operations are deterministic and invertible, the plaintext image can be accurately reconstructed when the correct secret key is provided.

4. Simulation and evaluation

This section provides a thorough evaluation of the performance and security features of the proposed algorithm. Encryption tests are conducted on color images of varying sizes. Simulations were run on a computer compatible with the Windows-11 operating system (16.00 GB memory and 13th Gen Intel (R) Core (TM) i5-13500H (2.60 GHz), on MATLAB 2020a and PyCharm 2025.2. All experimental images are from four well-known benchmark databases: USC-SIPI, CVIT, IPP, and MIT VisTex. The selected test images include a $256 \times 256 \times 3$ House image, a $512 \times 512 \times 3$ Airplane image, a Texture image, a $1024 \times 1024 \times 3$ Barbara image, and a $768 \times 512 \times 3$ Aeroview image. Figure 10 presents simulation results, where the generated ciphertext images effectively obscure the original plaintext's information characteristics.

Following image testing, multi-dimensional security evaluations of the encryption scheme are conducted. These include key space analysis, information entropy calculation, pixel histogram distribution characteristics analysis, pixel correlation analysis, and anti-differential attack analysis. The research results indicate that this encryption technology provides robust security for color images of various sizes and resolutions.

4.1. Quantitative evaluation of the scrambling effect

To quantitatively verify the effectiveness of the proposed two-stage scrambling scheme, a comparative experiment was conducted between a single-level scrambling counterpart and the complete proposed two-stage scrambling scheme. The adjacent-pixel correlation coefficients of the scrambled image in the horizontal, vertical, and diagonal directions were employed for evaluation, since they directly reflect the extent to which local positional dependence is destroyed.

Table 2 summarizes the quantitative comparison results. It can be observed that the single-level scrambling counterpart still retains relatively strong adjacent-pixel correlation, whereas the proposed two-stage scrambling scheme reduces the corresponding correlation coefficients to values very close to zero in all three directions.

These results indicate that the single-level scrambling counterpart can only provide limited positional disruption, especially in the horizontal direction, where strong local dependence is still preserved. In contrast, the proposed two-stage scrambling scheme more effectively destroys local spatial adjacency and provides a better foundation for the subsequent diffusion stage.

Table 2. Comparison of scrambling effectiveness between the single-level scrambling counterpart and the proposed two-stage scrambling scheme.

Method	Horizontal	Vertical	Diagonal
Single-step scrambling	0.6748	0.0946	0.0917
Proposed scrambling	-0.0001	-0.0004	-0.0014

4.2. Key space analysis

The key space of a cryptosystem refers to the entire collection of unique keys that can be produced, and it is an essential factor in evaluating the system's resilience to brute-force attacks. This section

evaluates the key space associated with the proposed encryption framework in order to analyze its security levels. The key space of the proposed scheme is mainly determined by the external secret key and the precision used for mapping the initial states and control parameters of the chaotic system. The specific calculation is as follows.

(i) Initial states and control parameters of system (2.1). The external secret key is mapped to the initial states (x_0, y_0, z_0, w_0) and the corresponding control parameters within predefined intervals. Assuming a floating-point precision of 10^{-15}, the contribution of these parameters to the key space can be estimated accordingly. Each parameter is mapped to the range $[-1, 1)$ with a floating-point precision of 10^{-15}. The number of possible values for a single parameter is 2×10^{15}. For the four parameters, the key space contribution is about 2^{203}.

(ii) External user-defined key. In order to ensure consistently high security performance and compatibility with the proposed encryption framework, the external key is normalized to 256-bit integers. This length is selected to balance computational efficiency and resist exhaustive attacks. The key space corresponding to the 256-bit key is 2^{256}, which far exceeds the computational feasibility threshold of exhaustive cracking under current and foreseeable computing resources.

The overall key space is characterized as the multiplicative combination of the contributions from the parameters of the chaotic system and the external keys. It reaches 2^{459}, giving the scheme strong key space performance and enhancing its ability to resist brute-force attacks.

To further evaluate the effectiveness of the proposed key generation strategy, the key space of the proposed scheme is compared with those of several representative chaos-based image encryption algorithms reported in the literature. The selected schemes cover different chaotic dimensions and key construction mechanisms, providing a fair and comprehensive comparison. The comparison results are summarized in Table 3.

Table 3. Comparison of key space sizes for different algorithms.

Algorithms	Proposed	[26]	[27]	[32]	[33]	[37]
Key space	$\geq 2^{459}$	2^{298}	2^{186}	2^{409}	2^{164}	2^{340}

As shown in Table 3, the proposed scheme achieves a larger key space than the compared methods, which significantly enhances its resistance to exhaustive key search attacks.

From a cryptographic perspective, a sufficiently large key space is the basic prerequisite for resisting exhaustive search attacks. Therefore, the large key space of the proposed scheme provides the theoretical foundation for brute-force resistance.

4.3. Key sensitivity analysis

To further verify the security of the proposed key system, key sensitivity experiments were conducted by introducing minimal perturbations into the secret key, including a one-bit change in the external key and a tiny perturbation in one chaotic initial parameter.

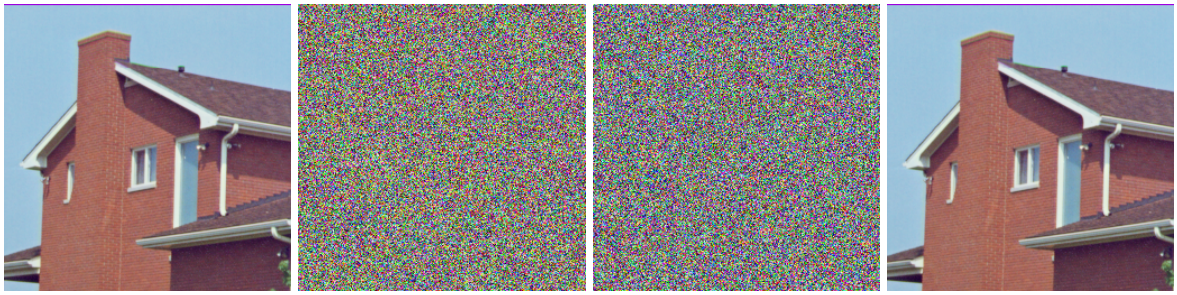
Let K and K' denote the original and perturbed keys, respectively. The same plaintext image was encrypted using both keys, and the resulting ciphertext images were compared in terms of the NPCR, UACI, and correlation coefficient. As shown in Table 4, even an extremely small key perturbation leads to a drastic change in the ciphertext image. The NPCR and UACI values remain close to their desirable

ranges, while the correlation coefficient remains close to zero. These results confirm the strong key avalanche effect of the proposed scheme.

Table 4. Results of encryption key sensitivity analysis.

Key perturbation	NPCR (%)	UACI (%)	Corr
$K \rightarrow K \oplus 1$	99.5992	33.5127	0.001357
$x_0 \rightarrow x_0 + 10^{-15}$	99.6109	33.3842	0.004205

To further verify the sensitivity of the decryption process to the secret key, the ciphertext generated by the original key was decrypted using the perturbed key. The corresponding results are shown in Figure 10. It can be seen that the decrypted image under the wrong key is completely noise-like and contains no visually recognizable plaintext information. This indicates that the proposed encryption scheme is highly sensitive to key mismatch and can effectively resist brute-force and key guessing attacks.



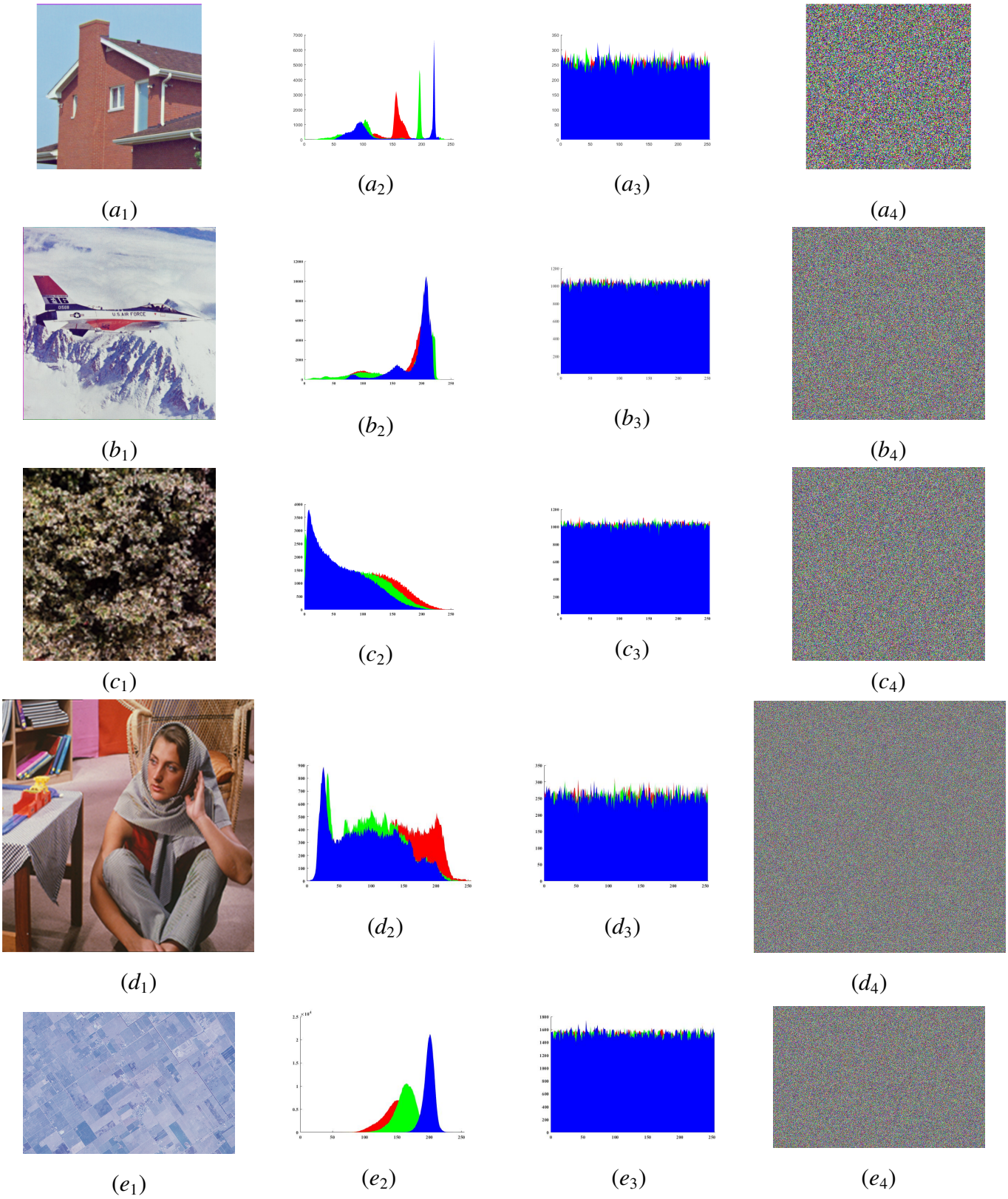
(a) (b) (c) (d)

Figure 10. Key sensitivity results of the House image: (a) plaintext image, (b) decrypted image with a perturbed initial parameter $x_0 + 10^{-15}$, (c) decrypted image with a one-bit changed external key, and (d) correctly decrypted image.

4.4. Histogram analysis

A histogram is an effective tool for describing the distribution of pixel intensity values in an image. In general, a visually meaningful plaintext image exhibits a non-uniform histogram, whereas the histogram of a secure ciphertext image should ideally be uniform.

As shown in Figure 11, the histogram of the original image is continuous and highly concentrated, preserving clear statistical characteristics. In contrast, the histogram of the encrypted image is much more uniform and differs significantly from that of the plaintext image. This indicates that the proposed encryption scheme effectively conceals the statistical features of the original image, thereby enhancing its resistance to statistical attacks.



(a_1) (a_2) (a_3) (a_4)

(b_1) (b_2) (b_3) (b_4)

(c_1) (c_2) (c_3) (c_4)

(d_1) (d_2) (d_3) (d_4)

(e_1) (e_2) (e_3) (e_4)

Figure 11. Histogram analysis results. Rows (a)–(e) correspond to House, Airplane, Texture, Barbara, and Aeroview, respectively.

In Figure 11, the first four columns sequentially display the original image, its associated histogram, the encrypted image, and the histogram corresponding to the encrypted image.

A nearly uniform ciphertext histogram indicates that the original gray-level distribution has been effectively flattened by the proposed encryption process. From a theoretical perspective, this reduces the exploitable statistical redundancy of the plaintext image and weakens the feasibility of histogram-based statistical attacks.

4.5. Correlation analysis

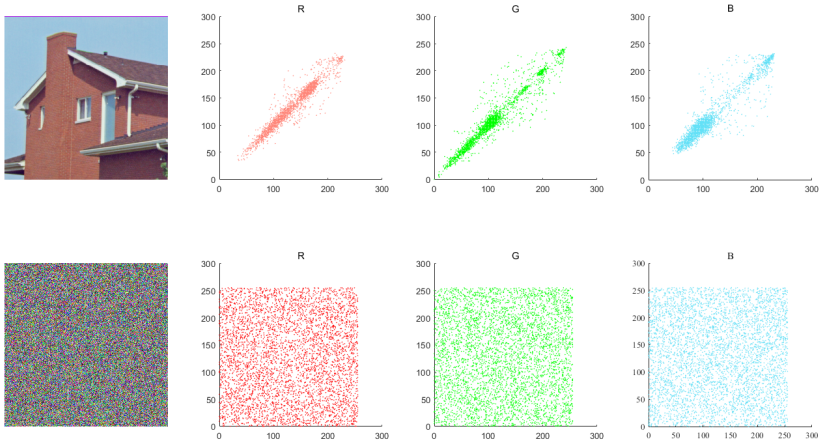
Correlation serves as an essential parameter utilized to assess the degree of interdependence between neighboring pixels. In a secure image encryption scheme, the encrypted image should have a correlation of adjacent pixels close to 0. This indicates nearly no linear relationship between pixels. Let x and y denote two adjacent pixels, with their correlation calculated as indicated in Eq (4.1).

$$\begin{cases} \mu = \frac{1}{N}\sum_{i=1}^{N} x_i, \\ \sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2, \\ \mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y), \\ \rho_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{\sigma_x^2\sigma_y^2}}, \end{cases} \tag{4.1}$$

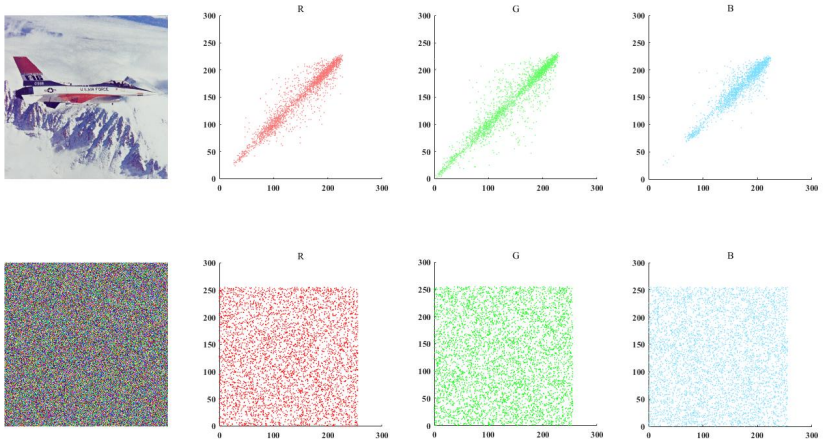
where N is the total number of pixel pairs selected for calculation, μ_x and μ_y are the means of x and y, respectively, σ_x^2 and σ_y^2 are the variances of x and y, $\mathrm{cov}(x, y)$ is the covariance between x and y, and ρ_{xy} is the correlation coefficient.

This section presents scatter plots of adjacent pixels in five color images and their encrypted versions, highlighting horizontal, vertical, and diagonal correlations. Original images show strong correlation along the line $y = x$, suggesting pixel dependency that could facilitate attacks. In contrast, encrypted images exhibit uniform scatter across orientations, indicating a significant reduction in correlation. This randomness disrupts the original image patterns, demonstrating the proposed scheme's effectiveness against statistical attacks. The pixel correlation distributions for five sets of experimental images are shown in Figure 12, with correlation coefficients detailed in Table 5.

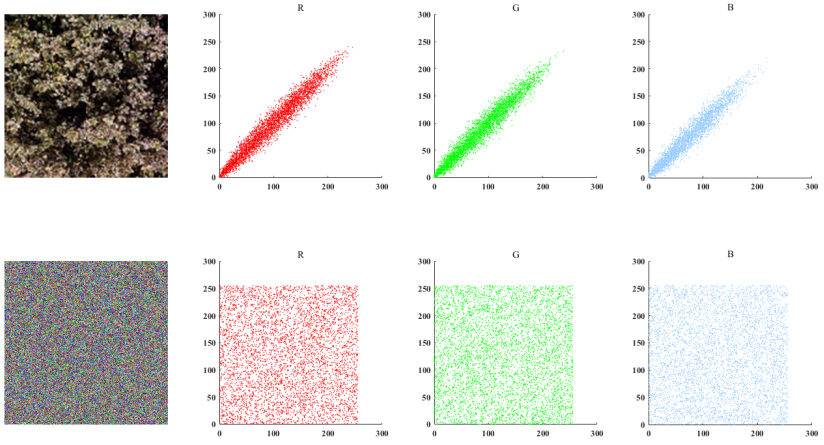
In natural images, adjacent pixels usually exhibit strong local dependence due to spatial continuity. The proposed hierarchical scrambling destroys the positional adjacency of pixels, while the subsequent bidirectional diffusion further disturbs their intensity relationship. Therefore, the correlation coefficients approaching zero indicate that both spatial and value-level dependencies have been effectively suppressed, which improves resistance to statistical analysis.



(a)

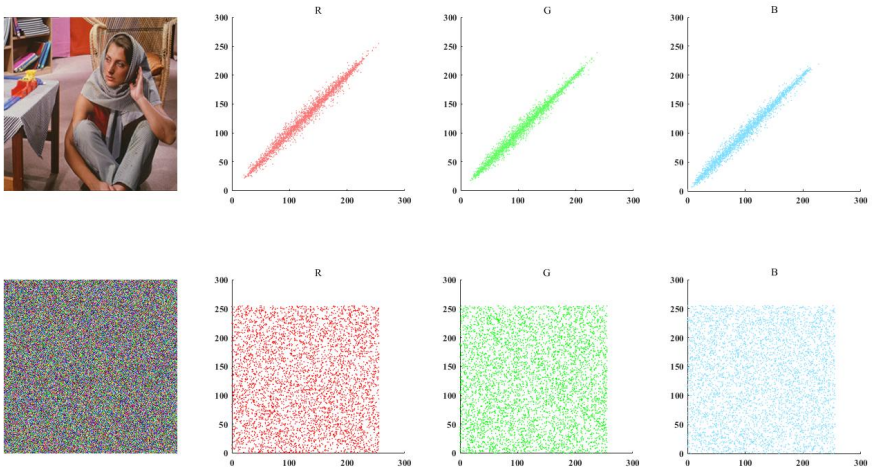


(b)

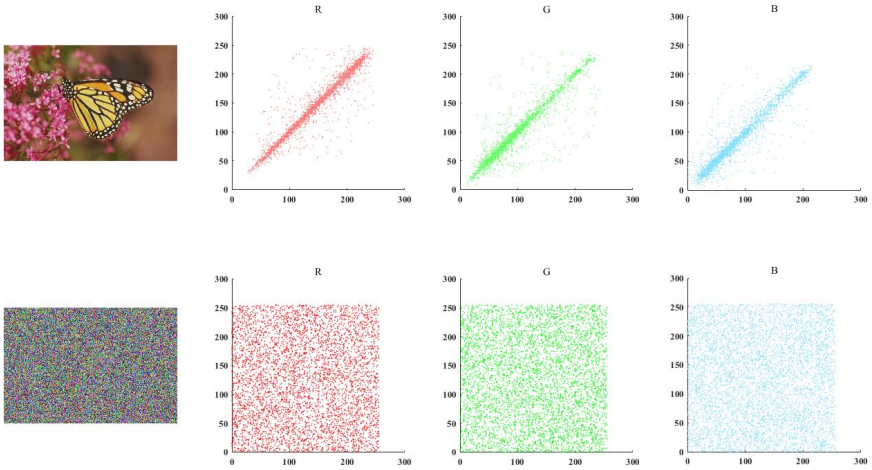


(c)

Continued on next page



(d)



(e)

Figure 12. Correlation scatter plots of color images: (a) house, (b) airplane, (c) texture, (d) barbara, and (e) aeroview.

Table 5. Correlation coefficients of adjacent pixels in the image.

		Plaintext image			Ciphertext image		
Images	Channels	H	V	D	H	V	D
	R	0.9403	0.9742	0.9255	-0.0072	0.0048	0.0050
House	G	0.9500	0.9669	0.9279	0.0178	0.0045	0.0209
	B	0.9431	0.9634	0.9203	-0.0067	-0.0087	-0.0010
	R	0.9686	0.9733	0.9447	0.0072	-0.0074	-0.0113
Airplane	G	0.9646	0.9722	0.9458	0.0184	0.0059	0.0063
	B	0.9591	0.9570	0.9274	-0.0001	-0.0102	0.0072
	R	0.9803	0.9797	0.9616	0.0013	-0.0091	-0.0027
Texture	G	0.9798	0.9789	0.9606	-0.0119	-0.0015	0.0119
	B	0.9764	0.9753	0.9541	0.0129	-0.0036	0.0175
	R	0.9686	0.9733	0.9447	-0.0284	0.0025	0.0236
Barbara	G	0.9646	0.9722	0.9458	0.0147	0.0207	0.0013
	B	0.9591	0.9570	0.9274	-0.0097	-0.0098	-0.0076
	R	0.9686	0.9733	0.9447	-0.0127	-0.0097	-0.0026
Aeroview	G	0.9646	0.9722	0.9458	0.0095	0.0036	-0.0194
	B	0.9591	0.9570	0.9274	0.0137	0.0012	-0.0025

4.6. Information entropy analysis

Information entropy functions as an essential parameter for evaluating the uncertainty attributes of an image, conveying the depth and intricacy of the information embedded within it. In a secure encryption framework, it is essential to ensure that the information entropy of the encrypted image closely matches its theoretical expectation. For an 8-bit image channel, the theoretical maximum information entropy is 8 bits. Therefore, the entropy of an encrypted image is expected to be close to 8. This suggests that the pixel values in the image demonstrate a considerable level of randomness and lack of predictability.

Table 6 below summarizes the results of the information entropy assessments conducted for both the original and the encrypted images generated through the proposed methodology discussed in this section. The results indicate that the information entropy of the encrypted images closely aligns with the theoretical maximum value of 8. This result not only confirms the effectiveness of the proposed method in improving data security but also underscores the inherent uncertainty attributes of the information present within the encrypted images. A higher level of information entropy indicates an increased uncertainty in the image, thereby obstructing an attackers ability to reconstruct the original data using elementary statistical analyses or pattern recognition techniques. Therefore, the difficulty faced by the attacker when trying to crack also increases, which provides an additional line of defense for data protection.

Table 6. Information entropy analysis.

Images	Size	Original images			Encrypted images		
		R	*G*	*B*	*R*	*G*	*B*
House	$256 \times 256 \times 3$	7.2353	7.5683	6.9176	7.9974	7.9977	7.9977
Airplane	$512 \times 512 \times 3$	6.7229	6.8105	6.2240	7.9995	7.9993	7.9993
Texture	$512 \times 512 \times 3$	7.6855	7.5227	7.2953	7.9994	7.9993	7.9994
Barbara	$1024 \times 1024 \times 3$	7.5908	7.4377	7.5126	7.9998	7.9998	7.9998
Aeroview	$768 \times 512 \times 3$	6.4983	6.0562	6.0788	7.9996	7.9995	7.9997

Although the above results demonstrate that the proposed scheme achieves information entropy values close to the theoretical maximum, a comparative analysis with existing methods is necessary to further evaluate its relative performance. Therefore, the information entropy of the proposed scheme is compared with several representative chaos-based image encryption algorithms under identical image resolutions. The comparison results are summarized in Table 7.

Table 7. Comparison of information entropy for different image sizes.

Scheme	256×256			512×512		
	R	*G*	*B*	*R*	*G*	*B*
[32] (2023)	7.9973	7.9972	7.9972	7.9994	7.9993	7.9993
[34] (2021)	-	-	-	7.9853	7.9630	7.9976
[36] (2024)	-	-	-	7.9992	7.9992	7.9992
[38] (2024)	-	-	-	7.9987	7.9985	7.9984
Proposed	7.9975	7.9976	7.9977	7.9995	7.9993	7.9993

Note: The symbol "-" indicates that the corresponding channel information entropy values of *R*, *G*, and *B* for a given original image size are not listed in the cited literature.

It should be noted that slight differences in entropy values may result from variations in test images, image resolutions, and evaluation methods adopted in different studies.

4.7. Anti-differential attack analysis

Differential attacks represent a common cryptographic threat, where slight modifications to plaintext can result in corresponding changes in ciphertext. An effective encryption scheme should ensure that minor variations in the input lead to significant discrepancies in the output, thereby complicating the efforts of an attacker. To evaluate the capability of the encryption algorithm based on system (2.1) in resisting differential attacks, we utilize two metrics: the number of pixels change rate (NPCR) and the unified average change intensity (UACI). These metrics quantify the ciphertext's response to perturbations in plaintext from the perspectives of spatial distribution and intensity variation.

Assume two plaintext images P_1 and P_2 with size $W \times H$, where P_2 is obtained by introducing a 1-pixel perturbation to P_1, and their corresponding ciphertexts after encryption are C_1 and C_2 (size

$W \times H$). The NPCR measures the proportion of pixel positions of different values between C_1 and C_2, reflecting the degree of diffusion of local plaintext perturbation in ciphertext. The formula for calculation is presented as Eq (4.2).

$$\text{NPCR} = \frac{\sum_{m=1}^{W}\sum_{n=1}^{H} D(m,n)}{W \times H} \times 100\%, \tag{4.2}$$

where the binary indicator $D(m,n)$ is defined as Eq (4.3).

$$D(m,n) = \begin{cases} 1, & \text{if } C_1(m,n) \neq C_2(m,n), \\ 0, & \text{if } C_1(m,n) = C_2(m,n). \end{cases} \tag{4.3}$$

The ideal value of the NPCR (for 256-level grayscale images) is 99.6094%. The UACI quantifies the average intensity difference of the changed pixels between C_1 and C_2, reflecting the severity of the ciphertext change caused by the plaintext perturbation. The formula for calculation is presented as Eq (4.4).

$$\text{UACI} = \frac{1}{W \times H}\left(\sum_{m=1}^{W}\sum_{n=1}^{H} \frac{|C_1(m,n) - C_2(m,n)|}{255}\right) \times 100\%, \tag{4.4}$$

where $|C_1(m,n) - C_2(m,n)|$ represents the absolute difference of pixel intensity, and 255 is the maximum intensity value of an 8-bit grayscale image. The optimal value for the UACI is 33.4635%.

Table 8 presents the quantitative outcomes of the NPCR and UACI metrics evaluated on test images of various sizes. The results obtained from the proposed algorithm across different types of images align closely with the theoretical ideal values, with deviations remaining minimal. This finding confirms the strong diffusion capability of the proposed algorithm with respect to pixel-level perturbations.

Table 8. Results of NPCR and UACI performance.

Images	NPCR (%)			UACI (%)		
	R	*G*	*B*	*R*	*G*	*B*
House	99.6124	99.6131	99.6063	33.4563	33.4639	33.4766
Airplane	99.6059	99.6067	99.6078	33.4630	33.4608	33.4643
Texture	99.6064	99.6034	99.6181	33.4657	33.4719	33.4609
Barbara	99.6076	99.5987	99.5989	33.4419	33.5068	33.5038
Aeroview	99.6094	99.6071	99.6094	33.4644	33.4744	33.4623

Although the above results demonstrate that the proposed scheme achieves NPCR and UACI values close to the theoretical optima, a comparative analysis with existing methods is conducted to further assess its relative performance. Accordingly, the NPCR and UACI results are compared with several representative chaos-based image encryption schemes under identical image resolutions, as summarized in Tables 9 and 10.

It should be noted that minor differences in NPCR and UACI values may arise from variations in test images, image resolutions, and experimental settings adopted in different studies.

Table 9. Comparison of NPCR (%) values for different algorithms under identical image resolutions.

Image size	Algorithm	*R*	*G*	*B*	Average
256 × 256	Proposed	99.6124	99.6131	99.6063	99.6106
	[27] (2022)	99.6213	99.6000	99.6147	99.6120
	[32] (2023)	-	-	-	99.6338
512 × 512	Proposed	99.6075	99.6098	99.6075	99.6083
	[27] (2022)	99.6215	99.6064	99.6110	99.6130
	[32] (2023)	-	-	-	99.6155
	[36] (2024)	-	-	-	99.5956
	[37] (2025)	-	-	-	99.6005

Note: The symbol "-" indicates that the corresponding channel-wise NPCR values of the *R*, *G*, and *B* channels are not reported in the cited literature, only the average value over the three channels is provided.

Table 10. Comparison of UACI (%) values for different algorithms under identical image resolutions.

Image size	Algorithm	*R*	*G*	*B*	Average
256 × 256	Proposed	33.4563	33.4639	33.4766	33.4656
	[27] (2022)	33.4931	33.4763	33.4421	33.4705
	[32] (2023)	-	-	-	33.4589
512 × 512	Proposed	33.4653	33.4594	33.4756	33.4667
	[27] (2022)	33.4546	33.4681	33.4502	33.4576
	[32] (2023)	-	-	-	33.4779
	[36] (2024)	-	-	-	33.4061
	[37] (2025)	-	-	-	33.4789

Note: The symbol "-" indicates that the corresponding channel-wise UACI values of the *R*, *G*, and *B* channels are not reported in the cited literature, only the average value over the three channels is provided.

It should be noted that the NPCR and UACI are saturation-type indicators. When different algorithms all approach the theoretical values, small numerical differences should not be regarded as the sole evidence of superiority. In this work, the NPCR and UACI mainly verify that the proposed scheme reaches the desired anti-differential level. The main advantages of the proposed method lie in the design of the square-term enhanced 4D chaotic system, quantization of the nonlinear chaotic sequence, hierarchical two-stage scrambling, a large key space, and strong sensitivity of the key.

4.8. Computational complexity and efficiency analysis

The computational complexity of the proposed encryption algorithm is analyzed according to its main operations. For a color plaintext image of size $H\times W\times 3$, let $L = H\times W$ denote the number of pixels

in each channel. The algorithm mainly consists of key initialization, chaotic sequence generation, two-stage scrambling, and symmetric bidirectional diffusion.

The key initialization and chaotic sequence generation stage requires one plaintext scan and generates chaotic sequences with lengths proportional to the image size. In the two-stage scrambling stage, row-column permutation, segmented rearrangement, and global shuffling involve sorting chaotic index sequences and performing index-based pixel rearrangement, while the zigzag and inverse zigzag transforms are implemented by sequential scanning and reconstruction. Therefore, the sorting-based scrambling operations constitute the main computational burden of the algorithm.

In the bidirectional diffusion stage, forward and reverse diffusion traverse all pixels successively and mainly involve XOR, a modular operation, and pixel-wise assignment. Hence, the diffusion cost increases approximately linearly with the number of pixels. Overall, the computational cost is mainly affected by the image size, sorting-based scrambling, and the number of permutation-diffusion rounds. The memory consumption mainly comes from chaotic sequences, permutation indexes, and intermediate images, and increases linearly with the image size.

To further evaluate the trade-off between security and computational efficiency, additional experiments were conducted by varying the number of permutation-diffusion rounds r. Specifically, $r = 1$, $r = 2$, and $r = 3$ were considered, and the corresponding encryption time, information entropy, NPCR, and UACI were recorded, as listed in Table 11.

Table 11. Computational efficiency and security performance under different iteration numbers.

Rounds r	Time (s)	Entropy	NPCR (%)	UACI (%)
1	0.89	7.9992	99.6062	33.4554
2	2.04	7.9993	99.6120	33.4573
3	4.62	7.9993	99.5972	33.4578

It can be observed that increasing the iteration number inevitably leads to a higher computational cost. However, the corresponding security indicators remain in the same desirable range and do not show a consistent or significant improvement as r increases. In particular, the entropy values remain very close to the ideal value, while the NPCR and UACI values stay close to their theoretical expectations. Therefore, additional permutation–diffusion rounds mainly increase the computational burden, while providing only marginal security gain. For this reason, the adopted fixed-iteration setting is considered a reasonable trade-off between security and efficiency, and one round is sufficient in the proposed scheme.

4.9. Noise robustness analysis

Although the proposed image encryption scheme is fully reversible under noise-free conditions, practical transmission channels may introduce disturbances into the ciphertext. To evaluate the decryption stability of the proposed algorithm under such conditions, noise robustness experiments were conducted by adding Gaussian noise and salt-and-pepper noise to the ciphertext image before decryption.

Specifically, Gaussian noise with variances of 1×10^{-5}, 3×10^{-5}, and 5×10^{-5}, and salt-and-pepper

noise with densities of 0.001, 0.003, and 0.005, were imposed on the ciphertext image. The noisy ciphertext images were then decrypted using the correct secret key. The quality of the recovered images was evaluated by the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM). The corresponding results are listed in Table 12.

Table 12. Noise robustness evaluation of the proposed encryption scheme.

Noise type	Noise level	PSNR (dB)	SSIM
Noise-free	0	∞	1.0000
Gaussian noise	1×10^{-5}	23.5348	0.7580
Gaussian noise	3×10^{-5}	21.0871	0.6581
Gaussian noise	5×10^{-5}	20.0370	0.6094
Salt-and-pepper noise	0.001	32.6150	0.9668
Salt-and-pepper noise	0.003	28.0590	0.9108
Salt-and-pepper noise	0.005	25.7710	0.8586

It can be observed that, although the injected noise inevitably degrades the recovered image quality, the main visual content and structural information of the plaintext image can still be preserved under low-intensity noise contamination. In particular, the decrypted results under low-intensity Gaussian noise and low-density salt-and-pepper noise remain visually recognizable. These results indicate that the proposed scheme has certain robustness against channel noise and can maintain acceptable decryption stability in the presence of low-level transmission disturbances.

5. Conclusions and outlook

To prevent the leakage of sensitive image information, this study proposed a square-term enhanced four-dimensional chaotic system and developed a color image encryption scheme based on hierarchical scrambling and symmetric bidirectional diffusion. Compared with representative existing four-dimensional chaotic systems, the proposed system exhibits a broader chaotic interval, stronger randomness, and improved attractor complexity. By combining the SHA-512 hash mechanism with the parameter characteristics of the proposed chaotic system, the encryption framework generates chaotic sequences for scrambling and diffusion, thereby producing secure ciphertext images. Experimental results show that the ciphertext histogram is approximately uniform, the adjacent-pixel correlation coefficients are close to zero, the information entropy is close to 8, and the NPCR and UACI values are close to their theoretical expectations. Moreover, the plaintext image can be accurately reconstructed during decryption with the correct key. These results demonstrate that the proposed scheme achieves good performance in security and reversibility, and has potential application value for secure image transmission and storage.

Nevertheless, the proposed scheme still has certain limitations from the perspective of practical engineering applications. The current validation is mainly based on numerical simulations and software experiments, while further investigation is still needed for real-time deployment, hardware-oriented implementation, and computational optimization under practical transmission environments. In addition, the robustness of the proposed framework under more complex communication conditions and large-scale image processing scenarios deserves further study.

In future work, several directions deserve further investigation. Adaptive parameter switching mechanisms may be introduced to improve the flexibility and efficiency of high-dimensional chaotic systems. Dynamic DNA operations can also be incorporated into the present framework to enhance the data-dependent nonlinear transformation capability. In addition, combining memristor computing or memristive neuron-map-based sequence generation may help develop more complex and hardware-friendly encryption architectures. A cross-layer secure image encryption framework that jointly considers spatial scrambling, transform-domain processing, and physical-layer protection may further provide a promising direction for practical secure multimedia communication.

Author contributions

Ping Gao: Conceptualization, validation, investigation, writing original draft, writing review and editing; **Tianxiu Lu:** validation, writing review and editing, supervision, funding acquisition; **Jiahua Dong:** formal analysis, investigation.

Funding sources

This research was funded by the Natural Science Foundation of Sichuan Province (No. 2023NSFC0070), the Graduate Student Innovation Fund (No. Y2025102), and the Luzhou Laojiao Graduate Student Innovation Fund (No. LJCX2024-8).

Use of AI tools declaration

The authors declare they have not used Artiffcial Intelligence (AI) tools in the creation of this article.

Data availability

All data and materials are openly available at https://sipi.usc.edu/database/ (USC-SIPI), https://www.imageprocessingplace.com/root_files_V3/image_databases.htm (IPP), https://vismod.media.mit.edu/pub/VisTex/FLAT/128x128/ (MIT VisTex), and https://www.cs.cmu.edu/ cil/v-images.html (CVIT).

Conflict of interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

1. A. Wajid, Z. P. Zhang, H. Muhammad, A novel chaotic-based image encryption scheme using multi-layer confusion and conditional diffusion, *Comput. Electr. Eng.*, **124** (2025), 110402. https://doi.org/10.1016/j.compeleceng.2025.110402
2. M. Yao, H. W. Deng, Z. Chen, P. Zhang, Efficient and secure image compression and encryption based on compressive sensing and four-dimensional hyperchaotic system, *Inf. Sci.*, **719** (2025), 122430. https://doi.org/10.1016/j.ins.2025.122430

3. Z. L. Man, J. Q. Li, X. Q. Di, Y. H. Sheng, Z. F. Liu, Double image encryption algorithm based on neural network and chaos, *Chaos, Solitons Fractals*, **152** (2021), 111318. https://doi.org/10.1016/j.chaos.2021.111318
4. B. Abd-El-Atty, A dual medical image encryption algorithm based on dynamic DNA operations, *Comput. Electr. Eng.*, **130** (2026), 110899. https://doi.org/10.1016/j.compeleceng.2025.110899
5. C. F. Zhao, Z. B. Zhai, B. Zeng, Delayed chaotic image encryption algorithm using cross-layer and DNA coding techniques, *Comput. Stand. Interfaces*, **93** (2025), 103974. https://doi.org/10.1016/j.csi.2025.103974
6. M. Alawida, A novel DNA tree-based chaotic image encryption algorithm, *J. Inf. Secur. Appl.*, **83** (2024), 103791. https://doi.org/10.1016/j.jisa.2024.103791
7. S. M. Wang, Q. Q. Peng, B. X. Du, Chaotic color image encryption based on 4D chaotic maps and DNA sequence, *Opt. Laser Technol.*, **148** (2022), 107753. https://doi.org/10.1016/j.optlastec.2021.107753
8. S. H. Yan, L. Li, W. L. Zhao, B. X. Gu, Design of a new four-dimensional chaotic system and its application to color image encryption, *Nonlinear Dyn.*, **111** (2023), 17519–17545. https://doi.org/10.1007/s11071-023-08726-x
9. B. Yogi, A. K. Khan, EHIES-ECCCA: An efficient hybrid image encryption scheme using ECC and cellular automata with secure shared key generation, *Signal Process. Image Commun.*, **144** (2026), 117527. https://doi.org/10.1016/j.image.2026.117527
10. C. F. Zhao, X. C. He, Y. F. Li, B. Zeng, Chaotic encryption algorithm for satellite images based on novel RNA coding, *Adv. Space Res.*, **75** (2025), 8334–8356. https://doi.org/10.1016/j.asr.2025.03.057
11. T. He, F. Yu, Y. Lin, S. Q. He, W. Yao, S. Cai, et al., Multi-scroll hopfield neural network excited by memristive self-synapses and its application in image encryption, *Chin. Phys. B*, **34** (2025), 120506. https://doi.org/10.1088/1674-1056/adfeff
12. Z. Huang, Z. Li, Q. Wang, W. J. Tan, X. M. Wu, A novel hyperchaotic multistable heterogeneous neural network with hidden attractors and its application in image encryption, *Chin. J. Phys.*, **96** (2025), 851–874. https://doi.org/10.1016/j.cjph.2025.05.037
13. F. Yu, X. Q. Wang, R. Y. Guo, Z. J. Ying, Y. He, Q. Zou, Discrete neuron models and memristive neural network mapping: A comprehensive review, *Chin. Phys. B*, **34** (2025), 120501. https://doi.org/10.1088/1674-1056/ae0a3b
14. L. Q. Huang, W. J. Li, X. M. Xiong, R. Yu, Q. X. Wang, S. T. Cai, Designing a double-way spread permutation framework utilizing chaos and S-box for symmetric image encryption, *Opt. Commun.*, **517** (2022), 128365. https://doi.org/10.1016/j.optcom.2022.128365
15. M. U. Safdar, T. Shah, A. Ali, Multiple-image encryption algorithm based on S-boxes and DNA Sequences, *Signal Process. Image Commun.*, **138** (2025), 117353. https://doi.org/10.1016/j.image.2025.117353
16. L. Shu, Y. Zhang, Z. W. Yu, L. T. Yang, M. Hauswirth, N. X. Xiong, Context-aware cross-layer optimized video streaming in wireless multimedia sensor networks, *J. Supercomput.*, **54** (2010), 94–121. https://doi.org/10.1007/s11227-009-0321-6

17. F. A. Khan, J. Ahmed, S. A. Alsuhibany, A new multi chaos-based compression sensing image encryption, *Comput. Mater. Continua*, **76** (2023), 437–453. https://doi.org/10.32604/cmc.2023.032236

18. X. L. An, S. Y. Liu, L. Xiong, J. G. Zhang, X. Y. Li, Mixed gray-color images encryption algorithm based on a memristor chaotic system and 2D compression sensing, *Expert Syst. Appl.*, **243** (2024), 122899. https://doi.org/10.1016/j.eswa.2023.122899

19. Y. L. Chen, T. X. Lu, G. R. Chen, Thumbnail-preserving encryption based on binary-decimal hybrid and a generalized coupled logistic map, *Int. J. Bifurcation Chaos*, **34** (2024), 2450193. https://dx.doi.org/10.1142/S0218127424501931

20. S. Gao, R. Wu, H. Ho-Ching Iu, U. Erkan, Y. Cao, Q. Li, et al., Chaos-based video encryption techniques: A review, *Comput. Sci. Rev.*, **58** (2025), 100816. https://doi.org/10.1016/j.cosrev.2025.100816

21. M. A. Ben Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation, *Opt. Laser Technol.*, **121** (2020), 105777. https://doi.org/10.1016/j.optlastec.2019.105777

22. Rohit, S. K. Tripathi, B. Gupta, S. Lamba, A companion matrix-based efficient image encryption method, *Signal Process.*, **228** (2025), 109753. https://doi.org/10.1016/j.sigpro.2024.109753

23. Z. Wang, T. Li, N. X. Xiong, Y. Pan, A novel dynamic network data replication scheme based on historical access record and proactive deletion, *J. Supercomput.*, **62** (2012), 227–250. https://doi.org/10.1007/s11227-011-0708-z

24. L. D. Singh, R. Thingbaijam, R. Patgiri, K. M. Singh, Cryptanalysis of cross-coupled chaotic maps multi-image encryption scheme, *J. Inf. Secur. Appl.*, **80** (2024), 103694. https://doi.org/10.1016/j.jisa.2023.103694

25. J. W. Yu, W. Xie, Z. Y. Zhong, H. Wang, Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation, *Chaos, Solitons Fractals*, **162** (2022), 112456. https://doi.org/10.1016/j.chaos.2022.112456

26. Y. Wang, K. W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters, *Chaos, Solitons Fractals*, **41** (2009), 1773–1783. https://doi.org/10.1016/j.chaos.2008.07.031

27. R. Parvaz, Y. K. Yengejeh, Y. Behroo, A new 4D chaos system with an encryption algorithm for color and grayscale images, *Int. J. Bifurcation Chaos*, **32** (2022), 2250214. https://doi.org/10.1142/S0218127422502145

28. X. Z. Yang, H. Tian, F. Wang, J. P. Ni, J. Q. Zhang, J. J. Jia, Bounded-chaos Duffing detector for weak occlusion signals in laser light screen system, *Opt. Lasers Eng.*, **203** (2026), 109824. https://doi.org/10.1016/j.optlaseng.2026.109824

29. M. Vogl, Chaos measure dynamics in a multifactor model for financial market predictions, *Commun. Nonlinear Sci. Numer. Simul.*, **130** (2024), 107760. https://doi.org/10.1016/j.cnsns.2023.107760

30. L. H. Gong, H. X. Luo, R. Q. Wu, N. R. Zhou, New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG, *Physica A: Stat. Mech. Appl.*, **591** (2022), 126793. https://doi.org/10.1016/j.physa.2021.126793

31. Z. Wan, N. X. Xiong, N. Ghani, A. Vasilakos, L. Zhou, Adaptive unequal protection for wireless video transmission over IEEE 802.11e networks, *Multimedia Tools Appl.*, **72** (2014), 541–571. https://doi.org/10.1007/s11042-013-1378-z

32. W. Y. Liang, L. M. Zhang, Z. B. Yang, T. T. Yu, J. J. Li, X. L. Li, Image encryption algorithm based on hyperchaotic system and dynamic DNA encoding, *Phys. Scr.*, **98** (2023), 115215. https://doi.org/10.1088/1402-4896/acfc71

33. G. R. Chen, Y. B. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons Fractals*, **21** (2004), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

34. S. A. Mehdi, Image encryption algorithm based on a novel 4D chaotic system, *Int. J. Inf. Secur. Privacy*, **15** (2021), 118–131. https://doi.org/10.4018/IJISP.2021100107

35. L. M. Wu, Z. J. Tian, W. Chen, Color image encryption scheme based on 5D fractional-order complex chaotic system and eight-base DNA cubes, *Expert Syst. Appl.*, **299** (2026), 129950. https://doi.org/10.1016/j.eswa.2025.129950

36. A. Panwar, G. Biban, R. Chugh, A. Tassaddiq, R. Alharbi, An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images, *Heliyon*, **10** (2024), e31618. https://doi.org/10.1016/j.heliyon.2024.e31618

37. X. J. Tong, L. M. Cheng, Y. H. Wang, Color image encryption algorithm based on a novel five-dimensional chaotic system, *Phys. Scr.*, **100** (2025), 095202. https://doi.org/10.1088/1402-4896/adfca7

38. M. X. Gong, X. L. Chai, Y. Lu, Y. S. Zhang, Exploiting four-dimensional chaotic systems with dissipation and optimized logical operations for secure image compression and encryption, *IEEE Trans. Circuits Syst. Video Technol.*, **34** (2024), 7628–7642. https://doi.org/10.1109/TCSVT.2024.3375868

39. W. Song, C. Fu, Y. Zheng, Y. F. Zhang, J. X. Chen, P. P. Wang, Batch image encryption using cross image permutation and diffusion, *J. Inf. Secur. Appl.*, **80** (2024), 103686. https://doi.org/10.1016/j.jisa.2023.103686

40. B. Y. Liu, W. Song, M. Y. Zheng, C. Fu, J. X. Chen, X. W. Wang, Semantically enhanced selective image encryption scheme with parallel computing, *Expert Syst. Appl.*, **279** (2025), 127404. https://doi.org/10.1016/j.eswa.2025.127404

41. F. Yu, X. Q. Wang, Y. Xiao, Y. He, W. Yao, S. Cai, et al., Extreme multistability in discrete memristive neuron maps and implications for dual-field applications, *Integration*, **109** (2026), 102688. https://doi.org/10.1016/j.vlsi.2026.102688

42. Q. Wang, H. W. Sang, P. Wang, X. Yu, Z. Y. Yang, A novel 4D chaotic system coupling with dual-memristors and application in image encryption, *Sci. Rep.*, **14** (2024), 29615. https://doi.org/10.1038/s41598-024-80445-8

43. A. A. Elsadany, S. Hussein, A. Al-Khedhairi, A. Elsonbaty, On dynamics of 4-D blinking chaotic system and voice encryption application, *Alexandria Eng. J.*, **70** (2023), 701–718. https://doi.org/10.1016/j.aej.2023.03.024

AIMS Press