scientific reports

OPEN

Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators

Ying Niu[1], Hangyu Zhou[2] & Xuncai Zhang[2]✉

To enhance the security of image data transmission, and address the weaknesses of existing image encryption schemes based on chaotic systems, particularly concerning resistance to differential attacks and the unstable performance of chaotic systems, this article introduces an improved four-dimensional chaotic system and integrates evolutionary operators to propose an image encryption scheme. Firstly, a method for generating pseudo-random sequences associated with the plaintext is designed. The change rate of the ciphertext pixel value exceeds 0.9967 after a slight modification of the plaintext pixel value, significantly improving the plaintext sensitivity and the scheme's ability to resist selected plaintext attacks. Secondly, an individual rearrangement operation is introduced to achieve bit-level scrambling, and pixel-level scrambling is achieved by selection strategy. Subsequently, crossover and mutation operations are incorporated into image encryption. To reflect the randomness of the pairing, we adopt the pseudo-random sequence generated by the chaotic system to control the crossover and mutation operators, and a diffusion operation is performed on selected pixel pairs. Finally, ciphertext feedback is applied. Experimental results and performance analysis demonstrate that the proposed scheme not only enhances the security of encrypted images but also effectively resists noise and cropping attacks. This method effectively meets the high-security requirements of images in network transmission and provides new ideas for further research in the field of image encryption.

Images, as an essential form of multimedia data, encompass a wide range of sensitive information, including personal privacy, business secrets, and medical images. With the continuous development of communication technology and the widespread use of information transmission, ensuring the security and confidentiality of image information has become particularly urgent. Image encryption, as a crucial technology in the field of information security, is essential to protect the safe transmission of such vital information. Due to the characteristics of images, such as massive data volume, strong correlation, high redundancy, and distinctive recognition features, traditional text encryption methods like AES and DES prove to be slow and ineffective in encrypting and decrypting images. These methods can no longer meet the encryption needs of large-capacity image data[1]. Consequently, researchers have begun exploring new methods for image encryption. Common approaches include image encryption schemes based on techniques such as wavelet transform encryption[2–4], invertible transform[5–7], deep learning[8–10], quantum encryption[11–13], and others. Chaotic systems have garnered significant attention in the field of information security due to their nonlinear dynamics and high sensitivity to initial conditions. In image encryption schemes, the integration of chaotic systems enhances unpredictability, thereby improving image security by introducing a certain degree of randomness. For instance, Wang[14] proposed an image encryption scheme based on logistic map. This approach first utilizes wavelet transform to focus on the key information features of the image in the low-frequency part, subsequently encrypting the low-frequency information through the random sequence generated by logistic map. Mondal[15] proposed an image encryption method based on two-dimensional Tent map, combined with meta-cellular automata. The random sequence generated by the Tent map serves as a cipher stream to control the state of each neighborhood cell and transforms each pixel value, achieving the encryption of the plaintext image. Although low-dimensional chaotic systems offer advantages in terms of simplicity, ease of implementation, and understanding, they have limitations in

[1]School of Architecture Environment Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China. [2]School of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China. ✉email: zhangxuncai@pku.edu.cn

generating random sequences. These limitations may result in relatively low randomness and susceptibility to statistical analysis attacks.

To ensure the security of encrypted images and prevent malicious theft, some researchers have begun utilizing high-dimensional chaotic systems to design image encryption methods, addressing the limitations of low-dimensional chaotic systems. For example, Ma[16] employed the three-dimensional Chen chaotic system and the Fisher-Yates permutation scheme to encrypt color images. In this approach, the sequence generated by the three-dimensional chaotic system serves as the cipher stream for the Fisher–Yates permutation scheme, disrupting the pixel positions. Subsequently, a new set of initial values is used to generate a new sequence through the chaotic system, ultimately operating with the plaintext pixel to alter its value. Three-dimensional chaotic systems provide higher security compared to their one-dimensional and two-dimensional systems, exhibiting more complex dynamical behavior, that enhances the system's unpredictability against potential attackers. Three-dimensional chaotic systems offer relatively robust protection with somewhat controllable computational complexity, making them suitable for moderately complex image encryption applications. However, although relatively secure, three-dimensional chaotic systems have a reasonably limited keyspace, which may need improvement in highly security-demanding scenarios. To overcome this deficiency, Zhao[17] proposed a new image encryption method using a four-dimensional chaotic system combined with DNA coding. Experimental analyses demonstrate that the method not only achieves a substantial keyspace but also enhances security performance. Four-dimensional chaotic systems provide a larger keyspace than three-dimensional systems, heightening the difficulty of attacks and improving encryption security. As dimensionality increases, the dynamical behavior becomes more intricate, further strengthening the encryption. Four-dimensional chaotic systems are better suited for scenarios with higher security requirements than three-dimensional systems. They can provide richer dynamics, increasing the difficulty for attackers to predict the system's state. Some scholars have explored five or higher-dimensional chaotic systems[18–20], where computational complexity grows exponentially with dimensionality. This may lead to a significant reduction in the real-time performance of image encryption in resource-constrained environments, such as embedded systems or mobile devices. Parameter tuning and optimization for high-dimensional chaotic systems are relatively more complex. Finding the right combination of parameters to ensure system stability and good cryptographic performance may require more time and computational resources. Additionally, higher-dimensional chaotic systems may be more demanding on hardware resources, which may limit applications on some resource-constrained devices. In practical applications of high-dimensional chaotic systems, these drawbacks and challenges should be comprehensively considered, balancing encryption security, computational efficiency, and hardware resource requirements.

As researchers delve deeper, they discover that single or structurally simple chaotic maps may have the potential to be less accurate and less secure. Therefore, image encryption methods are becoming increasingly diversified, typically employing not just one method but a combination of methods. Zhang[21] utilized Latin square and S-box to implement pixel substitution and replacement, respectively, aiming to enhance the resistance of the encryption system against attacks. Wang[22] employed a combination of dynamic parity row check and Z-transform to completely disrupt pixel positions. Additionally, the chunking method was used to diffuse different chunks of the ciphertext, thereby improving the robustness of the encryption system. Zhu[23] applied chunk scrambling and an optimized artificial fish swarm scheme to double scramble pixel positions. Furthermore, the DNA coding technique was employed to diffuse each pixel value, enhancing overall security. Based on this, this article extends the traditional three-dimensional chaotic system into a new four-dimensional chaotic system by introducing new state variables based on the three-dimensional Lorenz chaotic system. Simultaneously, incorporating evolutionary operators and employing image encryption with the assistance of evolutionary operators such as selection, recombination, and mutation further enhances the effectiveness of image encryption. This fusion approach introduces a novel idea and method for research in the field of image encryption. To strengthen the cryptosystem and provide higher security, this work fully utilizes the properties of pseudo-randomness and the traversal of evolutionary operators and chaos theory. This comprehensive approach addresses the security threats and inefficiencies encountered in image encryption.

The main contributions of this article are as follows:

(1) Proposing a new four-dimensional chaotic system by introducing new state variables and increasing the dimensionality of the system. This expansion results in a larger state space, offering increased degrees of freedom. Consequently, the system exhibits more complex trajectories with richer dynamical behavior.
(2) Analyzing the maximum Lyapunov exponent with one and two parameters, sensitivity, and NIST test of the new four-dimensional chaotic system. The chaotic system demonstrates a high Lyapunov exponent and sensitivity to the initial key. The generated chaotic sequences exhibit high complexity and randomness, thereby enhancing the security of image encryption schemes.
(3) Applying evolutionary operators to image encryption, utilizing sequences generated by the four-dimensional chaotic system to execute selection, mutation, and recombination operations on pixels. The approach facilitates highly random pixel value changes. Notably, the recombination operation involves eight rules, increasing the difficulty of cracking and improving the overall security of the encryption scheme.

The remaining sections of this article are outlined as follows: "Theoretical foundations" section introduces the concepts of three-dimensional Lorenz chaotic system and evolutionary operators; "Hyperchaotic system" section provides a detailed presentation of the proposed four-dimensional chaotic system and analyses its key performance metrics; "Image encryption scheme" section describes the detailed steps and procedures of the encryption scheme; "Simulation experiment results" section presents the experimental results and multiple security analyses; and "Conclusions" section concludes the article.

Theoretical foundations

Chaotic system

A chaotic system is a deterministic system characterized by seemingly random, irregular motions with attributes of uncertainty, irreducibility, and unpredictability. To strike a balance between the complexity and efficiency of chaotic systems, the Lorenz chaotic system, proposed by the meteorologist Edward Lorenz in his study of meteorology[24], is a three-dimensional nonlinear dynamical system that describes a convective phenomenon in which air or liquid forms a complex vortex structure in a confined space. This system consists of three coupled differential equations with expressions, as shown in Eq. (1).

$$\begin{cases} \dot{x} = \sigma\left(y - x\right) \\ \dot{y} = \gamma x - y - xz \\ \dot{z} = xy - bz \end{cases}, \tag{1}$$

where x, y, z are the state variables of the system, and σ, γ, b are the system's parameters. When the parameters are set to $\sigma = 10$, $\gamma = 28$, $b = 8/3$, with initial values of (1, 1, 1), the system exhibits classical chaotic phenomena, including extreme sensitivity to initial conditions and randomness. In a chaotic state, the system's trajectory displays complex and seemingly irregular motion, as depicted by its Lyapunov exponents in Fig. 1, which are (0.9021, − 0.0001, − 14.5686).

Evolutionary strategy

Evolutionary strategy[25] is an evolutionary computational method designed to tackle parameter optimization problems. The method draws inspiration from natural biological evolution and was first proposed by H.P. Schwefel of Germany in 1963. Evolutionary strategies find wide applicability across various optimization domains, including continuous, discrete, unconstrained, and constrained combinatorial search spaces, as well as hybrid search spaces. The core idea involves iteratively evolving a population of individuals containing candidate solutions through three key operators: selection, recombination, and mutation, to progressively refine solutions. The main search loop of the evolutionary strategy is illustrated in Fig. 2.

The evolutionary strategy comprises the following key steps:

(1) *Population initialization* A group of individuals is randomly generated, with each representing a potential solution to the problem. The parameters of these individuals are chosen randomly.
(2) *Fitness evaluation* Apply a problem-specific fitness function to each individual, to assess their performance in solving the problem. The fitness function quantifies the quality of individuals.
(3) *Recombination* Involves the combination of some features or parameters of single or multiple individuals to generate new individuals.
(4) *Mutation* Refers to the random or systematic perturbation of individual information to introduce new information and thus increase the diversity of the population.
(5) *Selection* Selection is based on the individual's adaptation, and the better-adapted individuals are retained through recombination and mutation operations. This mimics the process of natural selection, wherein individuals with superior adaptations have a greater likelihood of survival and reproduction.
(6) *Repeat iterations and algorithm termination* The above steps are repeated iterations, and the population evolves, with the better-adapted individuals being retained and continuously optimized to approach the optimal solution to the problem. The algorithm terminates when the maximum number of iterations, the adaptation threshold, or other specified conditions is reached; if the termination conditions are not reached, the algorithm returns to step 3.

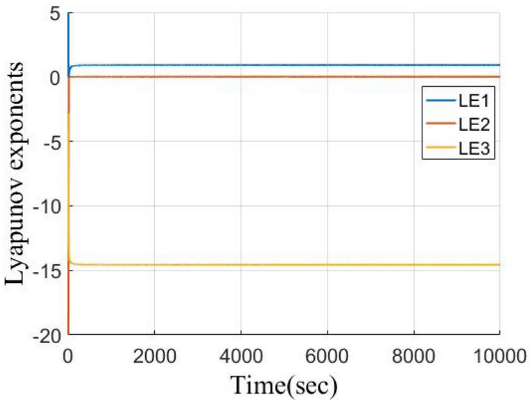


Figure 1. Lyapunov exponents of three-dimensional Lorenz chaotic system.

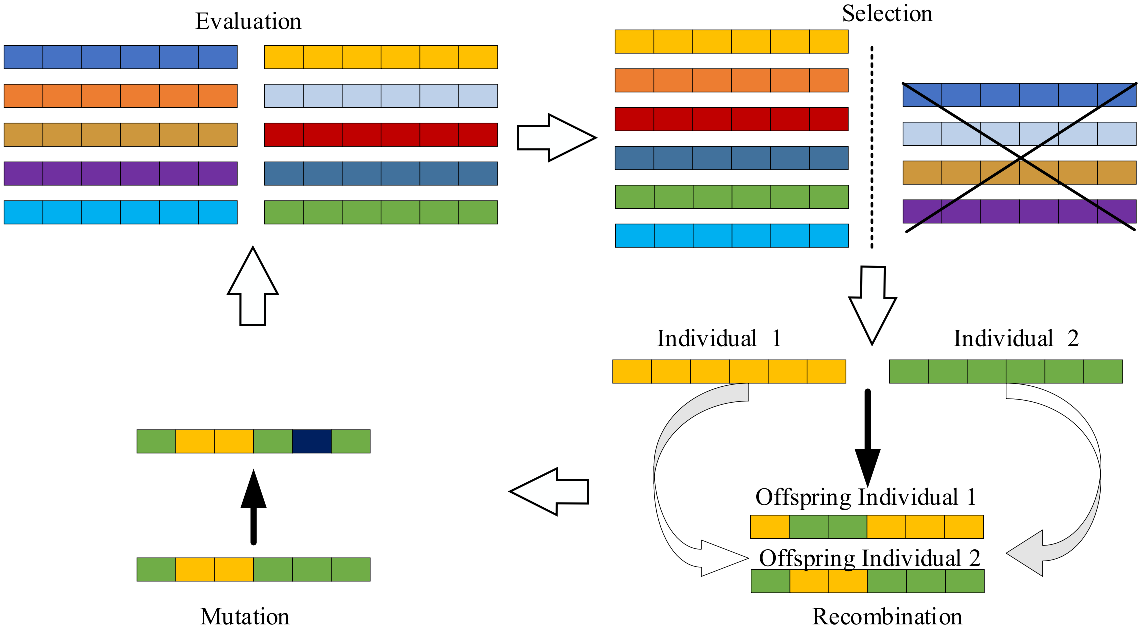


Figure 2. The main search loop of the evolutionary strategy.

Evolutionary strategies have strong local search ability and perform well in dealing with continuous optimization problems, enabling them to converge to the optimal solution quickly. Therefore, they are widely used in engineering optimization, machine learning, and computer simulation.

However, in the image encryption problem, although it is not a traditional optimization problem, the introduction of evolutionary operators aims to apply the selection, recombination, and mutation operations of biological evolution to image pixels. Encryption is achieved through pixel scrambling and diffusion via pixel selection, mutation of pixel values (expressed in binary form), and inter-pixel reorganization. Despite being applied to different domains, evolutionary operators demonstrate their flexibility and adaptability, successfully transitioning to the solution of the image encryption problem. Here, we define recombination operations in evolutionary operators for better application to image encryption, including:

(1) *Individual rearrangement* This refers to the manipulation of the interior of a single individual to generate a new one. This can involve restructuring, parameter changes, etc.
(2) *Crossover* It refers to selecting two or more individuals to generate new offspring by crossing over their parameters or structures. This emphasizes manipulation across individuals. Through crossover, evolutionary operators enable more flexible manipulation of pixels and produce a more comprehensive image encryption effect.

Hyperchaotic system

Proposed four-dimensional hyperchaotic system

As a nonlinear dynamical system, the three-dimensional Lorenz chaotic system has been widely utilized in image encryption due to its strong sensitivity to initial values and parameters, as well as its unpredictable trajectories. To further enhance the pseudo-randomness of the generated sequences, we introduce a new state variable, denoted as w, into the three-dimensional Lorenz system and couple it with the third dimension of the system to construct a four-dimensional hyperchaotic system. The state variable w interconnects the individual state variables and system parameters in a chaotic system to enhance the disorder and sensitivity of the chaotic system, whose expression is shown in Eq. (2).

$$\begin{cases} \dot{x} = a\left(y - x\right) + z \\ \dot{y} = bx - cy - xz \\ \dot{z} = xy - dz + ew \\ \quad \dot{w} = fx + y \end{cases}, \tag{2}$$

where x, y, z, and w represent the state variables of system, and a, b, c, d, e and f are the parameters controlling the chaotic behavior of the system. After parameter tuning, when the system parameters are set to $a = 34$, $b = 28$, $c = 2.6$, $d = 4$, $e = 1.8$, and $f = 2.4$, the system enters a hyperchaotic state with improved chaotic behavior. Given the initial values $x_0 = 0.1$, $y_0 = 0.2$, $z_0 = 0.2$, and $w_0 = 0.2$, the phase diagram of the hyperchaotic system is depicted in Fig. 3.

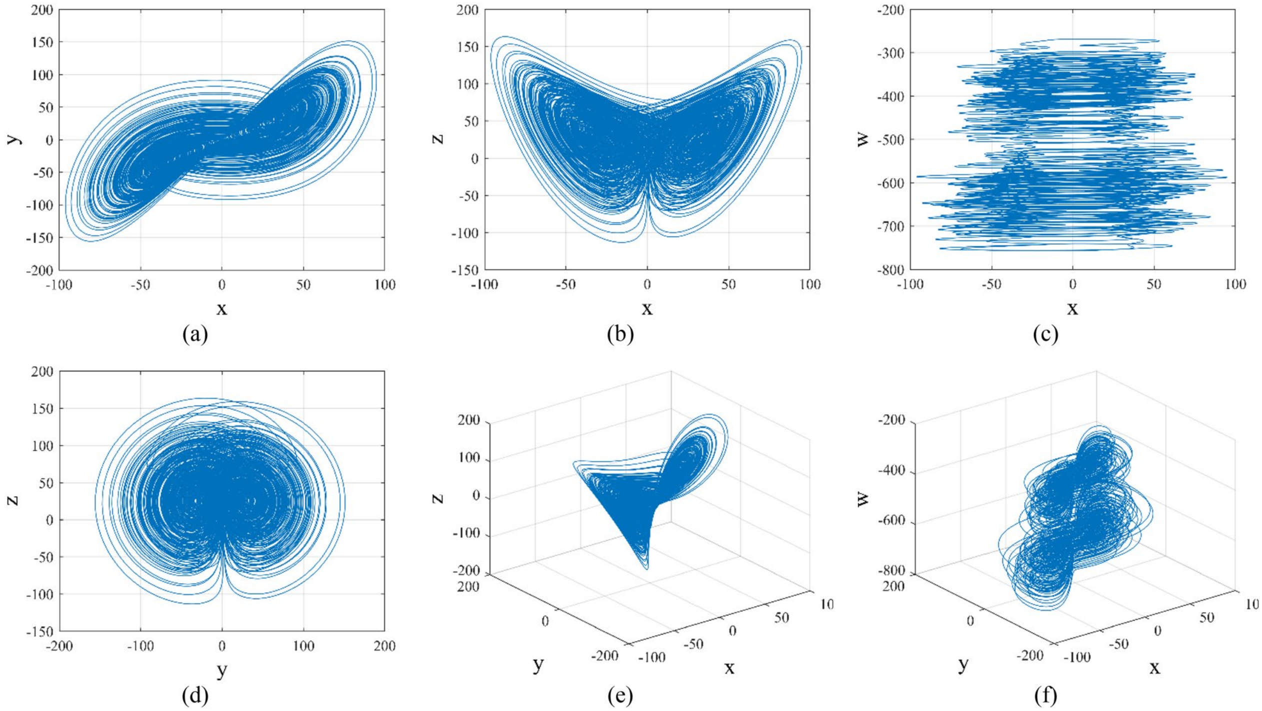


Figure 3. Phase diagram of hyperchaotic system: (**a**) *x*–*y* plane, (**b**) *x*–*z* plane; (**c**) *x*–*w* plane; (**d**) *y*–*z* plane; (**e**) *x*–*y*–*z* plane; (**f**) *y*–*z*–*w* plane.

Lyapunov exponent

The Lyapunov exponent quantitatively measures the dynamic properties of a system by assessing the rate of orbital mean dispersion. In a four-dimensional chaotic system, there are four Lyapunov exponents, with their sum being required to be less than zero, including at least two positive exponents[26]. Each parameter in the chaotic system has a distinct range, leading to different chaotic states and Lyapunov exponents. The Lyapunov exponents of the proposed four-dimensional chaotic system are depicted in Fig. 4, indicating LE1 = 6.6892, LE2 = 0.0189, LE3 = 0.0143, and LE4 = -47.3166. Since the sum is less than zero and there are three positive Lyapunov exponents, it can be inferred that the system enters a hyperchaotic state under these conditions.

The fractal dimension of the four-dimensional chaotic system, denoted as D_L, can be computed using Eq. (3).

$$D_L = j + \frac{\sum_{i=1}^{j} LE_i}{|LE_{j+1}|} = 3 + \frac{LE_1 + LE_2 + LE_3}{|LE_4|} = 3.1421, \tag{3}$$

where $j + 1$ represents the dimension of the chaotic system. If the fractal dimension falls within the range of $3 < D_L < 4$, it signifies a hyperchaotic system[27]. Upon calculation, the proposed system's fractal dimension satisfies $3 < D_L < 4$, affirming its hyperchaotic nature.

The single-parameter Lyapunov exponent diagram is employed to identify local maxima of a control parameter in a chaotic system, facilitating the visualization of the system's transition from cyclic to chaotic behavior. By

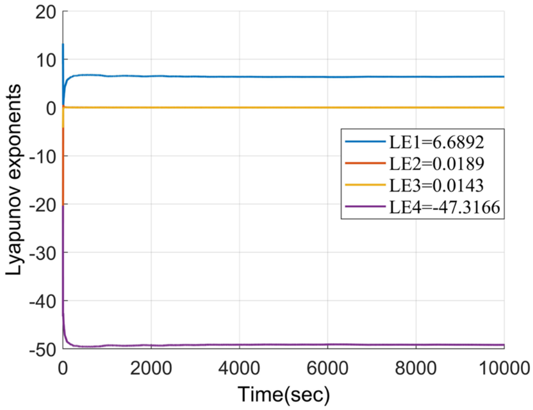


Figure 4. Lyapunov exponents of the improved hyperchaotic system.

leveraging these maxima, optimal parameter values can be selected to achieve an optimal chaotic state. Figure 5 illustrates the Lyapunov exponent for various parameters, showcasing the chaotic behavior induced by each parameter within a specified range. This analysis underscores the chaotic properties exhibited by the proposed four-dimensional chaotic system across the parameter spectrum, thereby enhancing the unpredictability of the generated pseudo-random sequences and expanding the keyspace.

The sequences generated by the three-dimensional Lorenz chaotic system often exhibit weak broadband characteristics, limited randomness, and monotonicity in localized regions[28]. To address these shortcomings, researchers have endeavored to enhance the three-dimensional Lorenz chaotic system for application in image encryption[8,29,30]. Table 1 compares the proposed four-dimensional chaotic system in this study with existing counterparts. Notably, the proposed system exhibits three positive Lyapunov exponents, whereas other existing systems feature only two. Additionally, the maximum Lyapunov exponent of the proposed system surpasses that of the others, indicating a more complex and nonlinear structure. Furthermore, the inclusion of multiple parameters in the proposed system results in a larger keyspace, bolstering image encryption security compared to other systems.

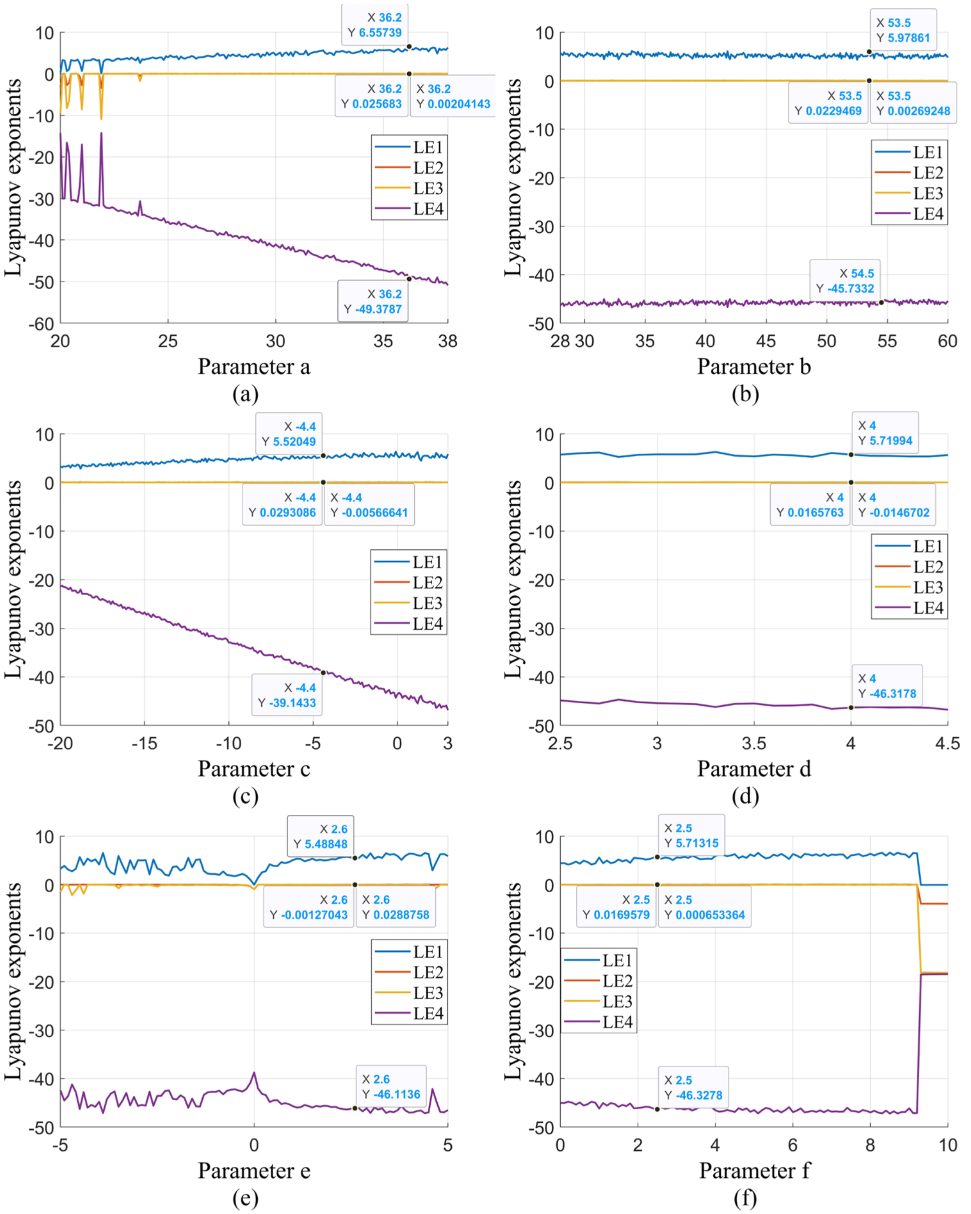


Figure 5. Single-parameter Lyapunov exponents: (**a**) parameter $a\in[20, 38]$; (**b**) parameter $b\in[28, 60]$; (**c**) parameter $c\in[-20, 3]$; (**d**) parameter $d\in[2.5, 4.5]$; (**e**) parameter $e\in[-5, 5]$; (**f**) parameter $f\in[0, 10]$.

Chaotic systems	LE1	LE2	LE3	LE4	Number of parameters
Our	6.6892	0.0189	0.0143	− 47.3166	6
[29]	3.3488	0.1399	0	− 17.1252	6
[30]	0.2000	0.3000	0	− 7.5600	4
[8]	0.3300	0.1586	0	− 15.1752	4

Table 1. Comparison of four-dimensional chaotic systems.

Maximum Lyapunov exponent for two-parameter

Chaotic systems are nonlinear dynamical systems characterized by intricate behavior and high sensitivity to system parameters. Even minor alterations in these parameters can significantly influence the system's trajectory. The two-parameter maximum Lyapunov exponent diagram offers insight into the dynamic behavior of chaotic systems. By setting initial values at (0.1, 0.2, 0.2, 0.2), the impact of parameters $a \in [20, 37]$ and $f \in [0, 10]$ on the system's behavior is investigated. Figure 6 illustrates the two-parameter maximum Lyapunov exponent diagram and its three-dimensional representation, with distinct colors denoting different Lyapunov exponents: darker shades (red) indicating larger exponents, and lighter shades (blue) indicating smaller ones.

Sensitivity analysis

When varying initial values within a chaotic system, different sequences are generated, underscoring the system's sensitivity to these values. Minor adjustments to initial values lead to distinct chaotic sequences, highlighting the system's high sensitivity. In this section, slight modifications are made to the initial values, with four sets of tests conducted using x_0 (0.1), y_0 (0.2), z_0 (0.2), w_0 (0.2), and $x_0 + 10^{-14}$, $y_0 + 10^{-14}$, $z_0 + 10^{-14}$, $w_0 + 10^{-14}$. The outcomes of these tests are depicted in Fig. 7. Notably, even minute changes in individual initial values yield markedly different sequences, underscoring the pronounced sensitivity of the proposed four-dimensional chaotic system to initial conditions.

Dissipative and equilibrium stability analysis

The total energy of the chaotic system diminishes over time, while the phase space contracts as the system evolves. This characteristic, known as the dissipative nature of a chaotic system[31], is defined by Eqs. (4) and (5):

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} < 0, \tag{4}$$

$$\frac{dV}{dt} = e^{\nabla V}, \tag{5}$$

where t represents time, and V denotes the dissipation volume. By substituting the system parameters, $a = 34$, $b = 28$, $c = 2.6$, $d = 4$, $e = 1.8$, and $f = 2.4$ into Eq. (4), we obtain $\nabla V = -a - c - d = -40.6$, indicating that $\nabla V < 0$. Therefore, at this juncture, the chaotic system is dissipative. As time progresses infinitely, the chaotic system's phase space eventually converges to a point, forming an attraction domain. Modifying one aspect of the chaotic system to 0, as depicted in Eq. (6):

$$\begin{cases} a(y - x) + z = 0 \\ bx - cy - xz = 0 \\ xy - dz + ew = 0 \\ fx + y = 0 \end{cases}. \tag{6}$$

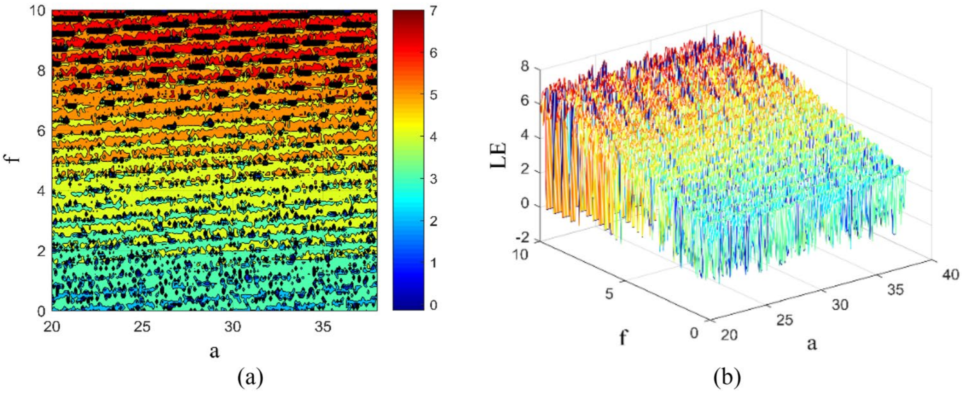
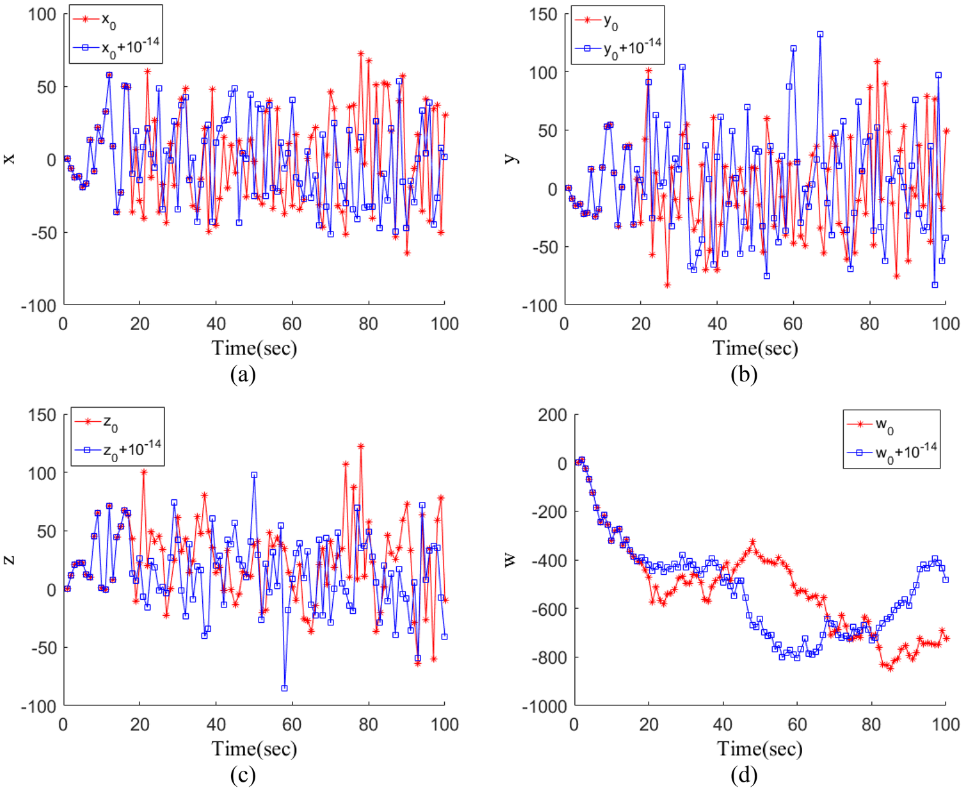


Figure 6. Two-parameter Lyapunov exponents: (**a**) maximum Lyapunov exponent diagram in (*a*–*f*) plane; (**b**) three-dimensional visualization diagram in (*a*–*f*) plane.



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

Figure 7. Initial value sensitivity test: (**a**) $x_0 + 10^{-14}$; (**b**) $y_0 + 10^{-14}$; (**c**) $z_0 + 10^{-14}$; (**d**) $w_0 + 10^{-14}$.

After computation, the chaotic system yields two equilibrium points: $E_1 = (0, 0, 0, 0)$ and $E_2 = (0.2962, -0.7109, 34.2400, 76.2059)$. The chaotic system's Jacobian matrix is shown in Eq. (7):

$$J = \begin{bmatrix} -a & a & 1 & 0 \\ b-z & -c & -x & 0 \\ y & x & -d & e \\ f & 1 & 0 & 0 \end{bmatrix}. \tag{7}$$

With control parameters $a = 34$, $b = 28$, $c = 2.6$, $d = 4$, $e = 1.8$, and $f = 2.4$, the eigenvalues of each equilibrium point are computed using the Jacobian matrix. For E_1, the four eigenvalues are $\lambda_1 = -52.9183$, $\lambda_2 = 16.3249$, $\lambda_3 = -0.0179$, $\lambda_4 = -3.9887$, while for E_2, the corresponding eigenvalues are $\lambda_1 = -24.1106$, $\lambda_2 = -12.4377$, $\lambda_3 = -4.1019$, and $\lambda_4 = 0.0501$.

According to the Routh-Hurwitz criterion[32], the coefficients of the eigen equations must all be negative for equilibrium points to be stable. However, not all coefficients of the eigenvalues for both equilibrium points are negative, indicating that they are unstable.

NIST test

The randomness of the sequence can be quantitatively assessed using the NIST randomization test[33]. In this experiment, the NIST test was conducted on four sequences generated by the four-dimensional chaotic system. Prior to the test, these sequences were converted into binary sequences. If $P > 0.01$, it indicates that the sequence is sufficiently random to pass the NIST test.

Table 2 displays the test results, indicating that the P values for all test items are highly significant, surpassing the significance level of 0.01. This verifies the randomness of the chaotic sequence, ensuring the encryption's security.

Image encryption scheme

The generation of initial parameters for the chaotic system involves combining the provided external key with the plaintext image to generate pseudo-random sequences associated with the plaintext. Subsequently, the plaintext undergoes scrambling through individual rearrangement and selection operations, resulting in double scrambling at both the bit-level and pixel-level. Additionally, the image is subjected to crossover and mutation operations as part of the image diffusion process, aiming to obscure the original image. The inclusion of pseudo-random sequences in the ciphertext feedback further aids in the diffusion process. The detailed encryption flowchart is depicted in Fig. 8.

NIST-Nnme	*P* value				Result
	x	*y*	*z*	*w*	
Frequency	0.976060	0.213309	0.739918	0.082177	Pass
Block frequency	0.407091	0.082177	0.082177	0.671779	Pass
Cumulative sums	0.602458	0.804337	0.671779	0.534146	Pass
Runs	0.671779	0.213309	0.949602	0.213309	Pass
Longest run	0.066882	0.253551	0.739918	0.213309	Pass
Rank	0.213309	0.911413	0.407091	0.066882	Pass
FFT	0.862344	0.949602	0.100508	0.299251	Pass
Nonperiodic template	0.911413	0.862344	0.949602	0.949602	Pass
Overlapping template	0.739918	0.299251	0.299251	0.534146	Pass
Universal statistical	0.468595	0.534146	0.213309	0.468595	Pass
Approximate entropy	0.739918	0.122325	0.468595	0.862344	Pass
Random excursions	0.122325	0.964295	0.739918	0.350485	Pass
Random excursions variant	0.122325	0.834308	0.534146	0.213309	Pass
Serial	0.976060	0.299251	0.862344	0.739918	Pass
Linear complexity	0.602458	0.407091	0.534146	0.100508	Pass

Table 2. NIST random test results.

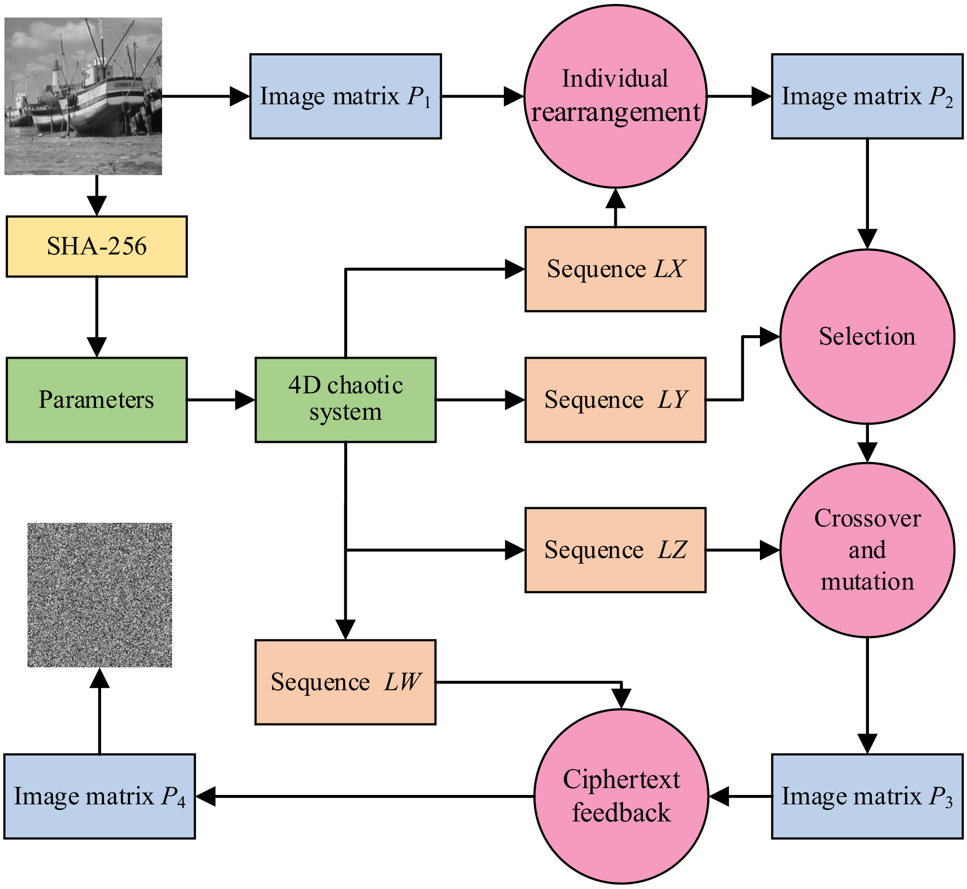


Figure 8. Flowchart of encryption scheme.

Key generation

To ensure that different keys are used for different images, we associate the key with the plaintext and use the plaintext image pixel values and hash values to update the key. Using the SHA-256 scheme, a 256-bit binary hash value (named K) is obtained by performing encryption operations on the plaintext image. Using this operation to perform key updates in every encrypt round. K is divided into 32 groups of 32 bytes by byte, each represented as K_1, K_2, …, K_{32}. According to Eqs. (8)–(10), the updated set of keys is computed to get the updated set of keys for the chaotic system and the initial values.

$$\begin{cases} Q_1 = \frac{4}{N}\sum\limits_{i=1}^{\frac{N}{4}} q_i - \left[\frac{4}{N}\sum\limits_{i=1}^{\frac{N}{4}} q_i\right] \\ Q_2 = \frac{4}{N}\sum\limits_{i=\frac{N}{4}+1}^{\frac{N}{2}} q_i - \left[\frac{4}{N}\sum\limits_{i=\frac{N}{4}+1}^{\frac{N}{2}} q_i\right] \\ Q_3 = \frac{4}{N}\sum\limits_{i=\frac{N}{2}+1}^{\frac{3N}{4}} q_i - \left[\frac{4}{N}\sum\limits_{i=\frac{N}{2}+1}^{\frac{3N}{4}} q_i\right] \\ Q_4 = \frac{4}{N}\sum\limits_{i=\frac{3N}{4}+1}^{N} q_i - \left[\frac{4}{N}\sum\limits_{i=\frac{3N}{4}+1}^{N} q_i\right] \end{cases}, \tag{8}$$

$$\begin{cases} \alpha = \frac{(K_1 \oplus K_2 \oplus K_3 \oplus K_4) + K_5 + K_6 + K_7 + K_8}{256*5} \\ \beta = \frac{(K_9 \oplus K_{10} \oplus K_{11} \oplus K_{12}) + K_{13} + K_{14} + K_{15} + K_{16}}{256*5} \\ \gamma = \frac{(K_{17} \oplus K_{18} \oplus K_{19} \oplus K_{20}) + K_{21} + K_{22} + K_{23} + K_{24}}{256*5} \\ \omega = \frac{(K_{25} \oplus K_{26} \oplus K_{27} \oplus K_{28}) + K_{29} + K_{30} + K_{31} + K_{32}}{256*5} \end{cases}, \tag{9}$$

$$\begin{cases} x_0 = mod(Q_1 + Q_2 - \alpha, 1) + x_0' \\ y_0 = mod(Q_2 + Q_3 - \beta, 1) + y_0' \\ z_0 = mod(Q_3 + Q_4 - \gamma, 1) + z_0' \\ \omega_0 = mod(Q_4 + Q_1 - \omega, 1) + \omega_0' \end{cases}, \tag{10}$$

where $[x]$ is a rounding function, q_i is determined by the average of the pixel values in the ith column of the plaintext image, N is the number of columns in the plaintext image, and x_0', y_0', z_0', ω_0' are given values.

Selection operation

In evolutionary strategy, the selection operation refers to the process of selecting individuals from the population based on their adaptability. The goal of the selection operation is to maintain or improve the overall quality of the population over consecutive generations, guiding the evolutionary process towards an optimal solution. In image encryption methods, to enhance the confusion effect, we need to introduce more randomness. Therefore, we have improved the selection operation to better adapt to the requirements of image encryption. In this article, we utilize the pseudo-randomness of chaotic sequences to achieve individual selection, aiming to achieve better pixel scrambling.

Given an image P of size $M \times N$, for traversing all the pixels, the selection in this article involves random traversal, differing from the selection in the optimization scheme. The randomness of selection is achieved here with the help of chaotic sequences due to their easy generation, strong sensitivity to initial conditions, and complete reproducibility.

To achieve this, rearrange the generated pseudo-random sequence in ascending order to obtain an ordered sequence. Determine the location of each element in the ordered sequence and its position in the original sequence. Then, form a new sequence from these position sequences in order, i.e., the position index sequence $Index = \{Index_1, Index_2, Index_3, \ldots Index_{M \times N}\}$. Based on the values of two adjacent pixels in the position index sequence, select the corresponding pixel positions in the image P according to Eq. (11) to obtain the pixel pairs $Pixel_A$ and $Pixel_B$. Figure 9 shows a schematic diagram of the selection strategy, where Fig. 9a shows the chaotic sequence, the ascending sequence, and the index sequence of length 4 × 4, Fig. 9b shows the pixel position pair representation corresponding to the 4 × 4 matrix, and Fig. 9c shows the 4 × 4 pixel matrix and its pixel pair selection schematic, where P is the plaintext image matrix. The selection formula (11) is described as follows:

$$\begin{cases} Pixel_A = P\big(floor((Index_i - 1)/N) + 1, mod(Index_i - 1, N) + 1\big) \\ Pixel_B = P\big(floor((Index_{i+1} - 1)/N) + 1, mod(Index_{i+1} - 1, N) + 1\big) \end{cases}, \tag{11}$$

where $P(\cdot)$ is the plaintext pixel, $Pixel_{A,}$ and $Pixel_B$ are the selected pixel pairs, $mod(\cdot)$ is the modulo operation, $floor(\cdot)$ is the rounding operation, i is odd, and $i < M \times N$.

Crossover and mutation operation

In this article, crossover and mutation are utilized to alter the bit sequence, enhancing the robustness and security of encryption. Given two parents and a random number, two offspring individuals are obtained after crossover. Here, the individuals are the pixels in the image, each represented by 256 grey levels with pixel values in an 8-bit binary. Following the previous selection strategy, for the selected pixel pairs noted as $Pixel_A = a_8a_7a_6a_5a_4a_3a_2a_1$

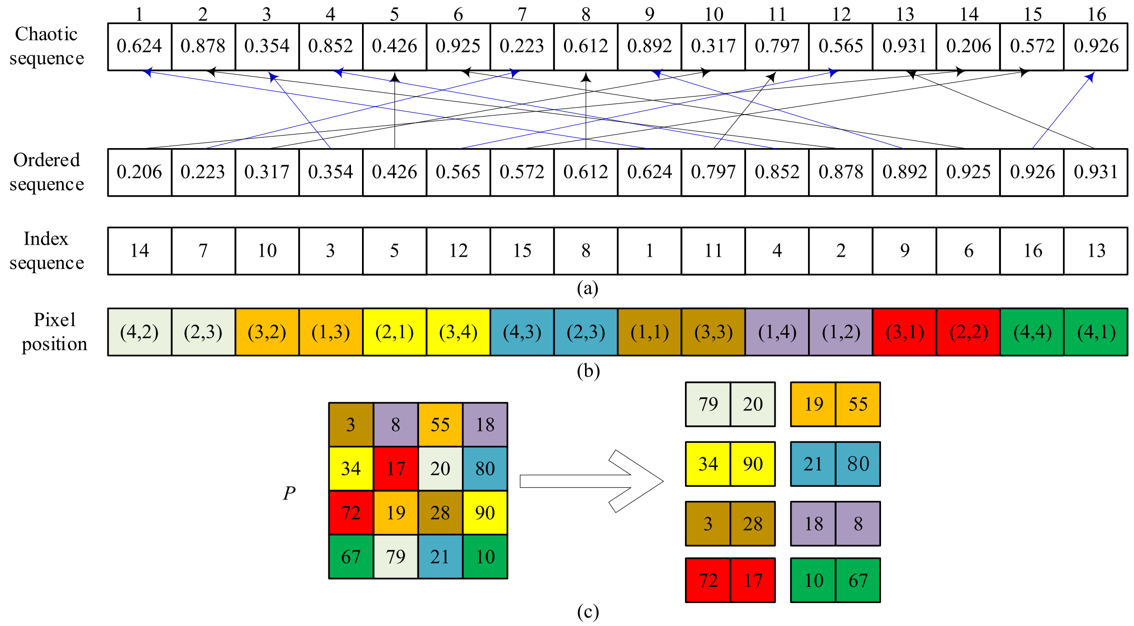


Figure 9. Schematic diagram of selection strategy: (**a**) the chaotic sequence, the ascending sequence, and the index sequence; (**b**) shows the pixel position pair representation corresponding to the 4×4 matrix; (**c**) the 4×4 pixel matrix and its pixel pair selection schematic.

and $Pixel_B = b_8b_7b_6b_5b_4b_3b_2b_1$, the pixel pairs producing the children are denoted as $Pixel'_A = a'_8a'_7a'_6a'_5a'_4a'_3a'_2a'_1$ and $Pixel'_B = b'_8b'_7b'_6b'_5b'_4b'_3b'_2b'_1$. The random number is noted as $C = c_8c_7c_6c_5c_4c_3c_2c_1$.

(1) *Crossover* According to the random number c, if $c_i = 0$, pixel $Pixel'_A$ inherits the value of the corresponding binary bit of $Pixel_B$, and pixel $Pixel'_B$ inherits the value of the corresponding binary bit of $Pixel_A$; if $c_i = 1$, pixel $Pixel'_A$ inherits the value of the corresponding bit of $Pixel_A$, and pixel $Pixel'_B$ inherits the value of the corresponding bit of Pixel$_B$.
(2) *Mutation* Non-uniform mutation is used, for the pixel to be varied, according to the random number c, if $c_i = 0$, the bit in which the new pixel is located inherits the value of the original pixel in the bit in which it is located; if $c_i = 1$, the corresponding bit of the pixel is varied: 0 becomes 1, or 1 becomes 0. Thus, two new individuals $Pixel'_A$ and $Pixel'_B$ are obtained.

The process of crossover and mutation is schematically shown in Fig. 10. For the selected pixel pairs, the same random number is used for crossover and mutation in this article, these operations can be performed simultaneously. Crossover and mutation can be described by Eqs. (12) and (13):

$$a'_i = \begin{cases} b_i \; if & c_i = 0 \\ \tilde{a}_i \; if & c_i = 1 \end{cases}, \tag{12}$$

$$b'_i = \begin{cases} a_i \; if & c_i = 0 \\ \tilde{b}_i \; if & c_i = 1 \end{cases}, \tag{13}$$

where a_i and b_i are the ith bit of the original pixel pairs, $\tilde{a}_i$ and $\tilde{b}_i$ are the results of the a_i and b_i non-operations, respectively, a'_i and b'_i are the ith bit of the new pixel pairs after crossover and mutation, and i is the number of bits in the binary sequence.

Individual rearrangement operation

With the idea of rearrangement, the grey value of the pixel to be encrypted is converted into an 8-bit binary sequence. The binary sequence of the pixel undergoes individual rearrangement to achieve bit-level scrambling. Here, eight individual rearrangement rules are defined, as shown in Fig. 11. For a given pixel, one individual

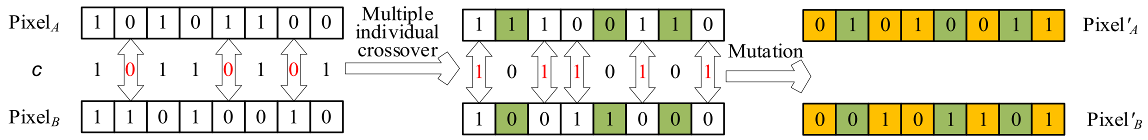


Figure 10. Schematic diagram of crossover and mutation.

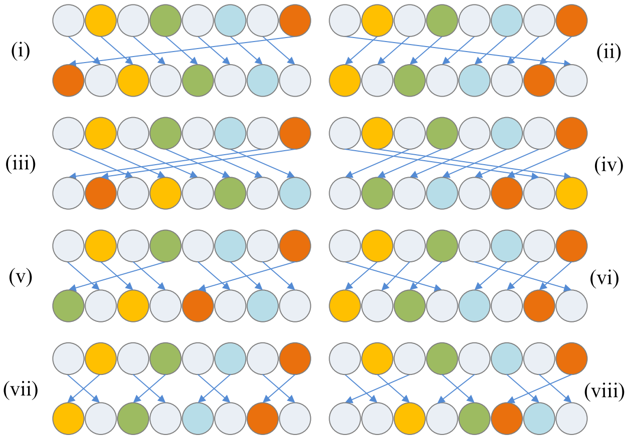


Figure 11. Individual rearrangement rules.

rearrangement rule is randomly selected to scramble its binary sequence, affecting the change in pixel value. The random selection is achieved using pseudo-random sequences generated by the chaotic system.

Ciphertext feedback

Ciphertext feedback is an operation designed to enhance the interaction between pixels and alter pixel values. It allows small changes in plaintext to diffuse throughout the entire ciphertext, boosting the scheme's resistance to differential and statistical attacks. The process efficiently propagates small changes in the plaintext image to the entire ciphertext image by modifying the pixel value based on the previous pixel value along with the generated pseudo-sequence value. Given a pseudo-random sequence $D=\{d_1, d_2, d_3,\ldots d_{M\times N}\}$ of length $M\times N$, where the element values in D range from 0 to 255, the image matrix is converted into a one-dimensional sequence $S=\{s_1, s_2, s_3,\ldots s_{M\times N}\}$ of length $M\times N$ in row-first order. The feedback image sequence is denoted as $C=\{c_1, c_2, c_3,\ldots c_{M\times N}\}$, and the feedback process is shown in Eq. (14):

$$c_i = s_i \oplus c_{i-1} \oplus d_i, \tag{14}$$

where the initial element $c_0=127$ and $i=1, 2, \ldots, M\times N$.

Complete the encryption process

The proposed image encryption scheme in this article comprises two parts: the evolutionary operators and the ciphertext feedback. The evolutionary operators involve selection, crossover, and mutation, performing double scrambling and diffusion at the bit and pixel levels. This encryption scheme is designed to encrypt images of any size. For any $M\times N$ image, if $M\times N$ is even, no processing is required; if $M\times N$ is odd, supplementary processing is done with '0'. The detailed encryption process is as follows:

Input a grey level image P of size $M\times N$, where M and N are the number of rows and columns of the image, with initial values of the parameters x_0', y_0', z_0' and w_0'; Output a ciphertext image E.

- *Step 1* Convert the grey level image P to be encrypted into an image matrix of size $M\times N$, denoted as matrix P_1.
- *Step 2* Use the hash function to calculate the hash value K of matrix P_1. Obtain the initial parameter values x_0, y_0, z_0, and w_0 of the chaotic system using Eqs. (8)–(10).
- *Step 3* The four-dimensional chaotic system is iterated $M\times N+1000$ times, and the values of the first 1000 iterations are discarded to eliminate transient effects, thereby obtaining four pseudo-random sequences LX, LY, LZ, and LW of length $M\times N$.
- *Step 4* Process the pseudo-random sequence LX according to Eq. (15), reshaping it into a matrix form for the selection of individual recombination rules. After the individual recombination operation in "Individual rearrangement operation" section, recombine and scramble each pixel in matrix P_1 to obtain the recombination matrix P_2.

$$lx_i' = mod\left(floor\left(10^{14} \times lx_i\right), 8\right) + 1. \tag{15}$$

- *Step 5* Sort the pseudo-random sequence LY in ascending order to obtain a new sequence LY'. Find the positions of each element in the original sequence LY within the new sequence LY', and arrange these position numbers into a new sequence to obtain the index sequence '*Index*'. According to the index sequence '*Index*', select the pixel pairs sequentially from the matrix P_2 using Eq. (11).
- *Step 6* Process the pseudo-random sequence LZ according to Eq. (16) to obtain the random sequence LZ' and ensure the value of each element in the random sequence LZ' is between 0 and 255. According to "Crossover and mutation operation" section, select the elements from the odd positions of the random sequence LZ' as the random numbers used in the crossover and mutation operations. Based on the selected random numbers,

the pixels selected in Step 5 are sequentially subjected to crossover and mutation operations to obtain the matrix P_3.

$$lz_i' = mod\left(floor\left(10^{14} \times lz_i\right), 256\right). \tag{16}$$

- *Step 7* Process the pseudo-random sequence *LW* according to Eq. (17). Convert matrix P_3 into a one-dimensional sequence, and according to the ciphertext feedback operation described in "Ciphertext feedback" section, perform ciphertext feedback for each pixel. Recover the result into matrix form to obtain matrix P_4, i.e., the ciphertext image *E*.

$$lw_i' = mod\left(floor\left(10^{14} \times lw_i\right), 256\right). \tag{17}$$

The decryption scheme is the inverse process of the above scheme and is not elaborated here. Additionally, this scheme is equally applicable to encrypting color images by simply decomposing pixels that are only images into RGB channels.

Simulation experiment results

To verify the feasibility and effectiveness of this method, we selected five grayscale images (Boat, House, Gray21, Pentagon, SanDiego) with a size of 256 × 256 from the image database (http://sipi.usc.edu/database/). These images were then subjected to encryption validation and tested on the Matlab 2018 platform, with the key given the value of $x_0' = y_0' = z_0' = w_0' = 0.01$. In terms of security analysis, only the Boat image was used as an example to demonstrate the advantages of our method. The plaintext, ciphertext and decrypted images are shown in Fig. 12, by visual observation, the ciphertext has completely lost the characteristics of the plaintext. The scheme is lossless, and the decrypted image obtained after decrypting the ciphertext is the same as the plaintext.

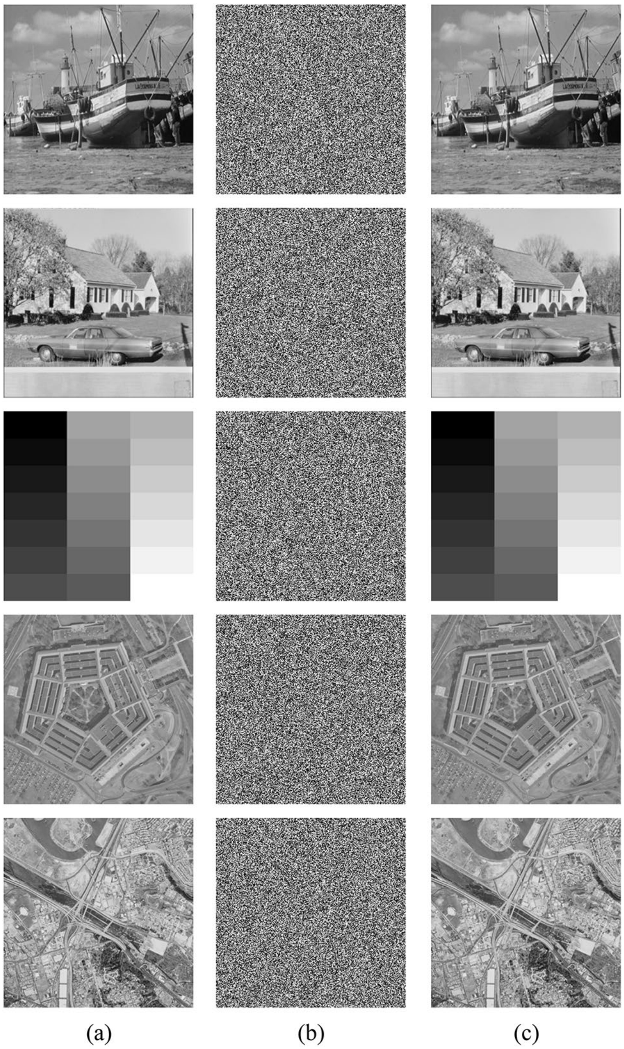


Figure 12. Simulation results: (**a**) plaintext images; (**b**) ciphertext images; (**c**) decrypted images.

An ideal encryption scheme must be key-sensitive and resistant to common attacks. Standard performance metrics are used to fully evaluate the proposed encryption scheme, including keyspace analysis, statistical attack analysis, differential attack analysis, and robust analysis.

Keyspace analysis

The key plays a crucial role in encryption systems and must have a high level of security. The proposed encryption scheme is so sensitive to its key, the plaintext image, and the ciphertext image that any small change in one of them can lead to a significant difference in the generated image. For example, the generated image is random if any slight disturbance is applied to the ciphertext image. The main reason for this is the application of chaotic systems, which are very sensitive to small changes.

An attacker will try to use all possible keys to try to break the encryption system. Therefore, a larger keyspace is more resistant to brute force attacks. It has been shown that even with powerful computers if the keyspace is more significant than 2^{128} [34], the encryption method cannot be cracked by a brute force attack within the specified time. In this article, the keystream length reaches $10^{60} > 2^{128}$, which is sufficient to resist any brute-force attack.

Statistical analysis

The performance of the proposed image encryption scheme is tested through statistical analysis. Statistical methods to analyze any predictable relationship between plaintext and ciphertext images.

Histogram analysis

The histogram represents the distribution of pixels across different grey levels in the image. In a robust cryptosystem, the pixel distribution in the ciphertext image should exhibit uniformity and be distinguishable from the histogram of the plaintext image. It is evident from Fig. 13 that the uniform distribution of pixel values in the ciphertext image prevents attackers from extracting any statistical information.

χ^2*test*

To prove that this uniformity is not only visually uniform but also theoretically uniformly distributed, the χ^2 test is performed on the ciphertext. The histogram of the image is represented by $hist_i(i = 0, 1, \ldots, 255)$. Equation (18) depicts the formula used to calculate the χ^2 distribution of the histogram.

$$\chi^2 = \frac{1}{256}\left(\sum_{i=0}^{255} hist_i - \frac{1}{256}\sum_{i=0}^{255} hist_i\right)^2. \tag{18}$$

The histogram obeys the χ^2 distribution with 255 degrees of freedom. The hypothesis is accepted given a significance level α such that $P\left\{\chi^2 \geq \chi^2_\alpha(n-1)\right\} = \alpha$, i.e., $\chi^2 < \chi^2_\alpha(n-1)$. When significant level α = 0.01, 0.05 and 0.1, there are $\chi^2_{0.01}(255) = 310.45739$, $\chi^2_{0.05}(255) = 293.24783$, and $\chi^2_{0.1}(255) = 284.33591$.

Displays the χ^2 distribution of the test images. All ciphertext images in Table 3 pass the test in experiments with significance levels of α = 0.01, α = 0.05, and α = 0.1. The comparison shows that the scheme significantly changes the histogram distribution of the images and can break the statistical features of plaintext images.

Correlation analysis

Neighboring pixels of a plaintext image correlate highly in all directions. An ideal encryption scheme aims to minimize the correlation between adjacent pixels in the ciphertext image, thereby effectively enhancing its resistance against statistical attacks. The calculation of the correlation coefficient can be performed using Eq. (19):

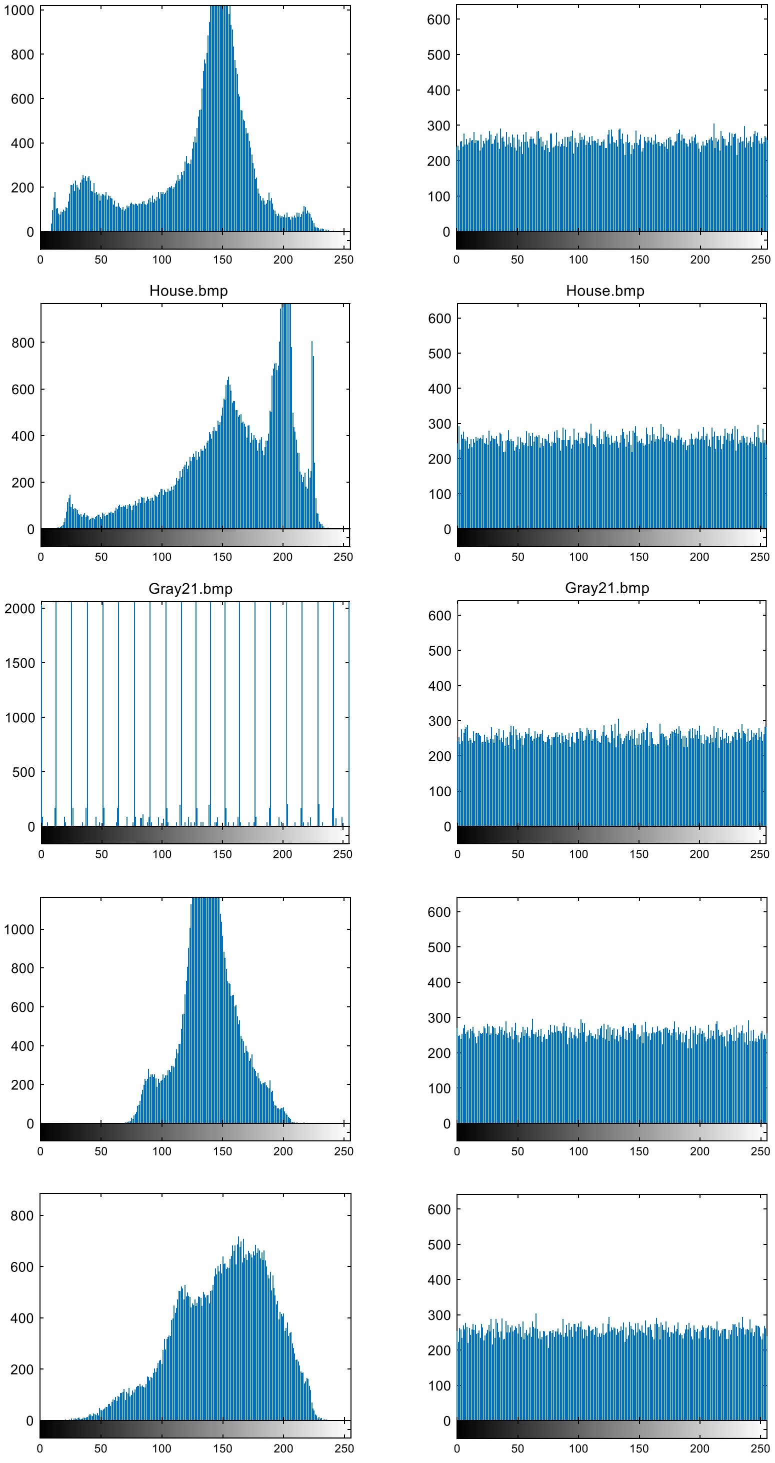
$$\begin{cases} E(x) = \frac{1}{N}\sum\limits_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum\limits_{i=1}^{N} (x_i - E(x))^2 \\ cov(x, y) = \frac{1}{N}\sum\limits_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\ r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \end{cases}, \tag{19}$$

where r_{xy} is the correlation coefficient, $cov(x, y)$, $D(x)$, and $E(x)$ represent the covariance, variance, and mean value, respectively.

To analyze adjacent pixel correlation in plaintext and ciphertext images, 10,000 randomly selected adjacent pixel pairs from plaintext and ciphertext images are tested, using the Boat image as an example. Figure 14 demonstrates that neighboring pixels in plaintext images are highly concentrated and have a strong correlation, whereas neighboring pixels in ciphertext images are randomly distributed, resulting in a reduced correlation between them. Furthermore, Table 4 shows that the correlation between neighboring pixels in ciphertext images is lower than in plaintext images.

Information entropy test

Information entropy is a statistical metric used to assess the randomness or disorder of information[35]. It measures the level of uncertainty or unpredictability associated with a given set of information, represented as Eq. (20):



(a)

(b)

Figure 13. Histogram: (**a**) histogram of plaintext images Boat, House, Gray21, Pentagon, SanDiego; (**b**) histogram of each corresponding ciphertext image.

$$H(m) = -\sum_{i}^{l} P(m_i)\log_2 P(m_i), \tag{20}$$

where l is the grey value of the image, take $l = 255$. m_i is the ith grey level value on the image, and $P(m_i)$ represents the probability of m_i.

	Plaintext images	Ciphertext images	α = 0.01	α = 0.05	α = 0.1
Boat	100,853.4922	243.7891	Passed	Passed	Passed
House	83,975.34375	269.0938	Passed	Passed	Passed
Gray21	614,162.6718	249.7891	Passed	Passed	Passed
Pentagon	151,407.1641	251.3203	Passed	Passed	Passed
SanDiego	59,757.75781	249.3359	Passed	Passed	Passed

Table 3. Statistics of χ^2 distribution of histograms.

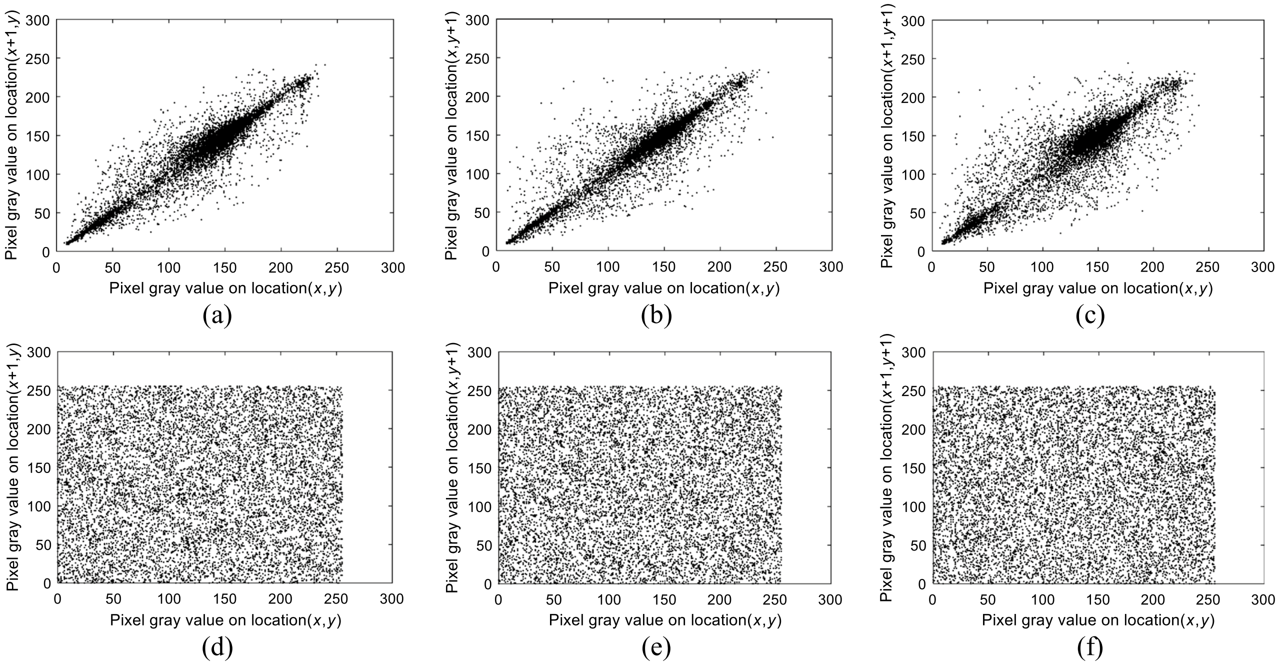


Figure 14. Pixel statistics of randomly selected pixel points and their neighboring pixel points of the Boat image: (**a**–**c**) are the neighboring pixel statistics of the plaintext in horizontal, vertical, and diagonal directions, respectively; (**d**–**f**) are the neighboring pixel statistics of the ciphertext in horizontal, vertical and diagonal directions, respectively.

Image	Horizontal	Vertical	Diagonal
Boat			
Plaintext	0.9458	0.9315	0.8861
Ciphertext	0.0043	0.0017	0.0017
House			
Plaintext	0.9359	0.9194	0.8742
Ciphertext	−0.0085	0.0079	0.0084
Gray21			
Plaintext	0.9998	0.9963	0.9961
Ciphertext	−0.0052	0.0010	0.0040
Pentagon			
Plaintext	0.8331	0.8089	0.7025
Ciphertext	0.0023	0.0050	−0.0071
SanDiego			
Plaintext	0.7804	0.7902	0.7071
Ciphertext	0.0039	0.0026	0.0056

Table 4. Correlation coefficients.

Image	Information entropy
Boat	
Plaintext	7.1572
Ciphertext	7.9973
House	
Plaintext	7.2298
Ciphertext	7.9970
Gray21	
Plaintext	4.8997
Ciphertext	7.9973
Pentagon	
Plaintext	6.5577
Ciphertext	7.9972
SanDiego	
Plaintext	7.2289
Ciphertext	7.9972

Table 5. Information entropy.

The ideal information entropy value for a completely random image is 8. By measuring the information entropy of the ciphertext image, we can determine how close it is to 8 and how random the image information is. As shown in Table 5, after encryption, the information entropy of all ciphertext images is close to 8.

Differential attack analysis

Differential attack involves studying the impact of differences in the plaintext on its corresponding ciphertext. The objective is to establish a connection between the plaintext and ciphertext images, aiming to identify vulnerabilities and potentially compromise the encryption algorithm. NPCR and UACI are the two methods to test whether the encryption scheme resists differential attacks[36]. NPCR measures the ratio of differing pixels found at corresponding locations in two images, relative to the total number of pixels in the image, with an ideal value of 99.6094%. UACI represents the average density of changes in an image, reflecting the overall intensity of change in the image, with an ideal value of 33.4635%. They are calculated using the Eq. (21):

$$\begin{cases} NPCR = \frac{\sum_{i,j} |P_1(i,j) \oplus P_2(i,j)|}{M \times N} \times 100\% \\ UACI = \frac{\sum_{i,j} |P_1(i,j) - P_2(i,j)|}{255 \times M \times N} \times 100\% \end{cases}, \tag{21}$$

where P_1 and P_2 are two different ciphertexts.

Five different ciphertext images of Boat, House, Gray21, Pentagon, and SanDiego are tested, and their NPCR and UACI values for the proposed encryption scheme are presented in Table 6, indicating strong resistance to differential attacks as all test results are close to ideal values.

Robustness analysis

Noise attack analysis

Effective image encryption schemes can reconstruct recognizable decrypted images even when noise interference or data loss occurs during transmission, as digital images may be disrupted by various factors. Pepper noise of 1%, 5%, and 10% are added to the ciphertext image of Boat and then decrypted. Figure 15 shows the experimental results of the images of Boat with noise intensity of 1%, 5%, and 10% and the decrypted image. The figure demonstrates that the decrypted image remains recognizable even under a noise intensity of 10%, indicating the proposed encryption scheme's effective resistance against noise attacks.

Scheme	NPCR (%)	UACI (%)
Boat	99.5851	33.4002
House	99.5926	33.3774
Gray21	99.6216	33.5847
Pentagon	99.6033	33.4884
SanDiego	99.6384	33.5156

Table 6. NPCR and UACI values.

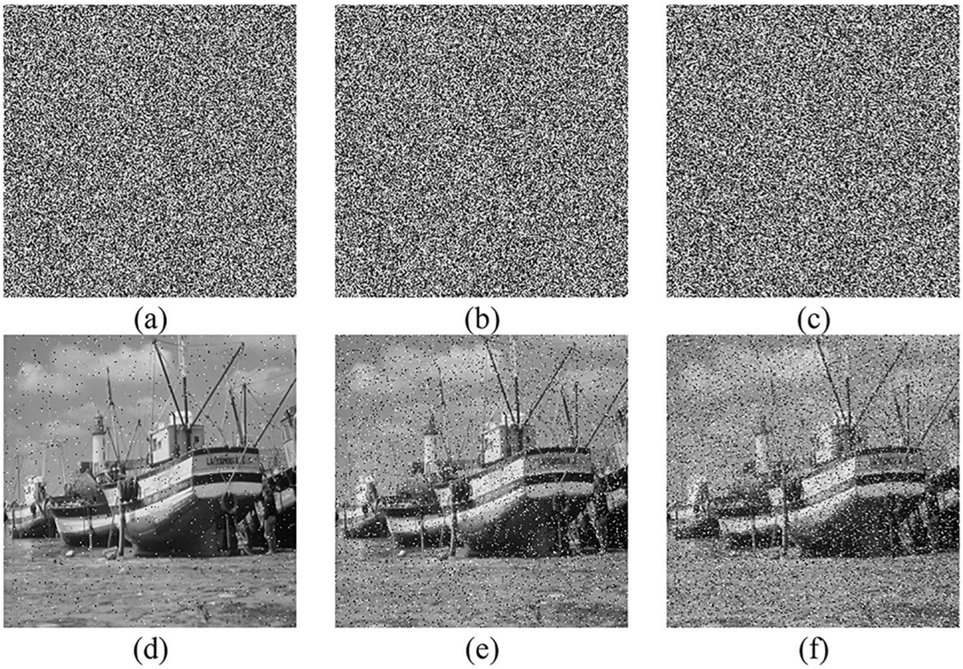


Figure 15. Ciphertext image and decrypted image after pepper noise attack with different strengths: (**a**–**c**) are the ciphertext images with 1%, 5%, and 10% pepper noise added, respectively; (**d**–**f**) are the decrypted images corresponding to (**a**–**c**).

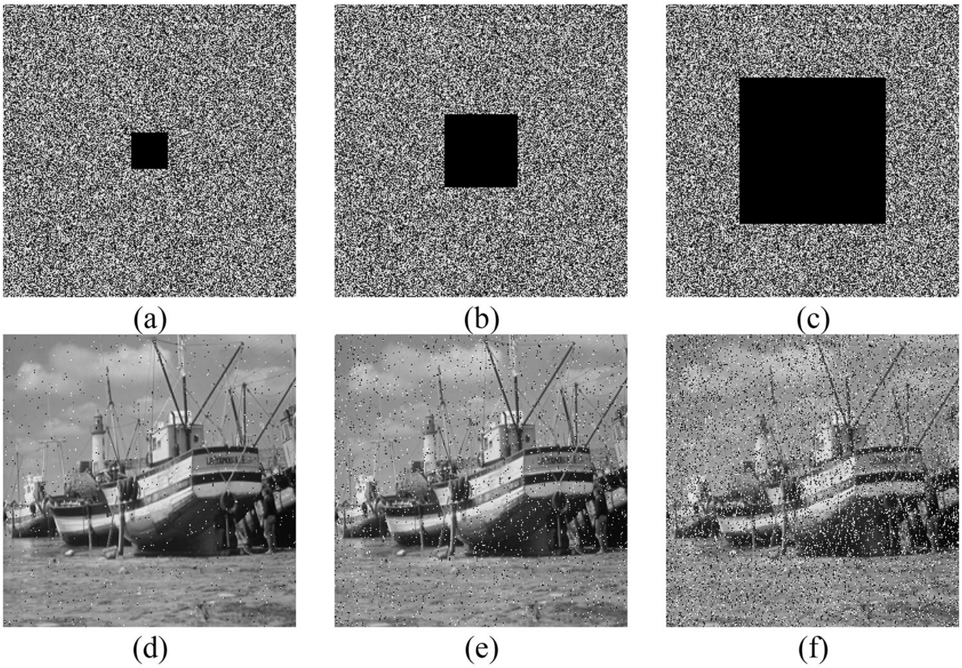


Figure 16. Cropping the ciphertext image and the corresponding decrypted image with different degrees of cropping: (**a**–**c**) are the ciphertext images cropped 1/64, 1/16, and 1/4 respectively; (**d**–**f**) are the decrypted images corresponding to (**a**–**c**).

Schemes	Entropy	NPCR	UACI	Correlation coefficient		
				Horizontal	Vertical	Diagonal
Our	7.9974	99.6735	33.2765	0.0018	0.0020	0.0001
[37]	7.9973	99.5859	28.6400	−0.0035	−0.0004	−0.0004
[38]	7.9972	99.6427	33.4741	0.0053	0.0059	0.0031
[39]	7.9974	99.6107	33.4576	−0.0022	0.0018	−0.0019
[40]	7.9960	99.5415	33.2400	0.0023	−0.0020	−0.0073
[41]	7.9970	99.6277	33.4390	0.0015	−0.0012	0.0021

Table 7. Comparison.

Clipping attack analysis

When images are transmitted over a network, data may be lost for various reasons. By cropping a portion of the ciphertext image and decrypting the cropped ciphertext image, we can test the ability of the ciphertext image to be recovered to the plaintext image in case of data loss and analyze the performance of the encryption scheme against the cropping attack. Cropping attack analysis can reflect the effect of the encryption algorithm on the scrambling of the plaintext image. The better the scrambling effect, the stronger the encryption algorithm recovers the visual features of the plaintext image when a part of the data is lost. In Fig. 16, the ciphertext image of Boat is decrypted after being cropped at different proportions (1/64, 1/16, and 1/4). The decrypted image retains identifiable information, demonstrating the robustness of the proposed encryption scheme against cropping attacks.

Comparative analysis

We compare the performance of this scheme with the literature of the last 3 years, and the newly compared schemes satisfy the criteria of image security based on both experimental results and performance analysis. They can represent the general level of image encryption security in recent years. Table 7 summarizes the comparative analysis results for the same image, focusing on the evaluation metrics of correlation, NPCR, UACI, and information entropy. It can be seen that, in terms of information entropy, the proposed scheme in this article is higher than others and closer to the ideal value. In terms of NPCR and UACI, the proposed scheme is closer to the ideal value than the others. In terms of relevance, the scheme proposed is better than the schemes[37–40], but slightly higher than the schemes[41]. Overall, the proposed encryption scheme has a superior performance in terms of security.

Conclusions

By introducing a new state variable, this article successfully injects a more complex dynamical component into the three-dimensional chaotic system. Through experimental analyses, it is verified that the proposed four-dimensional chaotic system exhibits higher stochasticity and sensitivity. This complexity brings significant benefits to image encryption applications by enhancing the strength and unpredictability of the encryption algorithm. It enables the algorithm to possess a larger keyspace and increases the difficulty of attacks. Furthermore, an image encryption scheme is proposed by combining evolutionary operators with the pseudo-randomness of chaotic systems. In this encryption scheme, the introduction of evolutionary operators effectively disrupts the correlation between neighboring pixels. The resistance to differential attacks is significantly enhanced through operations such as crossover and mutation, yielding remarkable results. The experimental and simulation results comprehensively demonstrate the feasibility and superiority of the scheme. With its vast keyspace and high sensitivity to keys, the scheme effectively withstands multiple attacks, including exhaustive attacks, statistical analysis, and differential attacks.

In summary, the image encryption scheme proposed in this article exhibits commendable performance, meeting the stringent security requirements of image transmission. It is expected to have a positive impact on security measures in practical applications. This research outcome provides valuable insights and practical solutions for further development and innovation in the field of image encryption. Future research could explore additional image security schemes based on chaotic systems and evolutionary strategies to further enhance the security and privacy of image transmission.

Data availability

All data generated or analyzed during this study are included in this published article.

Received: 24 November 2023; Accepted: 21 March 2024
Published online: 25 March 2024

References

1. Hui, Y., Liu, H. & Fang, P. A DNA image encryption based on a new hyperchaotic system. *Multimed. Tools Appl.* **82**, 21983–22007 (2023).
2. Noori Ghanim, Z. & Raheem Khoja, S. A. A partial image encryption scheme based on DWT and texture segmentation. *Cogent Eng.* **9**(1), 2026555 (2022).
3. Geng, S., Li, J., Zhang, X. & Wang, Y. An image encryption algorithm based on improved Hilbert curve scrambling and dynamic DNA coding. *Entropy* **25**(8), 1178 (2023).

4. Huang, X., Dong, Y., Ye, G. & Shi, Y. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Front. Comput. Sci.* **17**(3), 173804 (2023).
5. Wang, L., Ran, Q. & Ding, J. Quantum color image encryption scheme based on 3D non-equilateral Arnold transform and 3D logistic chaotic map. *Int. J. Theor. Phys.* **62**(2), 36 (2023).
6. Sun, X. & Chen, Z. A new image encryption strategy based on Arnold transformation and logistic map. In *Proceedings of the 11th International Conference on Computer Engineering and Networks* 712–720 (Springer, Singapore, 2022).
7. Panchikkil, S., Manikandan, V. M. & Zhang, Y. D. A convolutional neural network model based reversible data hiding scheme in encrypted images with block-wise Arnold transform. *Optik* **250**, 168137 (2022).
8. Zhou, S., Zhao, Z. & Wang, X. Novel chaotic colour image cryptosystem with deep learning. *Chaos Solitons Fractals* **161**, 112380 (2022).
9. Panwar, K., Kukreja, S., Singh, A. & Singh, K. K. Towards deep learning for efficient image encryption. *Procedia Comput. Sci.* **218**, 644–650 (2023).
10. Himthani, V., Singh Dhaka, V. & Kaur, M. A visually meaningful image encryption scheme based on a 5D chaotic map and deep learning. *Imaging Sci. J.* **69**(1–4), 164–176 (2021).
11. Guo, L., Du, H. & Huang, D. A quantum image encryption algorithm based on the Feistel structure. *Quantum Inf. Process.* **21**, 1–18 (2022).
12. Liu, X. & Liu, C. Quantum image encryption scheme using independent bit-plane pervariation and Baker map. *Quantum Inf. Process.* **22**(6), 262 (2023).
13. Dai, J. Y. & Zhou, N. R. Optimal quantum image encryption algorithm with the QPSO-BP neural network-based pseudo random number generator. *Quantum Inf. Process.* **22**(8), 318 (2023).
14. Wang, J., Geng, Y. & Liu, J. Adaptive quantum image encryption method based on wavelet transform. arXiv:1901.07762 (2019).
15. Mondal, B., Singh, S. & Kumar, P. A secure image encryption scheme based on cellular automata and chaotic skew tent map. *J. Inf. Secur. Appl.* **45**, 117–130 (2019).
16. Ma, K., Teng, L., Wang, X. & Meng, J. Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory. *Multimed. Tools Appl.* **80**, 24737–24757 (2021).
17. Zhao, J., Wang, S. & Zhang, L. Block image encryption algorithm based on novel chaos and DNA encoding. *Information* **14**(3), 150 (2023).
18. Ahuja, B., Doriya, R., Salunke, S., Hashmi, M. F. & Gupta, A. Advanced 5D logistic and DNA encoding for medical images. *Imaging Sci. J.* **71**(2), 142–160 (2023).
19. Sun, S. A new image encryption scheme based on 6D hyperchaotic system and random signal insertion. *IEEE Access* 66009–66016 (2023).
20. Ndassi, H. L. *et al.* A robust image encryption scheme based on compressed sensing and novel 7D oscillator with complex dynamics. *Heliyon* **9**, e16514 (2023).
21. Zhang, H., Wang, X., Xie, H., Wang, C. & Wang, X. An efficient and secure image encryption algorithm based on non-adjacent coupled maps. *IEEE Access* **8**, 122104–122120 (2020).
22. Wang, X. & Chen, X. An image encryption algorithm based on dynamic row scrambling and Zigzag transformation. *Chaos Solitons Fractals* **147**, 110962 (2021).
23. Zhu, Y., Wang, C., Sun, J. & Yu, F. A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. *Mathematics* **11**(3), 767 (2023).
24. Ye, G., Wu, H., Liu, M. & Shi, Y. Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Syst. Appl.* **205**, 117709 (2022).
25. Beyer, H. & Schwefel, H. Evolution strategies–a comprehensive introduction. *Nat. Comput.* **1**(1), 3–52 (2022).
26. Jasra, B. & Moon, A. H. Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system. *Expert Syst. Appl.* **206**, 117861 (2022).
27. Cun, Q., Tong, X., Wang, Z. & Zhang, M. A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing. *Vis. Comput.* 1–20 (2023).
28. Li, T., Yan, W. & Chi, Z. A new image encryption algorithm based on optimized Lorenz chaotic system. *Concurr. Comput. Pract. Exp.* **34**(13), e5902 (2022).
29. Yang, S., Tong, X. & Wang, Z. S-box generation algorithm based on hyperchaotic system and its application in image encryption. *Multimed. Tools Appl.* **82**, 25559–25583 (2023).
30. Arthi, G., Thanikaiselvan, V. & Amirtharajan, R. 4D Hyperchaotic map and DNA encoding combined image encryption for secure communication. *Multimed. Tools Appl.* **81**, 15859–15878 (2022).
31. De Dieu, N. J., Ruben, F. S. V., Nestor, T., Zeric, N. T. & Jacques, K. Dynamic analysis of a novel chaotic system with no linear terms and use for DNA-based image encryption. *Multimed. Tools Appl.* **81**(8), 10907–10934 (2022).
32. Gong, L. H., Luo, H. X., Wu, R. Q. & Zhou, N. R. New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG. *Phys. A Stat. Mech. Appl.* **591**, 126793 (2022).
33. Yu, J., Xie, W., Zhong, Z. & Wang, H. Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. *Chaos Solitons Fractals* **162**, 112456 (2022).
34. Rani, N., Sharma, S. R. & Mishra, V. Grayscale and colored image encryption model using a novel fused magic cube. *Nonlinear Dyn.* **108**(2), 1773–1796 (2022).
35. Erkan, U., Toktas, A. & Lai, Q. 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Syst. Appl.* **213**, 119076 (2023).
36. Lone, M. A. & Qureshi, S. Encryption scheme for RGB images using chaos and affine hill cipher technique. *Nonlinear Dyn.* **111**(6), 5919–5939 (2023).
37. Adhikari, S. & Karforma, S. An efficient image encryption method using henon-logistic-tent chaotic pseudo random number sequence. *Wirel. Pers. Commun.* **129**, 2843–2859 (2023).
38. Liang, Q. & Zhu, C. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. *Opt. Laser Technol.* **160**, 109033 (2023).
39. Gui, X., Huang, J. & Li, L. A novel hyperchaotic image encryption algorithm with simultaneous shuffling and diffusion. *Multimed. Tools Appl.* **81**, 21975–21994 (2022).
40. Wang, X. & Su, Y. Image encryption based on compressed sensing and DNA encoding. *Signal Process. Image Commun.* **95**, 116246 (2021).
41. Hussain, M., Iqbal, N. & Bashir, Z. A chaotic image encryption scheme based on multi-directional confusion and diffusion operations. *J. Inf. Secur. Appl.* **70**, 103347 (2022).

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grants 62102374 and 62072417.

Author contributions

Y.N.: review and editing, formal analysis, methodology, conceptualization, investigation, project administration, supervision. X.Z.: writing—original draft, writing—review and editing, software, methodology. H.Z.: data curation, validation.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to X.Z.