BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES
DOI: 10.24425/bpasts.2026.2512

Image Encryption and Restoration Based on a Bimodal Isomorphic Dynamical System

Qian Xiong[1], Zai-Fang Xi[1], Jia Duan[2], Wen-Xin Yu[1]

[1] School of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[2] Third Surveying and Mapping Institute of Hunan Province, Changsha 410000, China

Abstract. In this paper, an image encryption and restoration method based on a bimodal isomorphic dynamical system is proposed to address the issues of privacy security and large-scale data loss or damage in digital image transmission, particularly in scenarios characterized by high real-time requirements, unreliable links, or ongoing attacks. Unlike existing methods that treat encryption and restoration as separate modules, the proposed system achieves both functions within a unified architecture, where the same nonlinear framework can be switched between chaotic and stochastic resonance modes via parameter adjustment. Firstly, a foundational nonlinear system framework is constructed. Under the same architecture, parameters are adjusted to obtain a chaotic system for encryption and decryption, as well as a stochastic resonance system for noise reduction, followed by a characteristics analysis of these two systems. Secondly, a chaos-based encryption and decryption algorithm is investigated. In this algorithm, a random-point scrambling method combined with Latin matrix diffusion is developed to enhance the security and robustness of the encryption process. Thirdly, a restoration algorithm for extensively damaged images is studied. This algorithm integrates stochastic resonance denoising with integral restoration to suppress noise while preserving fine image details. Finally, simulation experiments are conducted: in the chaotic mode, the encryption and decryption results are evaluated through histogram analysis, correlation coefficients, information entropy, and other relevant experiments, verifying that the encryption algorithm provides excellent communication confidentiality. In the stochastic resonance mode, by comparing the restoration effects on different large-area damaged regions, it is demonstrated that the algorithm can effectively recover the image's characteristic information even under severe damage conditions.

Key words: Nonlinear System, Image Encryption and Decryption, Image Restoration

1. INTRODUCTION

Digital images serve as crucial carriers in the information age, making their secure transmission and integrity assurance vital across military, medical, financial, and personal privacy domains [1]. However, the transmission of image data over public network channels faces dual challenges: on the one hand, unauthorized access and malicious attacks persistently threaten the confidentiality and integrity of images [2]. On the other hand, inherent channel instability and packet loss can easily lead to widespread image corruption, significantly compromising the usability of the information.

It is noteworthy that in many practical application scenarios, traditional retransmission mechanisms are often difficult to implement due to their inherent limitations. For instance, in high-confrontation environments such as military communications and emergency command systems [3-4], the system faces stringent real-time constraints and transmission reliability challenges: tasks such as battlefield situational awareness and target identification require millisecond-level image response. Traditional retransmission mechanisms introduce additional delays and thus cannot meet real-time decision-making demands. Simultaneously, communication links subjected to interference or hijacking [5] further render retransmission requests ineffective or lead to repeated data packet corruption. Similarly, in scenarios with constrained communication resources, such as deep-space exploration and underwater sensor networks [6-7], narrow bandwidth, precious energy reserves, and extremely high transmission latency make the cost of retransmission prohibitive. Consequently, the receiving end must break away from traditional dependencies and possess the capability for immediate restoration of corrupted data, as well as the ability to reconstruct information from incomplete data in a single attempt. This is essential to ensure both information continuity and information recovery in scenarios where retransmission is either impossible or excessively costly.

To address security challenges, chaotic systems have emerged as an ideal tool for image encryption due to their extreme sensitivity to initial conditions, ergodicity, and pseudo-randomness. The field has evolved from early low-dimensional systems to contemporary complex dynamical structures such as high-dimensional [8] and multi-scroll [9] systems, further integrating with advanced technologies like DNA encoding [10] and complex tensor models [11]. Consequently, encryption algorithms [12-14] have continuously improved in both security and complexity. However, existing research has

predominantly focused on enhancing encryption strength, such as Gao JX et al.'s work on hybrid chaotic systems [15] or Fu ZW et al.'s construction of secure transmission protocols [16], often overlooking the realistic scenario where encrypted images may suffer severe damage due to attacks or interference after transmission. If encrypted data experiences large-scale loss during transmission, traditional decryption operations will struggle to reconstruct meaningful visual information.

In the field of image restoration, while existing techniques such as singular value denoising [17] or frequency selection [18] can handle noise or localized damage to some extent, their ability to restore large-scale data loss—particularly when pixel values of encrypted images exhibit random distribution—remains highly limited. Notably, stochastic resonance, as a physical mechanism that leverages noise to amplify weak signals, has demonstrated unique advantages in signal processing. The high-dimensional stochastic resonance system constructed by Zhou ZB et al. [19], as well as its coupling with vibrational resonance by Li JM et al. [20], has proven its effectiveness in extracting features under complex noise backgrounds. This offers a novel perspective for addressing the challenge of restoring large-scale damage in encrypted images.

Despite these advances, existing approaches typically treat encryption and restoration as separate modules, requiring independent system designs that lack flexibility and scalability. Moreover, most chaotic encryption schemes focus solely on security performance without considering the realistic scenario where encrypted images may suffer severe damage during transmission. When large-scale data loss occurs, conventional decryption operations struggle to reconstruct meaningful visual information. To overcome these limitations, this paper proposes a bimodal isomorphic dynamical system that unifies encryption and restoration within a single architecture. By simply adjusting system parameters, the same nonlinear framework can switch between chaotic mode for secure encryption and stochastic resonance mode for noise reduction and image restoration. This design not only simplifies the overall system structure but also ensures seamless integration of encryption and restoration functions, providing a more robust and adaptable solution for secure image transmission in challenging environments.

The remainder of this paper is structured as follows. Section 2 constructs a bimodal nonlinear system and analyzes the dynamical characteristics of its different modes under various parameter conditions. Sections 3 and 4 design a comprehensive encryption algorithm, which integrates chaotic sequence-based random-point scrambling with Latin matrix diffusion, achieving high-security image encryption. Section 4 further verifies the confidentiality performance of the algorithm in image communication through experiments including histogram analysis, correlation coefficients, and information entropy. Section 5 proposes a restoration algorithm for large-area damaged images, effectively recovering the characteristic information of images through stochastic resonance denoising and integral restoration.

2. MATHEMATICAL MODEL OF THE NONLINEAR SYSTEM

As shown in Eq. (1), a nonlinear system is constructed in this paper. Under different parameter conditions, this system can yield a four-dimensional chaotic system for encryption and decryption, as well as a stochastic resonance system for denoising.

$$\begin{cases} \dot{x} = -ax - by + czw \\ \dot{y} = dxz - eyz \\ \dot{z} = -fxw + gz \\ \dot{w} = kx - my - nw \end{cases} \tag{1}$$

where x, y, z, w represent the state variables of the system and $a, b, c, d, e, f, g, k, m, n$ denote the parameters.

(1) Chaotic Mode: When communication operates under normal conditions without attacks, only the chaotic system is employed for encryption and decryption.

(2) Stochastic Resonance Mode: When communication operates under conditions of high real-time requirements, extremely limited communication resources, unreliable links, or active attacks, resulting in large-scale data corruption, the stochastic resonance system is employed to denoise the frequency-expanded decrypted image.

2.1. Analysis of Chaotic Mode.

In this paper, chaotic sequences are utilized for encryption and decryption during transmission due to their high randomness. As shown in Eq. (2), a four-dimensional chaotic system is obtained by adjusting the parameters in Eq. (1).

$$\begin{cases} \dot{x} = -50x - 15y + 15zw \\ \dot{y} = 10xz - 11yz \\ \dot{z} = -26xw + 6z \\ \dot{w} = 30x - y - 10w \end{cases} \tag{2}$$

Set $a = 50, b = 15, c = 15, d = 10, e = 11, f = 26, g = 6, k = 30, m = 1, n = 10$, with an initial value of $[1\ 1\ 1\ 1]$, and conduct a chaos characteristic analysis on this four-dimensional chaotic system.

2.1.1 Analysis of Chaotic Characteristics.

To verify the chaotic characteristics of the four-dimensional chaotic system described by Eq. (2), the following analyses were conducted: time series diagrams, attractor phase portraits, and complexity analysis.

(1) When $c = 15$, the time series diagram and attractor phase portrait are shown in Fig. 1 and Fig. 2, respectively.

As illustrated in Figs. 1 and 2, the time-domain trajectory exhibits a continuous broadband spectrum, demonstrates noise-like characteristics, and displays non-periodic oscillations without repetition, which collectively indicate the inherent stochasticity of the dynamical behavior. The attractor forms a strange attractor with intricate fine-scale structure in phase space, where its trajectory undergoes stretching, folding, and

dense entanglement within a bounded region. These features reveal the nonlinear nature of the system, its sensitive dependence on initial conditions, and its long-term unpredictability.

(2) With $c \in (12,20)$, the SE complexity diagram and C0 complexity diagram at parameter c are shown in Fig. 3.

When $c \in (12,20)$, as shown in Fig. 3, the maximum SE complexity values for the x, y, z, w dimensions all exceed 0.6, while the maximum C0 complexity values for all dimensions exceed 0.2. This indicates that the chaotic sequences generated by this system possess a certain degree of complexity, making them suitable for use as pseudo-random sequences in image encryption and decryption processes to enhance the confidentiality of image encryption.

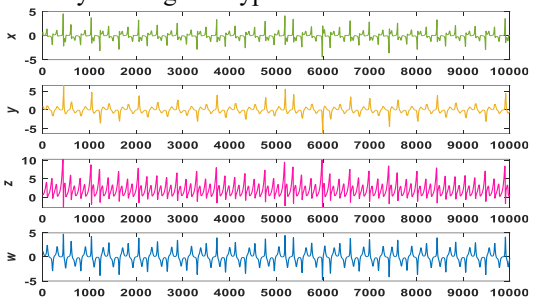
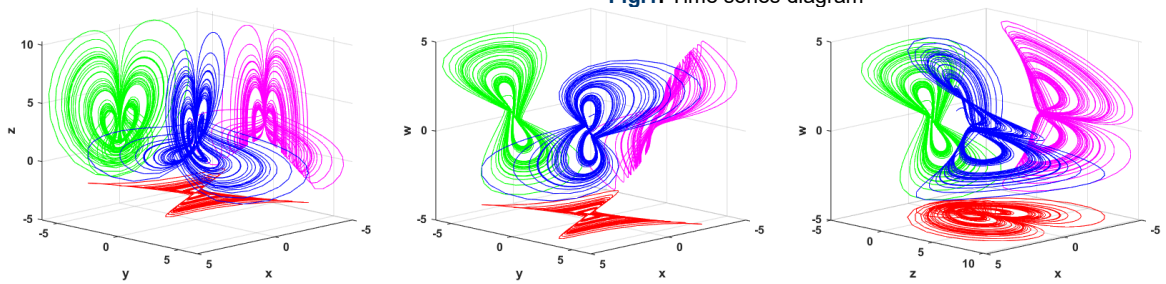
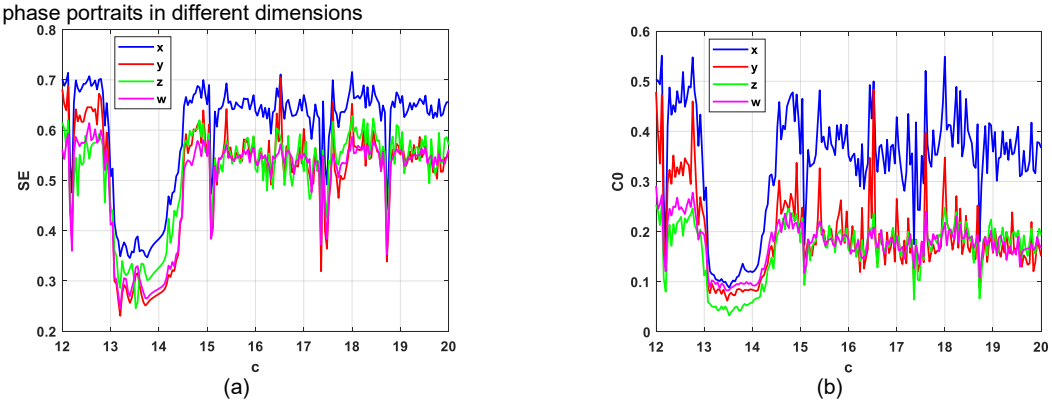


Fig.1. Time series diagram



(a) x-y-z dimensions (b) x-y-w dimensions (c) x-z-w dimensions

Fig.2. Attractor phase portraits in different dimensions



(a) (b)

Fig.3. (a) SE complexity diagram, (b) C0 complexity diagram

2.1.2 Dissipativity Analysis of the System.

The dissipativity of the system is expressed by Eq. (3):

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -a - ez + g - n \quad (3)$$

When $-a - ez + g - n = -54 - 11z < 0$, the phase volume of the system contracts exponentially at a rate of $e^{(-54-11z)}$. As time approaches infinity, any volume element containing the trajectory converges exponentially to zero. All orbits of the system are eventually confined to a limit set with zero volume, indicating that its asymptotic dynamical behavior condenses onto an attractor. This confirms the existence of a chaotic attractor in the system.

2.1.3 Equilibrium Points and Their Stability Analysis.

By setting $\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0$, the equilibrium points of the system can be derived as $(0,0,0,0)$, $(-\frac{\sqrt{5005}}{208}, -\frac{5\sqrt{5005}}{1144}, \frac{35}{24}, -\frac{2\sqrt{5005}}{143})$, and $(\frac{\sqrt{5005}}{208}, \frac{5\sqrt{5005}}{1144}, \frac{35}{24}, \frac{2\sqrt{5005}}{143})$. Linearizing the system near these equilibrium points yields the Jacobian matrix shown in Eq.(4).

$$J = \begin{bmatrix} -a & -b & cw & cz \\ dz & -ez & dx - ey & 0 \\ -fw & 0 & g & -fx \\ k & -m & 0 & -n \end{bmatrix} \quad (4)$$

To obtain the eigenvalues of the Jacobian matrix at the equilibrium points, let $|\lambda E - J| = 0$.

(1) Substituting the equilibrium point $(0,0,0,0)$ yields the characteristic equation as shown in Eq. (5).

$$\lambda(\lambda + a)(\lambda - g)(\lambda + n) = 0 \quad (5)$$

Based on the calculations, the obtained values are $\lambda_1=0,\ \lambda_2=-a,\ \lambda_3=g,\ \lambda_4=-n$, specifically $\lambda_1=0,\ \lambda_2=-50,\ \lambda_3=6,\ \lambda_4=-10$. According to the Routh–Hurwitz stability criterion, a necessary and sufficient condition for system stability is that the real parts of all eigenvalues are negative. Analysis of the eigenvalues λ_1、λ_2、λ_3、λ_4 shows that the system currently possesses eigenvalues with positive real parts. Therefore, this equilibrium point is unstable, indicating that the system may exhibit chaotic phenomena.

(2) Substituting the equilibrium points $(-\frac{\sqrt{5005}}{208},-\frac{5\sqrt{5005}}{1144},\frac{35}{24},-\frac{2\sqrt{5005}}{143})$ and $(-\frac{\sqrt{5005}}{208},-\frac{5\sqrt{5005}}{1144},\frac{35}{24},-\frac{2\sqrt{5005}}{143})$ yields eigenvalues $\lambda_1=-54.4264,\ \lambda_2=-17.3102,$ $\lambda_3=0.8475-11.3713i,\ \lambda_4=0.8475+11.3713i$.

Since the real parts of eigenvalues λ_3 and λ_4 are positive, according to the Routh–Hurwitz stability criterion, these equilibrium points are also unstable, indicating that the system may exhibit chaotic behavior.

2.2. Analysis of Stochastic Resonance Mode.

In this paper, a stochastic resonance system can be employed for signal denoising. As shown in Eq. (6), a stochastic resonance system with noise reduction capability is obtained by adjusting the parameters in Eq. (1).

$$\begin{cases}\dot{x}=-ax-by+czw+S(t)\\ \dot{y}=dxz-eyz\\ \dot{z}=-fxw+gz\\ \dot{w}=kx-my-nw\end{cases}\tag{6}$$

The first dimension is selected as the signal input terminal, where $S(t)$ denotes the noise-corrupted signal fed into the system. With parameters set as $a=1,b=-8,c=-12,$ $d=10,e=40,f=-90,g=-15,k=10,m=20,\ n=60$, the following analyses are conducted to validate the noise reduction performance of the stochastic resonance: equilibrium point curve analysis, potential function analysis, and sinusoidal signal denoising analysis.

2.2.1 Equilibrium Point Curve Analysis of the System.

When the stochastic resonance system represented by Eq.(6) is at the equilibrium point $(0,0,0,0)$, the relationship illustrated in Eq. (7) can be obtained.

$$\begin{cases}-ax-by+czw+S(t)=0\\ dxz-eyz=0\\ -fxw+gz=0\\ kx-my-nw=0\end{cases}\tag{7}$$

As shown in Eq. (8), y、z、w are expressed in terms of x.

$$y=\frac{d}{e}x,\ \ z=\frac{f(ek-md)}{gen}x^2,\ \ w=\frac{ek-md}{en}x\tag{8}$$

Substituting the relational expression given in Eq. (8) into $-ax-by+czw+S(t)=0$ yields the equilibrium equation for this stochastic resonance system, as shown in Eq. (9).

$$-ax-\frac{bd}{e}x+\frac{cf(ek-md)^2}{ge^2n^2}x^3+S(t)=0\tag{9}$$

Let $F(x)=-\frac{cf(ek-md)^2}{ge^2n^2}x^3+\frac{ae+bd}{e}x$. Then, $-F(x)+S(t)=0$, which implies that the intersection points of the equilibrium curve $F(x)$ and $S(t)$ correspond to the equilibrium points of this stochastic resonance system.

The schematic diagram of the input and output of the equilibrium points and the noise-containing signal in the x-dimension with the parameters incorporated is shown in Fig. 4, where the equilibrium point curve is given by Eq. (10).

$$F(x)=\frac{1}{2}x^3-x\tag{10}$$

The calculations yield the origin point $O(0,0)$, zero points $A(-\sqrt{2},0)$ and $B(\sqrt{2},0)$, a maximum point $C(-\frac{\sqrt{6}}{3},\frac{2\sqrt{6}}{9})$, and a minimum point $D(\frac{\sqrt{6}}{3},-\frac{2\sqrt{6}}{9})$.

Furthermore, as illustrated in Fig. 4, when $S(t)>\frac{2\sqrt{6}}{9}$ or $S(t)<-\frac{2\sqrt{6}}{9}$, the signal $S(t)$ intersects the curve $F(x)$ at only one point. When $S(t)=\frac{2\sqrt{6}}{9}$, it intersects $F(x)$ at points C and N. When $S(t)=-\frac{2\sqrt{6}}{9}$, the intersection occurs at points D and M. For $-\frac{2\sqrt{6}}{9}<S(t)<\frac{2\sqrt{6}}{9}$, $S(t)$ intersects $F(x)$ at three distinct points.

As shown in Fig. 4 and Eq. (11), when the stochastic resonance system performs denoising, the input $F(x)$ value yields the corresponding output x value. When stochastic resonance phenomenon occurs, the ratio of output signal to input signal is set as the system output gain φ.

$$\frac{1}{\varphi}=\frac{F(x)}{x}=\frac{\frac{1}{2}x^3-x}{x}=\frac{1}{2}x^2-1\tag{11}$$

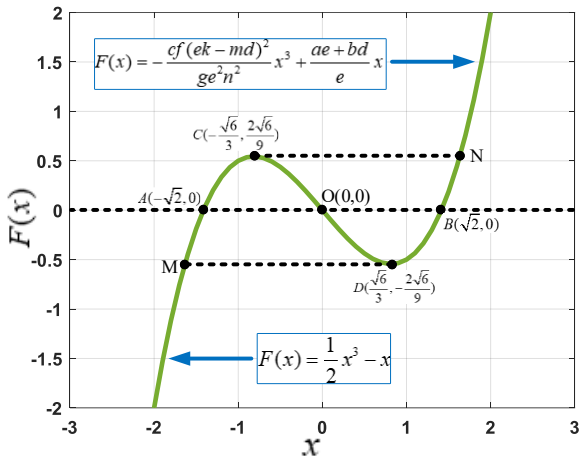


Fig.4. Schematic diagram of equilibrium points and input–output of noise-corrupted signals in the x-dimension

When $\varphi>1$, the amplitude of the output signal is greater than that of the input signal, and the input signal is enhanced. When $\varphi=1$, the amplitude of the input signal is equal to that of the output signal. When $\varphi<1$, output signal amplitude is less than the input signal amplitude, and the input signal is weakened.

However, since this study only requires the noise reduction capability of stochastic resonance, in order to enhance the image restoration effect, the x-value of the denoised and amplified signal is substituted back into Eq. (10) to obtain the corresponding $F(x)$ value, thereby restoring the signal gain effect.

2.2.2 Potential Function Analysis of the System.

The potential function $U(x)=\frac{1}{8}x^4-\frac{1}{2}x^2$ is derived from $F(x)=\frac{1}{2}x^3-x$ and is shown in Fig. 5. The potential function curve exhibits symmetric double-well characteristics. Calculations indicate that when $x=\pm\sqrt{2}$, the two local minima are located at $P(-\sqrt{2},-\frac{1}{2})$ and $Q(\sqrt{2},-\frac{1}{2})$, where the system is in a stable equilibrium state with a potential energy value of $U(\pm\sqrt{2})=-\frac{1}{2}$. The peak of the potential barrier between these two wells is situated at the origin $O(0,0)$, with a barrier height of $\Delta U=U(0)-U(\pm\sqrt{2})=\frac{1}{2}$.

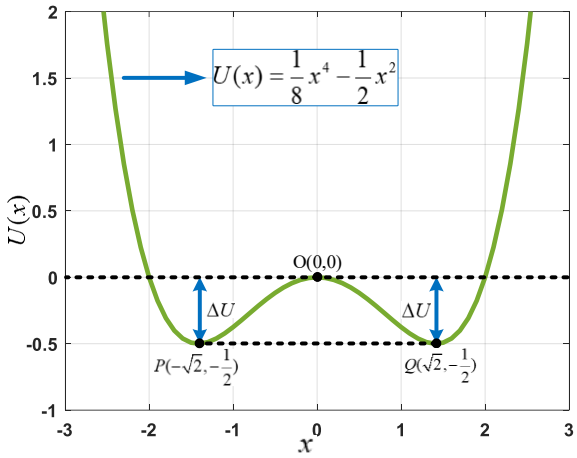


Fig.5. Potential function curve

When a noise-corrupted signal is input into this stochastic resonance system, the particle can convert noise energy into the driving force that enables the signal to cross the potential barrier. This process extracts and amplifies the weak signal component through nonlinear response, thereby achieving effective signal denoising.

3. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

As shown in Fig. 6, the image is first subjected to random-point scrambling, followed by diffusion using a Latin square matrix applied to the scrambled matrix to obtain the encrypted image. Finally, the decrypted image is recovered by reversing the encryption process.

Taking the 256×256 Magnolia image, the 256×256 House image, and the 512×512 Baboon image as examples, the feasibility of the scrambling and diffusion algorithms is individually verified.

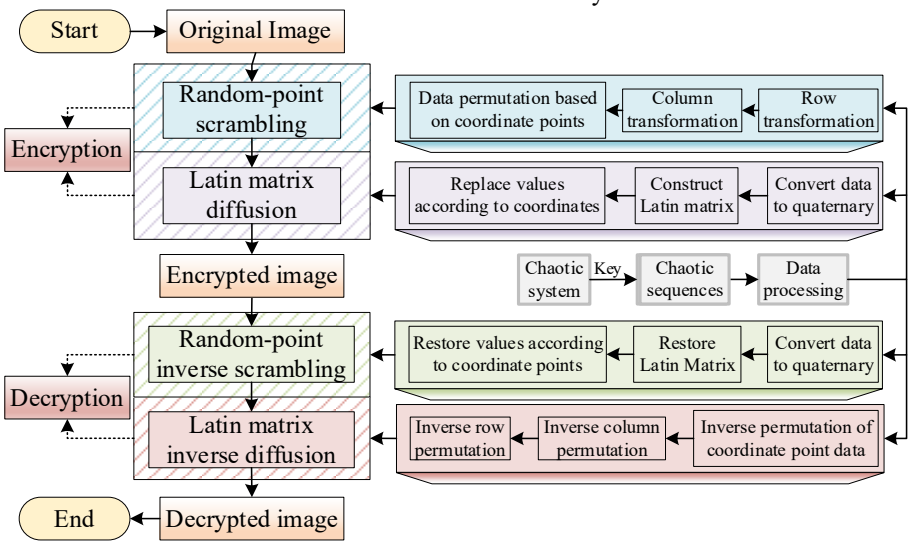


Fig.6. Flowchart of image encryption and decryption

3.1. Random-Point Scrambling.

Chaotic sequences exhibit high randomness. Leveraging this characteristic, the RGB three-layer matrices can first be randomly shuffled and mixed, followed by the random rearrangement of data within each layer matrix.

S1. Input an image matrix A of size $r \times c$, as given in Eq. (12), the chaotic sequences x, y, z, w are first quantized to the intervals $[1, r]$ and $[1, c]$. Two quantized sequences from different value ranges are randomly paired and then processed through cyclic-shift pairing, deduplication, and completion to generate two non-repeating coordinate sets R_1 and R_2, each forming a complete permutation of all $r \times c$ pixel positions.

$$\begin{aligned} I_i &= mod\left(floor\left(N \times 2^{16}\right), M\right) + 1 \\ R \leftarrow unique\left(\left[I_k', I_l'\right] \cup \left[I_k\left(u+1:end\right)', I_l\left(1:end-u\right)'\right]\right) & \\ k, l \in i, u = 1, 2, 3, \ldots & \end{aligned} \tag{12}$$

where i can individually take the values 1,2,3,4. N can represent x, y, z, w, and M can denote r or c.

S2. After decomposing the RGB layers of the original image, the three-layer matrices are first folded left and right. Following the row-column transformation rules presented in Table 1, row transformations are performed based on the random point count I_r. Subsequently, the transformed layer matrices are folded top and bottom, and column transformations are applied according to the random point count I_c.

$$\begin{aligned} I &= mod\left(floor\left(x \times 2^{16}\right), 3\right) \\ I_r &= I(1:r), \quad I_c = I(r+1:r+c) \end{aligned} \tag{13}$$

TABLE 1. Row-column transformation rules

Value of I	0	1	2
Row transformation	Unchanged	←	→
Column transformation	Unchanged	↑	↓

where "←、→、↑、↓" indicates the direction of the row-column transformation. As illustrated in Fig. 7, the matrix transformation is demonstrated using $I = [0\ 1\ 2\ 0\ 1\ 2]$ as an example.

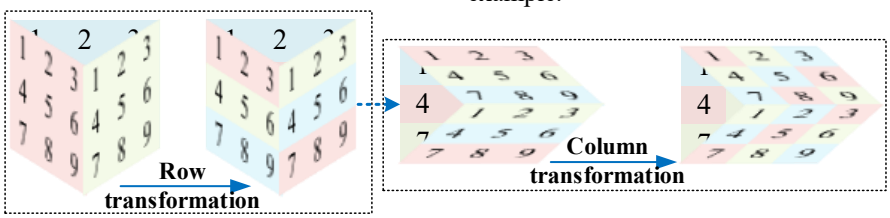


Fig.7. Example diagram of row-column transformation

S3. Extract the data from the row–column positions corresponding to R_1 sequentially and store them in a one-dimensional matrix B. Then, place B into matrix C according to the order specified by R_2, resulting in a scrambled matrix C of size $r \times c$. As shown in Fig. 8, the random-point scrambling process is illustrated using $R_1 = [1,2|2,2|2,1|1,1]$ and $R_2 = [2,1|1,2|1,1|2,2]$ as examples.

As shown in Fig. 9, the experimental results of the random-point scrambling algorithm demonstrate that no characteristic information of the original image is discernible in the scrambled output. The scrambled image exhibits a highly random distribution of noise, effectively severing visual correlation with the original image. This ensures the concealment and security of the image information.

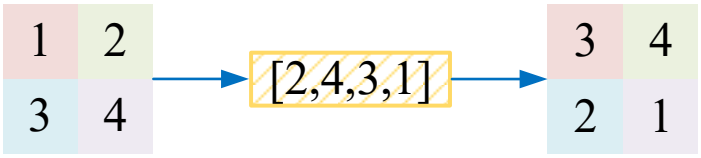


Fig.8. Example diagram of random coordinate permutation

(a) (b) (c)

(d) (e) (f)

Fig.9. (a) Original Magnolia image. (b) Original House image. (c) Original Baboon image. (d), (e), (f) represent the results of applying the random-point scrambling algorithm to images (a), (b), and (c), respectively

3.2. Latin Matrix Diffusion.

T1. Input matrix C, and preprocess chaotic sequences x, y of length $r \times c \times 4$ according to Eq. (14) to obtain I_5 and I_6 with a value range of $[0,3]$.

$$\begin{aligned} I_5 &= mod\left(floor\left(x \times 2^{16}\right),4\right); \\ I_6 &= mod\left(floor\left(y \times 2^{16}\right),4\right); \end{aligned} \tag{14}$$

T2. Traverse matrix I_5 sequentially until a one-dimensional matrix D of size 1×4 containing only distinct numerical values is stored. Then, perform a planar addition of 1 and a spatial addition of 1 on matrix D to obtain a Latin matrix E of size $4 \times 4 \times 4$ with a value range of $[0,3]$.

Taking the one-dimensional matrix $D = [0\ 2\ 3\ 1]$ as an example, planar and spatial addition operations (i.e., $0 \to 1,\ 1 \to 2,\ 2 \to 3,\ 3 \to 1$) are performed to obtain a $4 \times 4 \times 4$ Latin matrix

$$E = \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 2 & 3 & 1 & 1 & 3 & 0 & 2 & 2 & 0 & 1 & 3 & 3 & 1 & 2 & 0 \\ 1 & 3 & 0 & 2 & 2 & 0 & 1 & 3 & 3 & 1 & 2 & 0 & 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 & 3 & 1 & 2 & 0 & 0 & 2 & 3 & 1 & 1 & 3 & 0 & 2 \\ 3 & 1 & 2 & 0 & 0 & 2 & 3 & 1 & 1 & 3 & 0 & 2 & 2 & 0 & 1 & 3 \end{array}\right],$$

which can be represented as the cubic diagram shown in Fig.10.

T3. Convert matrix C into a one-dimensional matrix F, and transform its values from decimal to quaternary representation to obtain a one-dimensional matrix G of size $1 \times (4 \times r \times c)$.

T4. Map the values of I_5 to the x-axis in Fig. 10, the values of I_6 to the y-axis, and the values of matrix G to the z-axis. As shown in Eq. (15), the corresponding new values H_h can be obtained to achieve data diffusion.

$$H_h = (x_h, y_h, z_h), h \in (1,2,...,4 \times r \times c) \tag{15}$$

T5. The channel values are extracted from the three-dimensional point set H_h and converted from quaternary to decimal representation, yielding the components R', G', B'. To enhance pixel-wise correlations, GF(257) field multiplication is applied to each component, followed by spatial reassembly into the encrypted matrix J of size $r \times c$.

As shown in Fig. 11, the experimental results of the Latin matrix diffusion algorithm demonstrate that the diffused image exhibits a noise-like distribution. The contours, textures, and structural features present in the original image are completely disrupted, effectively breaking the spatial correlation among image pixels. This ensures randomness and uniformity in the statistical characteristics.

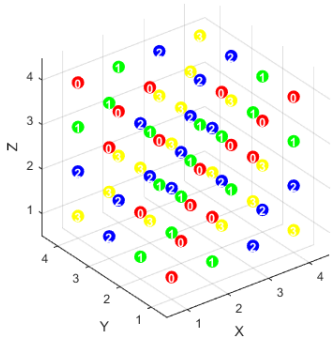
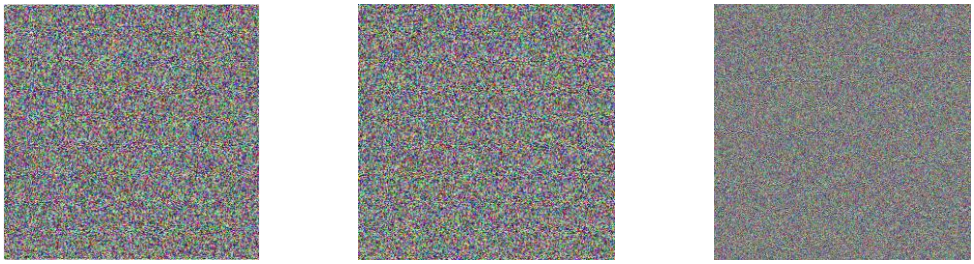


Fig.10. Cubic coordinate diagram of the Latin matrix E

(a) (b) (c)



(d) (e) (f)

Fig.11. (a) Original Magnolia image. (b) Original House image. (c) Original Baboon image (d), (e), (f) show the results of applying the Latin matrix diffusion algorithm to images (a), (b), and (c), respective

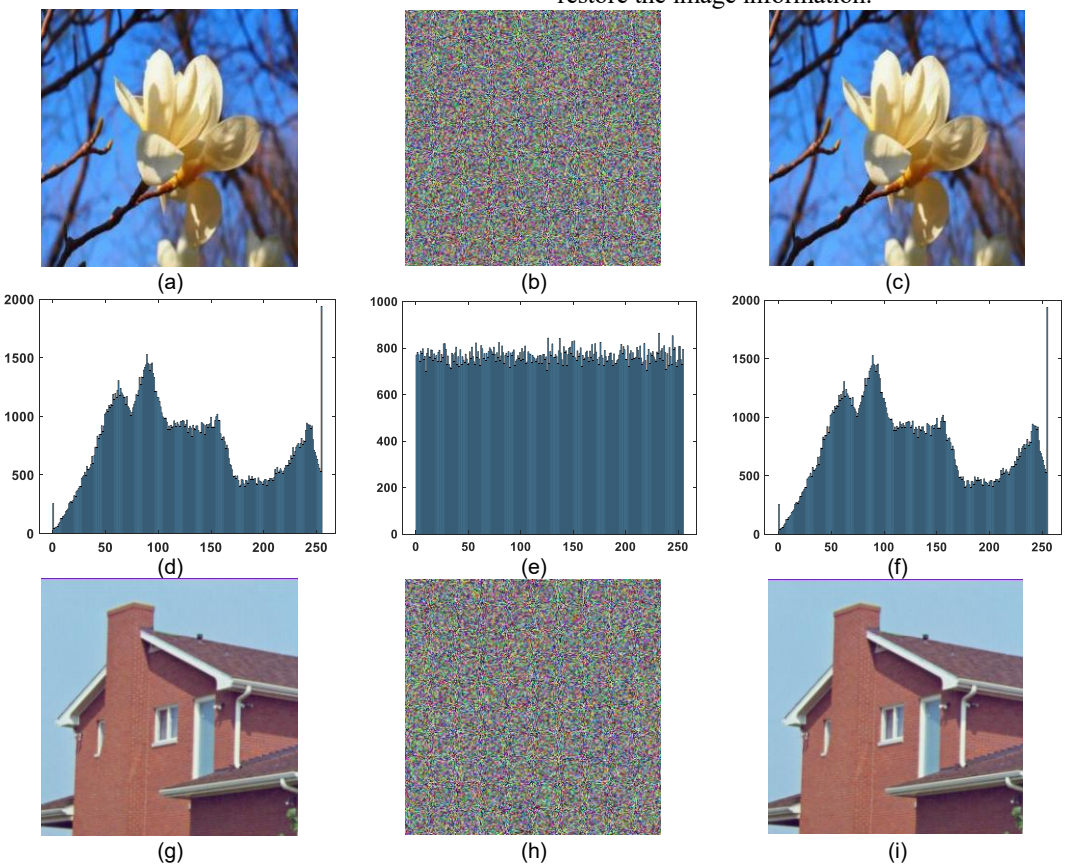
4. SECURITY ANALYSIS OF IMAGE ENCRYPTION AND DECRYPTION

To verify the communication confidentiality of the algorithm, image encryption and decryption experiments were conducted using a 256×256 Magnolia image, a 256×256 House image, and a 512×512 Baboon image. The results and analysis are presented below.

4.1. Image Encryption and Decryption with Histogram Analysis.

As shown in Fig. 12, the original, encrypted, and decrypted images of the Magnolia, House, and Baboon images are presented, along with their corresponding histograms.

From Fig. 12, it can be observed that the encrypted image is entirely different from the original image. In terms of histogram statistics, the original image exhibits multiple distinct peaks and fluctuations in its pixel value distribution, whereas the encrypted image shows an approximately uniform distribution. This indicates that the pixel value information has been effectively concealed, enabling resistance against analysis attacks based on statistical characteristics. Furthermore, comparing the original image with the decrypted image reveals that the decrypted image displays the same characteristic information as the original, and their histogram distributions are highly consistent. This demonstrates that the encryption algorithm possesses good reversibility and can accurately restore the image information.



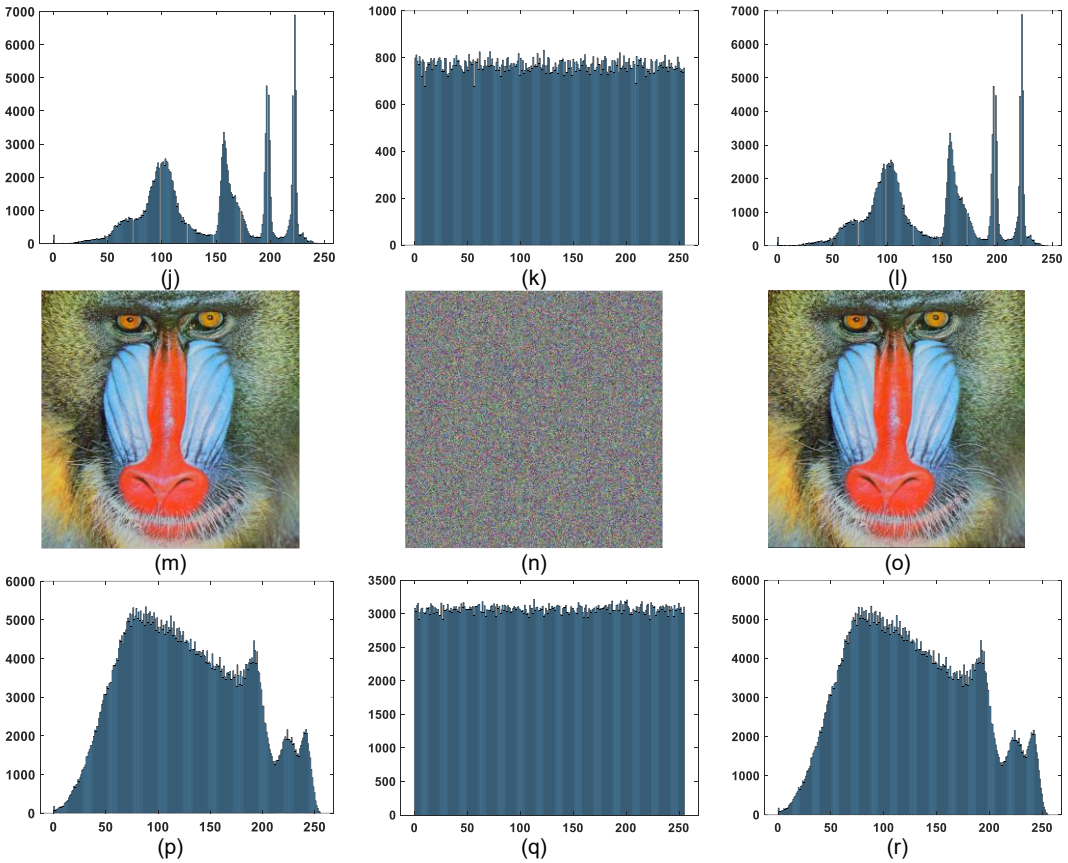
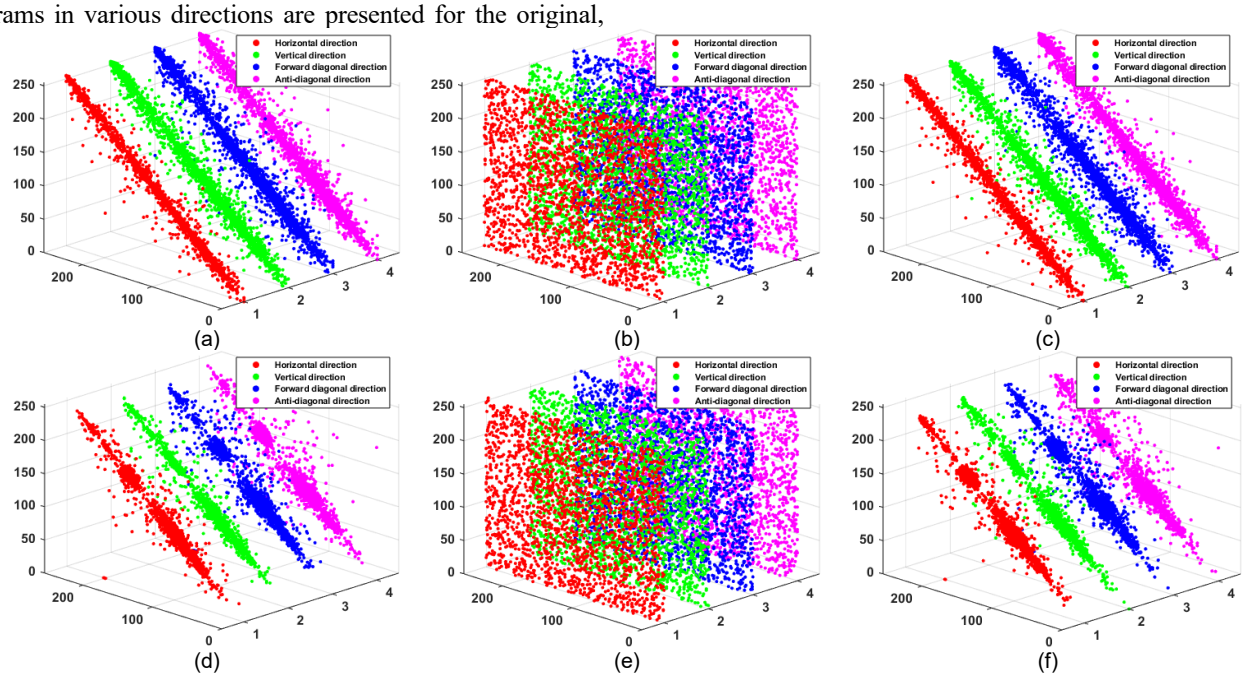


Fig.12. Left to right: Original (a, g, m), encrypted (b, h, n), and decrypted (c, i, o) images of Magnolia, House, and Baboon. Below each image row are the corresponding histograms (d–f, j–l, p–r)

4.2. Correlation Coefficient Analysis.

As shown in Fig. 13, correlation coefficient analysis diagrams in various directions are presented for the original, encrypted, and decrypted images of the Magnolia, House, and Baboon images.



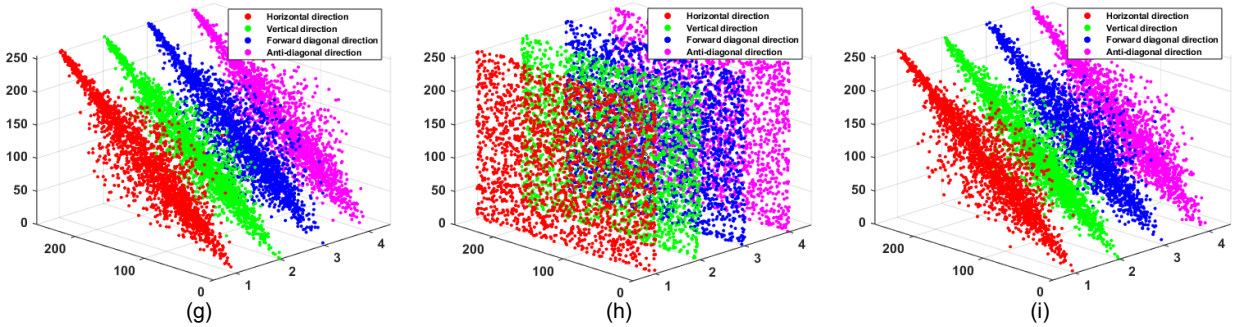


Fig.13. Correlation plots for original (a, d, g), encrypted (b, e, h), and decrypted (c, f, i) images of Magnolia, House, and Baboon along horizontal, vertical, forward-diagonal, and backward-diagonal directions.

TABLE 2. Correlation coefficients of original, encrypted, and decrypted images

Image	r1	r2	r3
Magnolia	0.9857, 0.9776, 0.9625, 0.9762	0.0234, -0.0029, 0.0276, 0.0007	0.9849, 0.9773, 0.9635, 0.9755
House	0.9578, 0.9803, 0.9287, 0.9418	0.0139, 0.0100, -0.0014, -0.0056	0.9617, 0.9731, 0.9399, 0.9484
Baboon	0.8536, 0.9024, 0.8177, 0.8252	-0.0307, 0.0042, 0.0031, -0.0338	0.8300, 0.9095, 0.8043, 0.8281

As shown in Table 2, the correlation coefficients for the Magnolia, House, and Baboon images are listed, where r1 corresponds to the original images, r2 to the encrypted images, and r3 to the decrypted images.

From Fig. 13 and Table 2, it can be observed that the correlation coefficient points of the original and decrypted images are densely distributed near the diagonal line, indicating a high degree of correlation. In contrast, the correlation coefficient points of the encrypted images exhibit a uniform distribution, with the values of r2 in all directions approaching zero. This reflects a significant reduction in pixel correlation after encryption, demonstrating strong statistical security.

4.3. Entropy Analysis.

As shown in Table 3, the entropy values for the Magnolia, House, and Baboon images are listed, where H1 corresponds to the original images, H2 to the encrypted images, and H3 to the decrypted images.

TABLE 3. Entropy values of original, encrypted, and decrypted images

Image	H1	H2	H3
Magnolia	7.8492	7.9990	7.8492
House	7.0686	7.9992	7.0686
Baboon	7.7624	7.9998	7.7624

Based on the numerical results, all three H2 values are close to the ideal value of 8, indicating that the pixel value distribution of the encrypted images exhibits near-ideal randomness. This reflects the algorithm's strong encryption effectiveness at the information entropy level. Furthermore, the information entropy values of the original and decrypted images correspond one-to-one, demonstrating that the image information can be fully restored. This confirms the algorithm's excellent decryption performance.

4.4. Key Sensitivity Analysis.

As shown in Fig. 14, the original images, encrypted images, and decrypted images using modified keys are presented for the Magnolia, House, and Baboon images, respectively.

As shown in Fig. 14, when only the first digit of the initial key is slightly perturbed, changing it from $[1\ 1\ 1\ 1]$ to $[1+1*10^{-14}\ 1\ 1\ 1]$, the original image cannot be decrypted at all. This demonstrates that the algorithm is highly sensitive to the key, as even an extremely minor alteration results in decryption failure, thereby confirming the algorithm's strong confidentiality and key sensitivity.

4.5. Damage Attack Analysis.

As shown in Fig. 15, the robustness of the proposed encryption algorithm against cropping attacks is systematically evaluated using the Magnolia image as a representative case.

Specifically, images (b) and (e) correspond to 25% and 50% area cropping, respectively. By comparing the decrypted results in images (c) and (f), it can be observed that the image quality gradually deteriorates as the cropping proportion increases. Nevertheless, the primary structural features and key visual information remain clearly discernible in both cases.

These findings demonstrate that the proposed algorithm exhibits strong robustness against image data loss and maintains high resilience to cropping attacks, thereby ensuring reliable decryption performance even under moderate to severe cropping conditions.

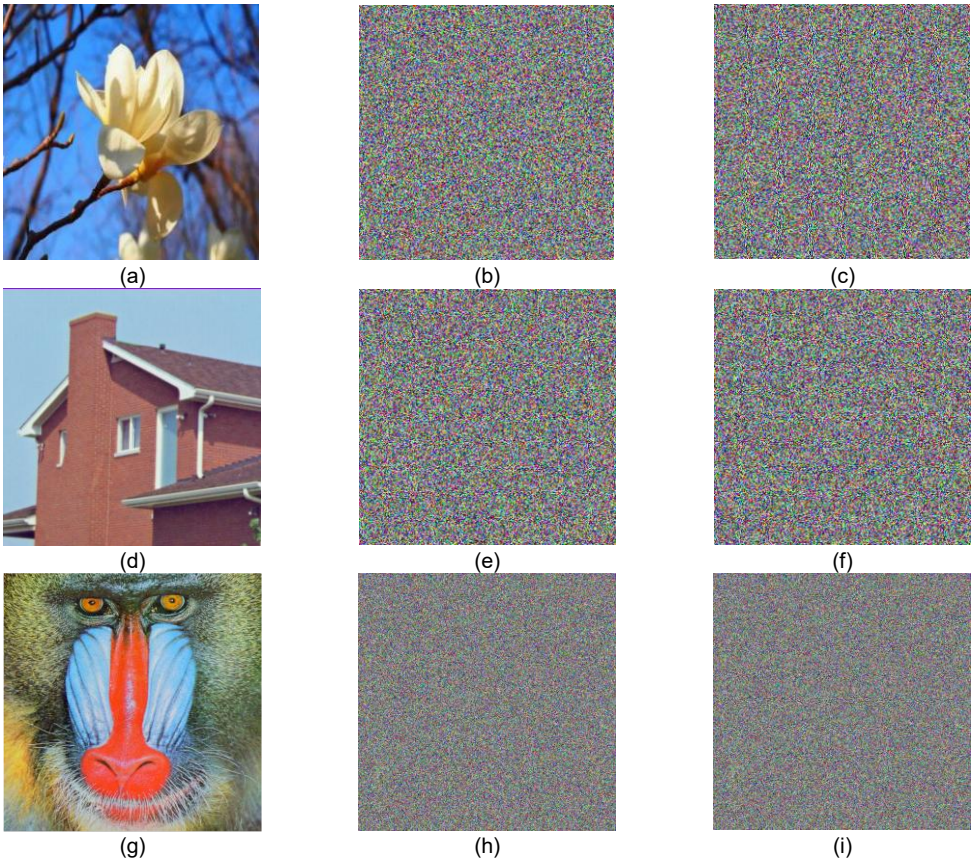


Fig.14. Original (a, d, g), encrypted (b, e, h), and decrypted-with-modified-key (c, f, i) images for Magnolia, House, and Baboon, respectively.

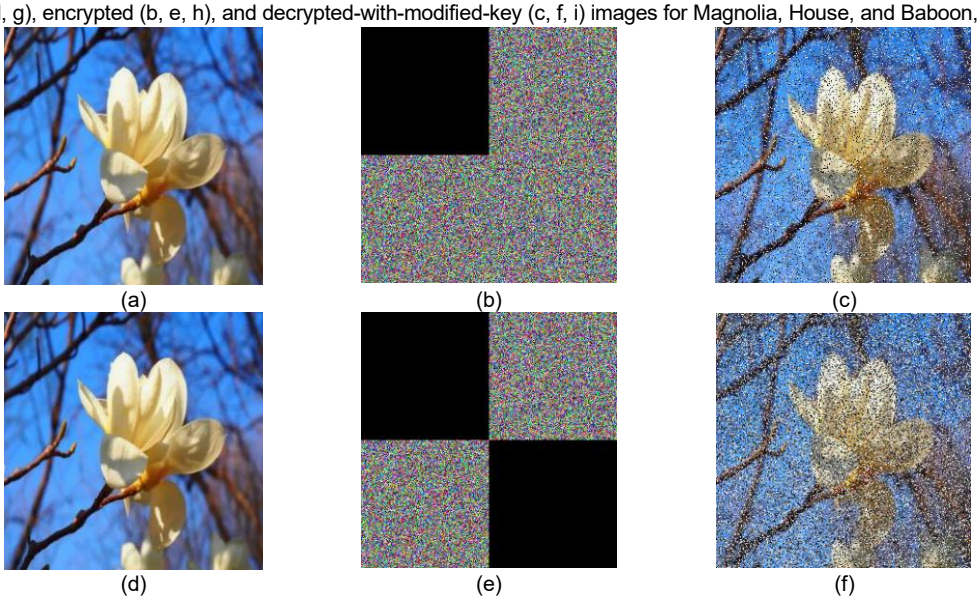


Fig.15. Magnolia image: original (a, d), encrypted with 1/4 damage (b), encrypted with 1/2 damage (e), and corresponding decrypted images (c, f).

4.6. .Encryption quality analysis.

Three commonly used metrics, namely MSE, PSNR, and SSIM, are adopted to evaluate the encryption quality. MSE quantifies the average squared difference between pixel values of two images, with larger values indicating more significant discrepancies. PSNR, derived from MSE, is a widely recognized measure of image fidelity, and for high-quality encrypted images, PSNR values are generally expected to remain below 10 dB. SSIM measures the structural similarity between images, yielding a value of 1 for identical images and approaching 0 for completely different ones.

The results presented in Table 4 demonstrate that, across all RGB channels, the encrypted images exhibit high MSE, PSNR below 10 dB, and SSIM close to 0. These quantitative results confirm that the encrypted images differ substantially from the original images with negligible structural similarity, thereby fully demonstrating the excellent encryption performance of the proposed system.

TABLE 4. Encryption quality results

Image	MSE			PSNR(dB)			SSIM		
	R	G	B	R	G	B	R	G	B
Magnolia	9485	8040	11880	8.3603	9.0782	7.3828	0.0087	0.0094	0.0096
House	6892	8609	9559	9.7474	8.7812	8.3268	0.0096	0.0100	0.0102
Baboon	8653	7773	9485	8.7589	9.2247	8.3602	0.0092	0.0076	0.0066

4.7. Differential attack test.

Differential attack is a common cryptanalysis technique in which an attacker introduces a minor modification—typically altering a single pixel value—to a plaintext image and encrypts both the original and modified versions. By comparing the resulting ciphertext images, the attacker seeks to identify statistical patterns or correlations that could reveal vulnerabilities in the encryption system. To quantitatively assess the resistance against such attacks, two widely recognized metrics are employed: NPCR and UACI. For two images P_1 and P_2 of size $M \times N$, the corresponding formulas for NPCR and UACI are presented in Eq. (16).

TABLE 5. Results of differential attack tests

Image	NPCR	UACI
Magnolia	99.4998%	33.4852%
House	99.5806%	33.5546%
Baboon	99.5833%	33.2293%

$$NPCR(P_1,P_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|Sign(P_1(i,j)-P_2(i,j)\right|\times 100\% \quad (16)$$
$$UACI(P_1,P_2)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{\left|P_1(i-j)-P_2(i-j)\right|}{255-0}\times 100\%$$

where $P_1(i,j)$ and $P_2(i,j)$ denote the coordinates (i,j) of any pixel in images P_1 and P_2, and $Sign(\cdot)$ is the sign function, $Sign(x)=\begin{cases}1, & x>0\\ 0, & x=0\\ -1, & x<0\end{cases}$.

The experimental results in Table 5 demonstrate that two ciphertext images derived from slightly different plaintext images exhibit substantial differences. The computed NPCR and UACI values are close to the theoretical ideals of 99.6094% and 33.4635%, respectively. These findings confirm that the proposed encryption scheme is robust against differential attacks.

4.8. Comparison of encryption performance.

The Baboon image, a commonly used test image in encryption experiments, is encrypted using the proposed algorithm. To evaluate the encryption performance, several metrics including NPCR, UACI, information entropy, MSE, PSNR, and correlation coefficients are calculated and compared with those of the algorithms reported in Ref. [21–25]. The corresponding numerical results are presented in Table 6.

As shown in Table 6, the information entropy of the proposed algorithm reaches 7.9993, approaching the theoretical maximum of 8 and slightly higher than that of [21–24]. The NPCR is 99.5833% and the UACI reaches 33.5546%, both close to the theoretical ideal values, indicating that the algorithm is highly sensitive to plaintext. Moreover, all compared algorithms yield low correlation coefficients in all three directions. The proposed algorithm, together with those in Ref. [24–25], achieves relatively high MSE values, and the PSNR values of the algorithms in Ref. [21, 24–25] and the proposed algorithm remain below 10 dB. These results demonstrate that the proposed encryption algorithm exhibits favorable encryption performance and security.

TABLE 6. Comparison of the proposed algorithm with other algorithms in the literature for Baboon image encryption.

Baboon	Information entropy	MSE	PSNR	NPCR	UACI	correlation coefficients			
						Horizontal	Vertical	Diagonal	Back-diagonal
Proposed algorithm	7.9998	R:9485 G:8040 B:11880	R:8.3603 G:9.0782 B:7.3828	99.5833%	33.2293%	-0.0307	0.0042	0.0031	-0.0338
Ref. [21]	7.999301	—	9.5322	99.6016	33.4039%	-0.014340	0.011214	0.001345	—
Ref. [22]	7.9993	—	—	99.6009	33.4709%	0.002155	0.000515	0.000555	—
Ref. [23]	7.9994	—	—	—	—	-0.0043	-0.0036	-0,0044	—
Ref. [24]	7.99902	8291.16	8.94465	99.6089	29.4430%	0.00152662	-0.00774664	0.00793051	—
Ref. [25]	7.9998	R:8678 G:10708 B:8719	R:8.13 G:7.83 B:8.72	99.5040%	33.7267%	0.0007	0.0022	−0.0029	−0.0001

4.9. Time efficiency analysis.

In the proposed encryption scheme, implemented in MATLAB R2022b, the encryption algorithms consume 1.147219 seconds, respectively, using a 256×256×3 House image as an example.

TABLE 7. Time test results (s)

256×256	Encryption time	Machine Specifications (CPU and RAM)
Proposed	1.147219	3.80 GHz AMD R7 7700, 32 GB
Ref. [22]	0.9654	3.20 GHz AMD R7 5800H, 16 GB
Ref. [26]	2.582389	2.9 GHz Intel® Core™ i9, 32 GB
Ref. [27]	3.702	N/A
Ref. [28]	2.750966	3.4 GHz Intel® Core™ i7, 8 GB

As shown in Table 7, the proposed algorithm achieves high encryption efficiency without compromising security, rendering it well-suited for real-time image encryption applications. Moreover, in comparison with the methods reported in Ref. [26–28], our algorithm exhibits a distinct advantage in encryption speed, further attesting to its effectiveness and practicality in terms of computational efficiency.

5. STOCHASTIC RESONANCE DENOISING AND INTEGRAL RESTORATION ALGORITHM

When communication operates under high real-time requirements, faces extremely limited communication resources, encounters unreliable links, or is subjected to active attacks, leading to large-scale image damage and massive data loss, the stochastic resonance mode of the nonlinear system proposed in this paper is employed to design a stochastic resonance denoising and integral restoration method that resists attacks during the encryption-decryption process.

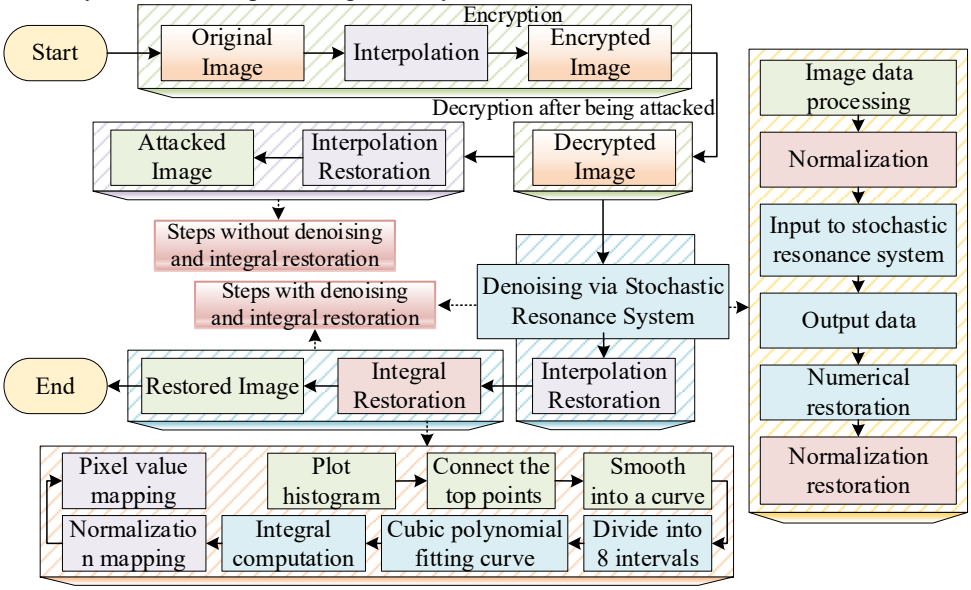


Fig.16. Basic flowchart of denoising and integral restoration

As shown in Fig. 16, to prevent image data from being treated as noise by stochastic resonance, the original image is first upscaled by a factor of 100 through interpolation before encryption. After the data suffers from attacks during transmission, the damaged image information is input into the x-dimension of the stochastic resonance system described by Eq.(6) with tuned parameters. At this stage, most of the noise has been filtered out, but the image information remains insufficiently clear. To address this issue, an integral restoration algorithm is introduced: the denoised image is first downscaled to its original size via interpolation, and then its histogram is used to plot a top envelope curve. This curve is divided into eight segments, each of which undergoes integral processing to generate a piecewise integral restoration curve. This operation enhances the clarity and prominence of the image's characteristic information. The following experiment is conducted using a 128 × 128 Magnolia image as an example.

5.1. Denoising with the Stochastic Resonance System.

Stochastic resonance can denoise noisy signals. This paper applies it to the recovery experiment of attacked images in the chaotic encryption and decryption process. The detailed restoration algorithm flow is illustrated in Fig. 16.

5.1.1 Algorithm Steps.

E1. Set the interpolation factor to 100. Expand the signal of the original image using linear interpolation, then perform encryption and decryption operations. If the transmission suffers from a large-scale attack, process the data of the decrypted image before interpolation restoration into a one-dimensional matrix, normalize the data to the range $[-1,1]$, and input it into the x-dimension of the system for denoising.

E2. Map the output data back to their original magnitude prior to numerical amplification by the stochastic resonance system using the curve $F(x)=\frac{1}{2}x^3-x$, thereby retaining only the denoising effect of the stochastic resonance system.

E3. The values restored by the curve are normalized to the range $[0,255]$, followed by interpolation-based reconstruction, and finally reassembled to form the required denoised image.

5.1.2 Image Signal Denoising Experiment.

As shown in Fig. 17, the image data are converted into signals for the experiment. The signal in (a) suffers from a 50% regional data attack during the encryption–decryption transmission process, resulting in the noisy signal shown in (b). After normalization, this signal is input into the system for denoising and then normalized back to obtain the signal displayed in (c).

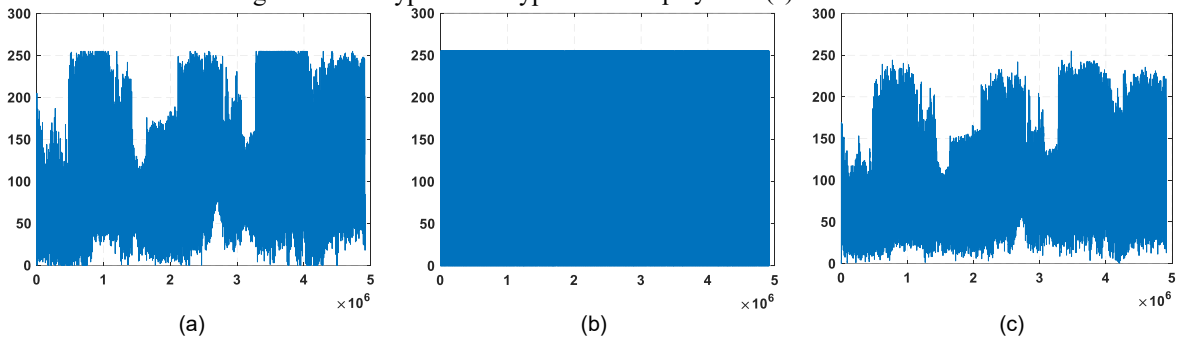


Fig.17. Signal plots: (a) interpolated original image, (b) decrypted signal after 50% area attack, (c) denoised signal via stochastic resonance

From Fig. 17, it can be observed that the noise signal in (b) is so dense that it almost completely obscures the data information of the original image. However, after denoising by the system, the signal in (c) exhibits a high degree of numerical agreement with the interpolated original signal shown in (a).

As shown in Fig. 18, subfigure (b) corresponds to (a) in Fig. 17, and subfigure (d) corresponds to (b) in Fig. 17. The original image (a) is transformed into (b) after interpolation. (b) is then encrypted and subjected to a 50% area attack during transmission, resulting in (c). (c) is decrypted to yield (d). Without denoising, (d) is directly restored through interpolation, yielding the noise-containing decrypted image (e). In contrast, after denoising via the stochastic resonance system followed by interpolation-based restoration, (d) is converted into the denoised decrypted image (f).

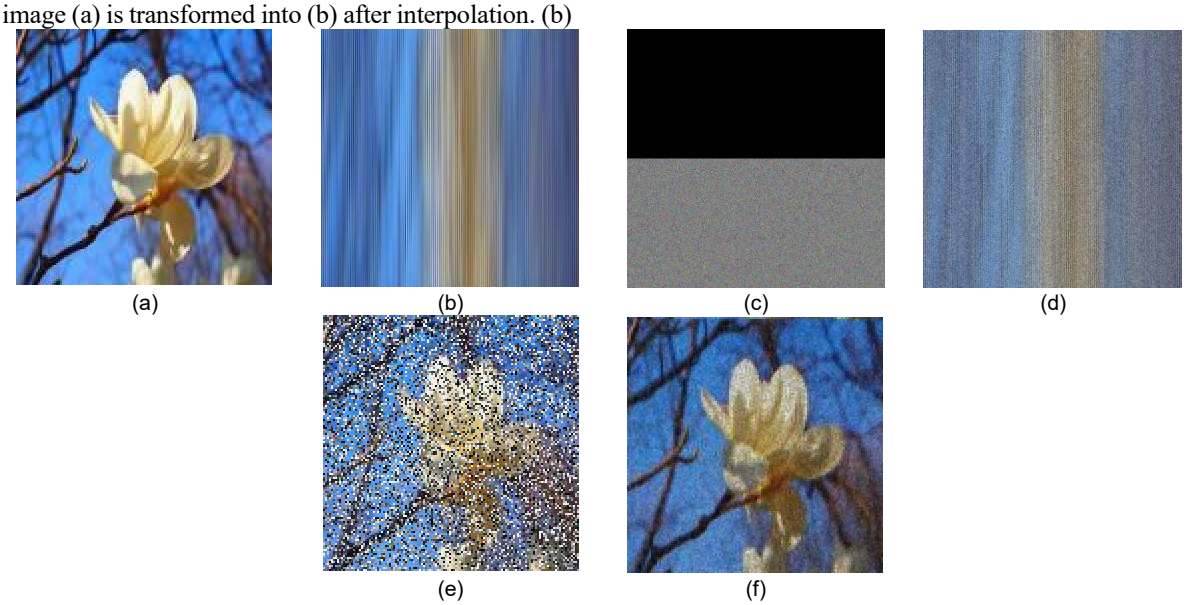


Fig.18. (a) Original. (b) Interpolated (for encryption). (c) Encrypted (50% area attacked). (d) Decrypted. (e) Decrypted via interpolation-based restoration. (f) Decrypted with stochastic-resonance denoising and interpolation-based restoration

Comparing (e) and (f) in Fig. 17, it is demonstrated that when 50% of the area suffers from attacks during chaotic encryption-decryption transmission, the application of the stochastic resonance system can effectively denoise and restore most of the characteristic information of the image.

5.2. Integral Restoration Algorithm.

From the histogram presented in Fig. 19(a), the distribution range of image pixel values can be observed. Utilizing this characteristic, the clustered pixel values can be dispersed, thereby making certain feature information of the image more prominent and easier to discern. The detailed restoration algorithm flow is illustrated in Fig. 16.

5.2.1 Algorithm Steps.

P1. Obtain the histogram corresponding to the image, connect the top points of the histogram, and smooth them into a curve.

P2. Evenly divide the curve into 8 subintervals, and within each interval, perform least-squares fitting to obtain a cubic polynomial curve as shown in Fig. 19(b), thereby accurately describing the distribution characteristics of the histogram. Subsequently, integrate each segmented polynomial and adjust the integration constants to ensure continuity at the boundaries between adjacent segments, resulting in a smooth integral curve as illustrated in Fig. 19(c).

P3. Perform global normalization on the integral curve, mapping it entirely to the range $[0, 255]$ that meets the requirements for image pixel values. Then, based on the piecewise continuous transformation function, transform each pixel value of the image according to the mapping relationship to the corresponding numerical value, and finally reconstruct and output the image.

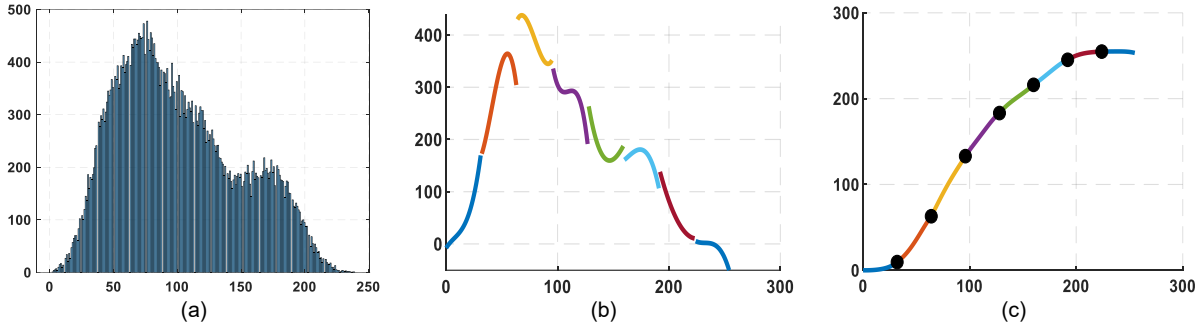


Fig.19. (a) Histogram of the image to be restored. (b) cubic polynomial fitting curve based on (a). (c) integral curve of (b)

5.2.2 Integral Restoration Algorithm Experiment.

As shown in Fig. 20, subfigure (c) corresponds to Fig. 18(f). By applying integral restoration to (c) and comparing (a), (c), and (d), it can be observed that the dark and blurred regions in (c) reveal more characteristic information in (d), with color boundaries also appearing more distinct and clear.

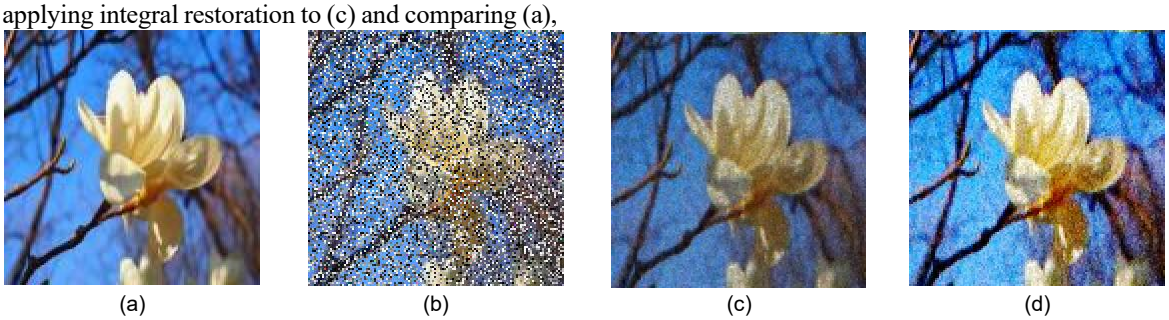


Fig.20. (a) Original, (b) Noisy (unrestored), (c) Denoised only, (d) Denoised and integral restored

By comparing Fig. 20(a), (b) (which corresponds to Fig. 18(e)), and (d), it can be observed that (d) reveals more characteristic information of (a) than (b), indicating the effectiveness of the restoration process.

5.3. Comparative Experiments.

To validate the performance of the denoising and restoration algorithm in recovering images subjected to different large-area attacks during chaotic encryption and decryption, a comparative experiment was conducted.

5.3.1 Experimental Visualization Results.

As shown in Fig. 21, using the House image as an example, the encrypted images with attacked area ratios ranging from 75% to 95% are presented. The decrypted images under various levels of data loss were then subjected to denoising and restoration. The experimental results for the Magnolia, House, and Baboon images are shown in Figs. 22–26, respectively.

It can be observed that images (b) in Figs. 22–26 obscure most of the characteristic information of the image. As the attacked area increases, the amount of concealed information also rises. Correspondingly, the available normal pixel data for restoration in images (c) and (d) of Figs. 22–26 gradually decreases. However, comparing (b) with (d) across Figs. 22–26, more characteristic information of (a) can be discerned in (d), whereas (b) reveals little or even none of such information. This indicates that when large-area attacks occur during chaotic encryption and decryption, the proposed denoising and restoration algorithm can effectively recover characteristic information that is otherwise obscured by noise.

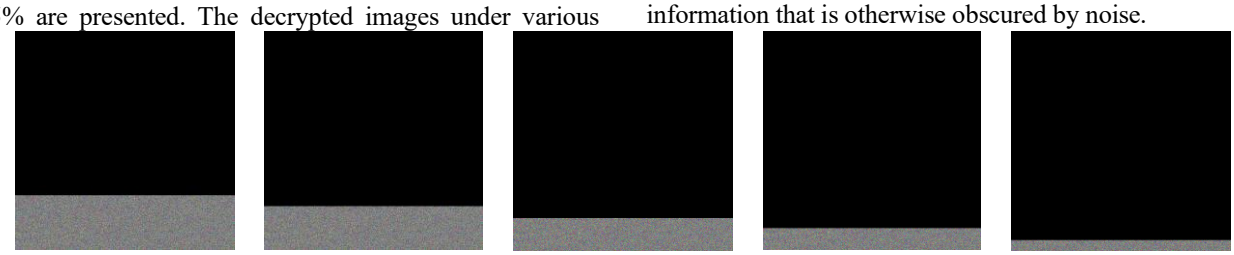


Fig.21. Encrypted images under different attacked area ratios: (a) 75%, (b) 80%, (c) 85%, (d) 90%, and (e) 95%

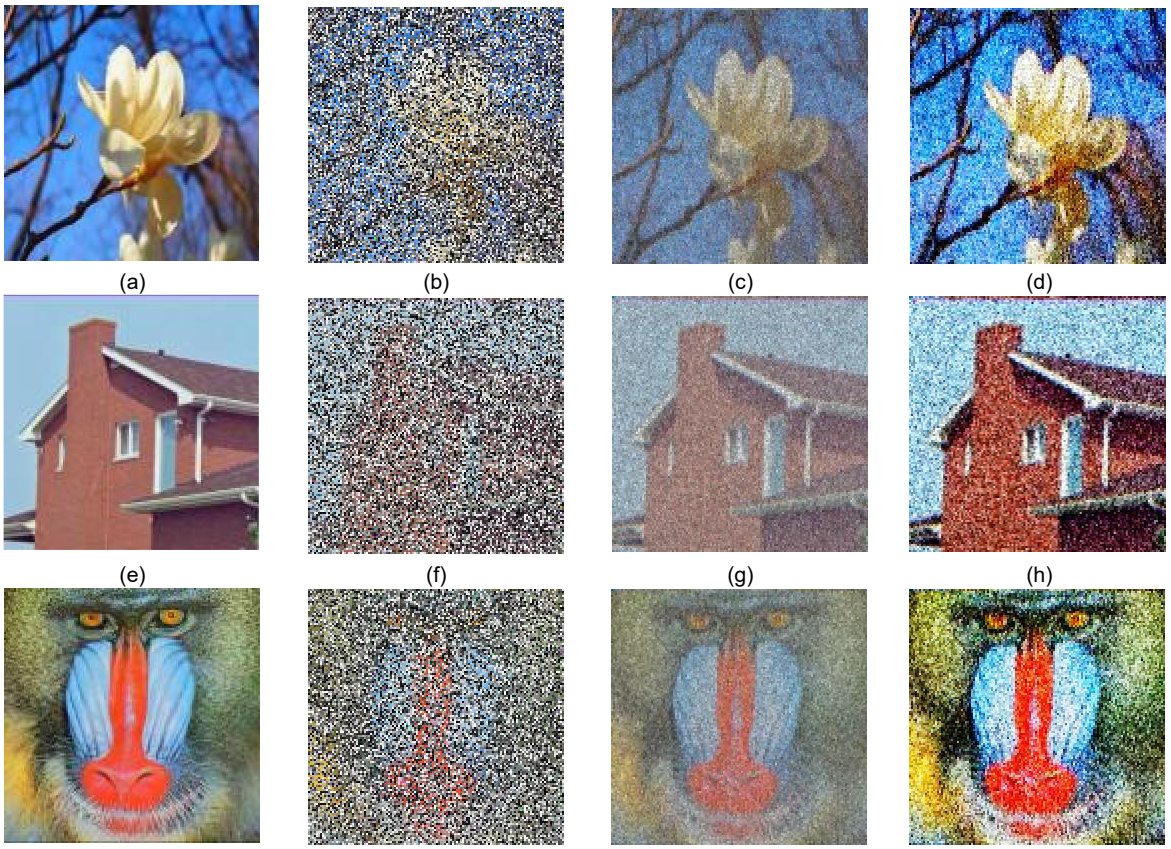


Fig.22. Restoration performance under 75% data loss: Magnolia: (a) Original. (b) Decrypted & only interpolation-restored. (c) Decrypted, denoised & interpolation-restored. (d) Integral restoration of (c). House: (e) Original. (f) Decrypted & only interpolation-restored. (g) Decrypted, denoised & interpolation-restored. (h) Integral restoration of (g). Baboon: (i) Original. (j) Decrypted & only interpolation-restored. (k) Decrypted, denoised & interpolation-restored. (l) Integral restoration of (k)

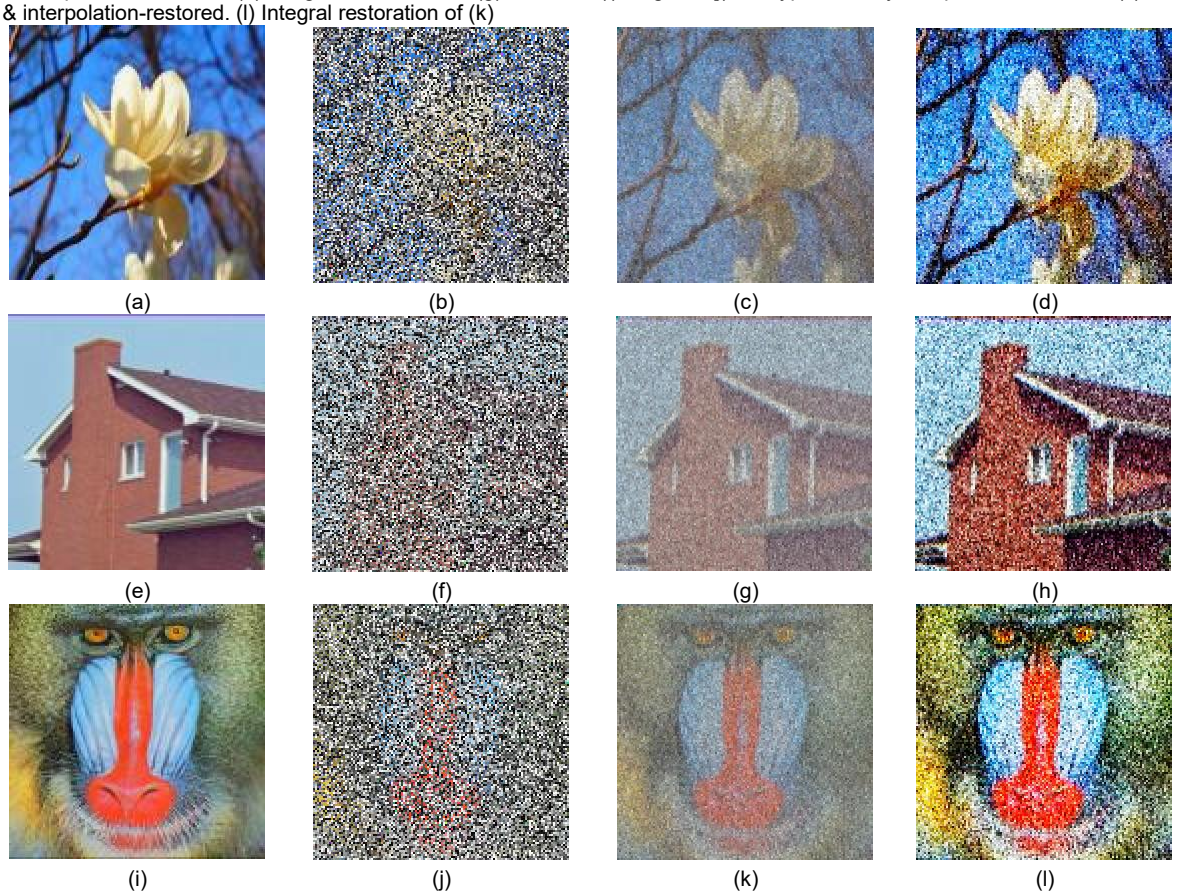
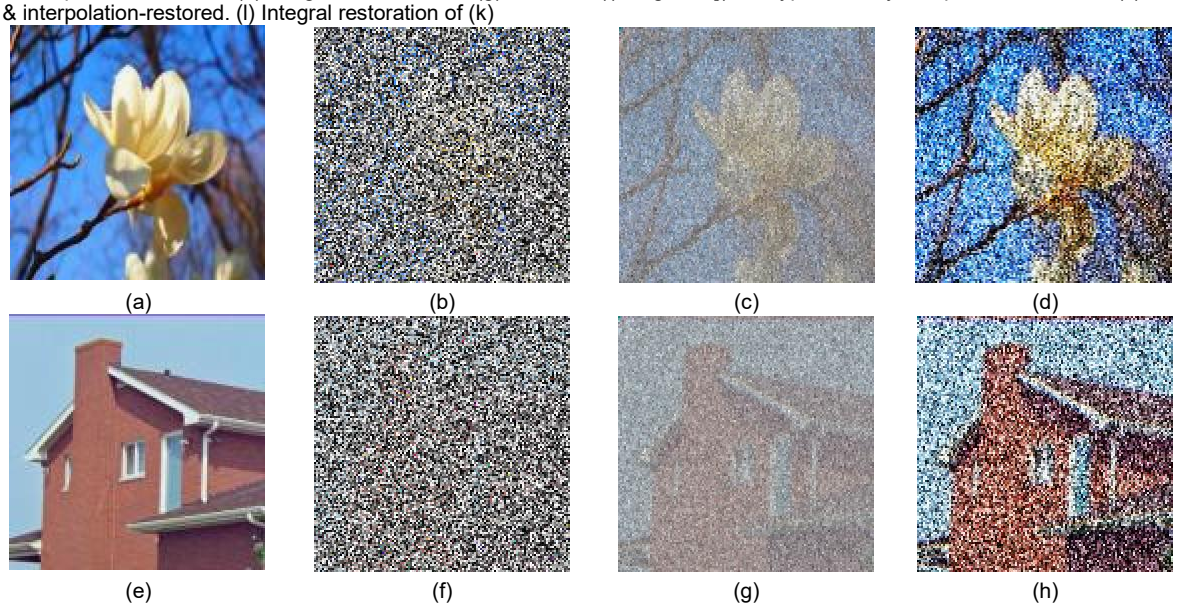
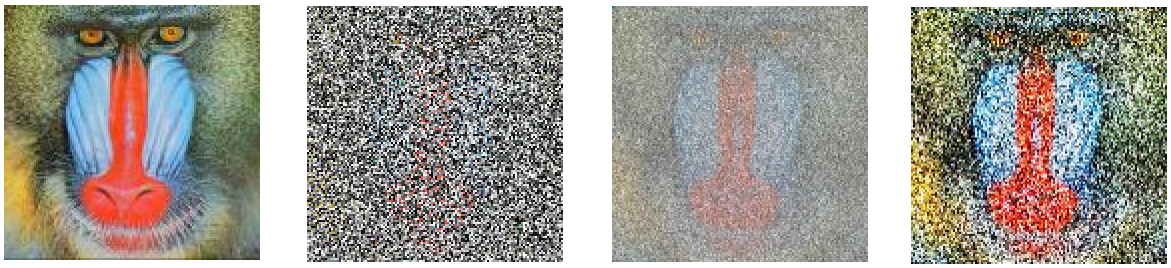


Fig.23. Restoration performance under 80% data loss: Magnolia: (a) Original. (b) Decrypted & only interpolation-restored. (c) Decrypted, denoised & interpolation-restored. (d) Integral restoration of (c). House: (e) Original. (f) Decrypted & only interpolation-restored. (g) Decrypted, denoised & interpolation-restored. (h) Integral restoration of (g). Baboon: (i) Original. (j) Decrypted & only interpolation-restored. (k) Decrypted, denoised & interpolation-restored. (l) Integral restoration of (k)

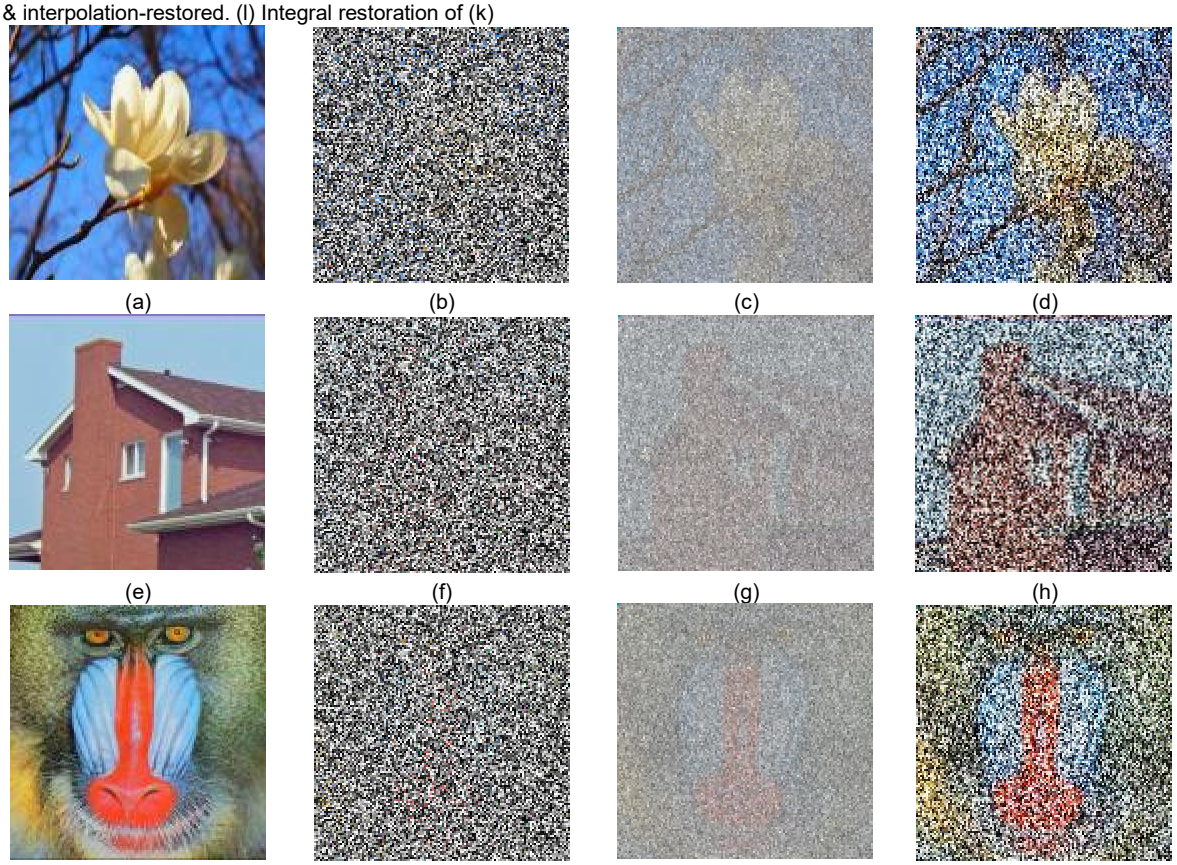
Fig.24. Restoration performance under 85% data loss: Magnolia: (a) Original. (b) Decrypted & only interpolation-restored. (c) Decrypted, denoised & interpolation-restored. (d) Integral restoration of (c). House: (e) Original. (f) Decrypted & only interpolation-restored. (g) Decrypted, denoised & interpolation-restored. (h) Integral restoration of (g). Baboon: (i) Original. (j) Decrypted & only interpolation-restored. (k) Decrypted, denoised & interpolation-restored. (l) Integral restoration of (k)





(i) (j) (k) (l)

Fig.25. Restoration performance under 90% data loss: Magnolia: (a) Original. (b) Decrypted & only interpolation-restored. (c) Decrypted, denoised & interpolation-restored. (d) Integral restoration of (c). House: (e) Original. (f) Decrypted & only interpolation-restored. (g) Decrypted, denoised & interpolation-restored. (h) Integral restoration of (g). Baboon: (i) Original. (j) Decrypted & only interpolation-restored. (k) Decrypted, denoised & interpolation-restored. (l) Integral restoration of (k)



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

(e) (f) (g) (h)

(i) (j) (k) (l)

Fig.26. Restoration performance under 95% data loss: Magnolia: (a) Original. (b) Decrypted & only interpolation-restored. (c) Decrypted, denoised & interpolation-restored. (d) Integral restoration of (c). House: (e) Original. (f) Decrypted & only interpolation-restored. (g) Decrypted, denoised & interpolation-restored. (h) Integral restoration of (g). Baboon: (i) Original. (j) Decrypted & only interpolation-restored. (k) Decrypted, denoised & interpolation-restored. (l) Integral restoration of (k)

5.3.2 Restoration quality analysis.

To quantitatively evaluate the restoration performance, we employed three metrics: MSE, PSNR, and SSIM. In Table 8, "–" denotes images without restoration, "SR" denotes images processed with stochastic resonance denoising, and "IRA" denotes images further processed with integral restoration after SR. The percentages indicate the proportion of data loss.

As shown in Table 8, unrecovered images consistently yield the highest MSE and lowest PSNR/SSIM across all data loss rates, with values deteriorating as loss increases, even approaching those of encrypted images. This indicates severe information loss in decrypted images without restoration. After SR denoising, MSE decreases significantly while PSNR and SSIM improve accordingly. For instance, for the Magnolia image at 75% data loss in the R channel, MSE drops from 7077 to 1344, PSNR rises from 9.6323 dB to 16.8469 dB, and SSIM increases from 0.0460 to 0.4535, demonstrating that stochastic resonance effectively suppresses noise and recovers partial image structure.

Furthermore, as observed in Table 8 and Figs. 22–26, although most IRA metrics do not consistently outperform SR, the contours and fine details of IRA-processed images become increasingly distinct as data loss increases, surpassing both unrecovered and SR-only results. This indicates that IRA better preserves structural fidelity and restores textural details, yielding restored images visually closer to the originals.

In summary, the SR-based denoising effectively reduces noise and improves image quality, while the subsequent IRA further enhances restoration by recovering fine structural details. These results confirm the effectiveness of the proposed cascaded restoration strategy for robust image recovery under severe data loss.

TABLE 8. Restoration performance metrics

Image	loss	trial	MSE			PSNR(dB)			SSIM		
			R	G	B	R	G	B	R	G	B
Magnolia		—	7077	5990	8623	9.6323	10.3565	8.7741	0.0460	0.0536	0.0641
	75%	SR	1344	1043	2441	16.8469	17.9495	14.2556	0.4535	0.4674	0.4478
		IRA	1149	1340	1425	17.5265	16.8591	16.5938	0.3519	0.3776	0.4500
		—	7554	6407	9195	9.3489	10.0639	8.4955	0.0372	0.0420	0.0505
	80%	SR	1969	1302	2526	15.1887	16.9838	14.1072	0.3786	0.3981	0.3901
		IRA	1539	1745	1759	16.2591	15.7123	15.6770	0.2845	0.3065	0.3814
		—	8033	6797	9763	9.0819	9.8075	8.2351	0.0293	0.0324	0.0324
	85%	SR	2917	1795	2867	13.4811	15.5913	13.5561	0.3028	0.3245	0.3218
		IRA	2298	2538	2468	14.5178	14.0861	14.2078	0.2109	0.2288	0.2953
		—	8450	7166	10319	8.8621	9.5781	7.9946	0.0237	0.0252	0.0295
	90%	SR	4246	2538	3440	11.8514	14.0865	12.7654	0.2249	0.2445	0.2421
		IRA	3670	3793	3921	12.4846	12.3404	12.1969	0.1391	0.1487	0.1970
		—	8909	7541	10795	8.6323	9.3567	7.7987	0.0175	0.0170	0.0191
	95%	SR	5927	3509	4262	10.4023	12.6790	11.8346	0.1465	0.1591	0.1522
		IRA	6158	5738	6795	10.2363	10.5434	9.8086	0.0645	0.0719	0.0956
House		—	5230	6351	7241	10.9461	10.1021	9.5327	9.5327	0.0404	0.0363
	75%	SR	521	1102	1414	20.9602	17.7073	16.6260	0.3735	0.3599	0.3181
		IRA	1683	1929	2130	15.8700	15.2768	14.8465	0.2148	0.2319	0.2025
		—	5589	6787	7729	10.6577	9.8143	9.2498	0.0301	0.0332	0.0300
	80%	SR	649	1471	1791	20.0097	16.4532	15.5991	0.3246	0.3137	0.2815
		IRA	2272	2301	2442	14.5664	14.5111	14.2525	0.1715	0.1962	0.1711
		—	5949	7231	8244	10.3864	9.5386	8.9696	0.0238	0.0253	0.0229
	85%	SR	806	1910	2270	19.0650	15.3212	14.5698	0.2760	0.2657	0.2436
		IRA	3121	2944	3044	13.1884	13.4414	13.2961	0.1291	0.1543	0.1350
		—	6299	7661	8722	10.1379	9.2877	8.7246	0.0185	0.0189	0.0177
	90%	SR	997	2439	2853	18.1440	14.2588	13.5773	0.2247	0.2154	0.2024
		IRA	4274	4095	4254	11.8226	12.0084	11.8431	0.0874	0.1066	0.0940
		—	6589	8024	9116	9.9426	9.0871	8.5326	0.0131	0.0124	0.0122
	95%	SR	1350	3314	3715	16.8262	12.9273	12.4311	0.1688	0.1576	0.1530
		IRA	5566	5885	6346	10.6755	10.4332	10.1058	0.0486	0.0574	0.0521
Baboon		—	6135	5271	6465	10.2526	10.9117	10.0248	0.0498	0.0477	0.0477
	75%	SR	982	754	1320	18.2105	19.3576	16.9254	0.4221	0.4221	0.3185
		IRA	1748	2087	2088	15.7055	14.9362	14.9339	0.3069	0.2441	0.2414
		—	6541	5642	6910	9.9741	10.6166	9.7361	0.0411	0.0396	0.0387
	80%	SR	1228	936	1725	17.2406	18.4171	15.7630	0.3651	0.3181	0.2790
		IRA	2244	2599	2503	14.6200	13.9834	14.1457	0.2405	0.1939	0.2008
		—	6957	6033	7368	9.7065	10.3256	9.4571	0.0326	0.0307	0.0297
	85%	SR	1631	1355	2534	16.0065	16.8104	14.0933	0.2990	0.2630	0.2303
		IRA	2972	3302	3165	13.4003	12.9424	13.1268	0.1734	0.1441	0.1544
		—	7349	6358	7756	9.4685	10.0973	9.2343	0.0254	0.0242	0.0230
	90%	SR	2196	1883	3506	14.7145	15.3825	12.6830	0.2315	0.2076	0.1814
		IRA	4109	4292	4298	11.9939	11.8043	11.7980	0.1113	0.0960	0.1051
		—	7712	6657	8139	9.2593	9.8982	9.0252	0.0188	0.0186	0.0172
	95%	SR	2766	2357	4452	13.7126	14.4075	11.6453	0.1632	0.1496	0.1298
		IRA	5824	5601	6158	10.4787	10.6482	10.2367	0.0585	0.0523	0.0568

6. CONCLUSIONS

This paper addresses the dual challenges of privacy security and large-area damage in image transmission by proposing an image encryption and restoration method based on a bimodal isomorphic dynamical system. Unlike conventional approaches that treat encryption and restoration as separate modules, the proposed system achieves both functions within a unified architecture, where the same nonlinear framework is switched between chaotic and stochastic resonance modes via parameter adjustment.

Firstly, by constructing a four-dimensional chaotic system and a stochastic resonance system, a theoretical foundation has been laid for subsequent encryption and restoration algorithms. Secondly, chaotic sequences have been utilized for random-point scrambling and Latin matrix diffusion, with security analysis conducted on image encryption and decryption experiments. The results have demonstrated that the encryption algorithm effectively disrupts the statistical characteristics of image pixels. Its favorable information

entropy, MSE, PSNR, and SSIM values, along with NPCR and UACI values close to the theoretical ideals, high key sensitivity, and strong resistance to damage attacks collectively verify the algorithm's high confidentiality and robustness. Finally, by addressing the potential severe data loss after image transmission, the proposed algorithm based on stochastic resonance denoising and integral restoration has exhibited outstanding recovery performance across tests on damaged regions of varying sizes and shapes. Experimental results have confirmed that the algorithm can effectively extract and reconstruct the characteristic information of the original image from severely damaged image data, significantly enhancing the survivability and usability of images in harsh transmission environments.

In summary, this research has integrated the encryption advantages of chaotic systems with the restoration potential of stochastic resonance systems, providing an effective technical pathway for addressing integrity issues in secure image transmission. Future work will focus on exploring more complex scrambling and diffusion algorithms to further enhance decryption resistance, as well as optimizing restoration algorithms to handle more complex damage scenarios.

References

[1] L. Huang, H. Gao, "Multi-Image Encryption Algorithm Based on Novel Spatiotemporal Chaotic System and Fractal Geometry," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 71, no. 8, pp. 3726-3739, 2024, doi: 10.1109/TCSI.2024.3407809.

[2] C. Wang, Y. Ming, H. Liu, et al. "Security-Enhanced Data Transmission With Fine-Grained and Flexible Revocation for DTWNs," *IEEE Transactions on Information Forensics and Security,* vol. 20, pp. 1237-1250, 2025, doi: 10.1109/TIFS.2024.3523765.

[3] J.R. Blum, A. Eichhorn, S. Smith, et al. "Real-time emergency response: improved management of real-time information during crisis situations," *Journal on Multimodal User Interfaces,* vol. 8, no. 2, pp. 161-173, 2014, doi: 10.1007/s12193-013-0139-7.

[4] N. Cecchinato. A. Toma, C. Drioli, et al. "A Secure Real-time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain," *Procedia Computer Science,* vol. 205, pp. :50-57, 2022, doi: 10.1016/j.procs.2022.09.006.

[5] H. Pirayesh, H. Zeng. "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials,* vol. 24, no. 2, pp. 767-809, 2022, doi: 10.1109/COMST.2022.3159185.

[6] O.Y. Bursalioglu, G. Caire, D. Divsalar. "Joint source-channel coding for deep-space image transmission using rateless codes," *IEEE Transactions on Communications,* pp. 1-10, 2011.

[7] Y. Zhang, H. Li, B. Li, et al. "An underwater acoustic semantic communication approach to underwater image transmission," *Intelligent Marine Technology and Systems,* vol. 3, no. 1, pp. 5, 2025, doi: 10.1007/s44295-025-00054-7.

[8] G. Biban, R. Chugh, A. Panwar. "Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix," *Chaos, Solitons & Fractals,* vol. 170, pp. 113396, 2023, doi: 10.1016/j.chaos.2023.113396.

[9] N. Wang, M. Cui, X. Yu, et al. "Generation of no-equilibrium multi-fold chaotic attractor for image processing and security," *Applied Mathematical Modelling,* vol. 133, pp. 271-285, 2024, doi: 10.1016/j.apm.2024.05.022.

[10] Q. Peng, K. Zhang, B. Zheng, et al. "Color image encryption method based on four-dimensional multi-scroll multi-wing hyperchaotic system and DNA mutation mechanism," *Journal of King Saud University Computer and Information Sciences,* vol. 37, no. 5, pp. 110, 2025, doi: 10.1007/s44443-025-00108-0.

[11] L. Xiao, X. Li, P. Cao, et al. "A Dynamic-Varying Parameter Enhanced ZNN Model for Solving Time-Varying Complex-Valued Tensor Inversion With Its Application to Image Encryption," *IEEE Transactions on Neural Networks and Learning Systems,* vol. 35, no. 10, pp. 13681-13690, 2023, doi: 10.1109/TNNLS.2023.3270563.

[12] M. Roohi, C. Zhang, Y. Chen, et al. "Adaptive model-free synchronization of different fractional-order neural networks with an application in cryptography,". *Nonlinear Dynamics,* vol. 100, pp. 3979-4001, 2020, doi:10.1007/s11071-020-05719-y.

[13] Y. Ding, Z. Wang, Z. Qin, et al. "Backdoor Attack on Deep Learning-Based Medical Image Encryption and Decryption Network," *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 280-292, 2024, doi: 10.1109/TIFS.2023.3322315.

[14] Y. Chen, H. Huang, K. Huang, et al. "A selective chaos-driven encryption technique for protecting medical images,". *Physica Scripta,* vol. 100, pp. 0152a3, 2025, doi:10.1088/1402-4896/ad9fad.

[15] J. Gao, Y. Shen, S. Li, et al. "An enhanced hybrid chaotic system and its application in image encryption," *Journal of King Saud University Computer and Information Sciences,* vol. 37, no. 9, pp. 295, 2025, doi: 10.1007/s44443-025-00320-y.

[16] Z. Fu, Y. Liu, X. Cui. "Chaos-based broadcast encryption with authenticated secure message transmission scheme," *Information Sciences,* vol. 719, pp. 122433, 2025, doi: 10.1016/j.ins.2025.122433.

[17] J. Li, Z. Chen, S. Li. "Selection of the number of effective singular values for noise reduction," *Mechanical Systems and Signal Processing,* vol. 191, pp. 110175, 2023, doi: 10.1016/j.ymssp.2023.110175.

[18] Y. Cui, W. Ren, X. Cao, et al. "Image Restoration via Frequency Selection," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 46, no. 2, pp. 1093-1108, 2024, doi: 10.1109/TPAMI.2023.3330416.

[19] Z. Zhou, W. Yu, J. Wang, et al. "A high dimensional stochastic resonance system and its application in signal processing," *Chaos, Solitons & Fractals,* vol. 154, pp. 111642, 2022, doi: 10.1016/j.chaos.2021.111642.

[20] J. Li, X. Cheng, S. Zhang, et al. "Fault feature extraction method of rolling bearings based on coupled resonance system with vibrational resonance-assisted enhanced stochastic resonance," *Mechanical Systems and Signal Processing,* vol. 208, pp. 111069, 2024, doi: 10.1016/j.ymssp.2023.111069.

[21] M. Zhou, C. Wang. "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks,". *Signal Processing,* vol. 171, pp. 107484, 2020, doi:10.1016/j.sigpro.2020.107484.

[22] Q. Liang, C. Zhu. "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding,". *Optics & Laser Technology,* vol. 160, pp. 109033, 2023, doi:10.1016/j.optlastec.2022.109033.

[23] Z. Guo, S. Chen, L. Zhou, et al. "Optical image encryption and authentication scheme with computational ghost imaging,". *Applied Mathematical Modelling,* vol. 131, pp. 49-66, 2024, doi:10.1016/j.apm.2024.04.012.

[24] W. Alexan, K. Hosny, M, Gabr. "A new fast multiple color image encryption algorithm,". *Cluster Computing,* vol. 28, pp. 325, 2025, doi:10.1007/s10586-024-04919-0.

[25] Q. Xiao, W. Yu. "A random decomposition method for chaotic sequences to improve the security of image encryption,". *Physica Scripta,* vol. 100, pp. 035237, 2025, doi:10.1088/1402-4896/adb523.

[26] W. Alexan, M. ElBeltagy, A. Aboshousha. "RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System,". *Symmetry,* vol. 14, pp. 443, 2022, doi:10.3390/sym14030443.

[27] H. Zang, M. Tai, X. Wei, et al. "Image Encryption Schemes Based on a Class of Uniformly Distributed Chaotic Systems,". *Mathematics,* vol. 10, pp. 1027, 2022, doi:10.3390/math10071027.

[28] W. Alexan, M. Elkandoz, M. Mashaly, et al. "Color Image Encryption Through Chaos and KAA Map,". *IEEE Access,* vol. 11, pp. 11541-11554, 2022, doi:10.1109/ACCESS.2023.3242311.

Bulletin of the Polish Academy of Sciences Technical Sciences (BPASTS)
https://www.editorialsystem.com/bpasts

LICENSE TO PUBLISH

The following License to Publish ("License") must be signed and returned to the Journal Owner before a manuscript can be published. If the copyright in the contribution is owned by the author's employer, the employer or an authorized representative must sign this form. In the event that the Journal Owner decides not to publish the Work, this License shall be null and void.

Please read the terms of this agreement, print initial page 1, print and sign page 2, scan and upload the document as one file according to the Editors' guidelines (submit via Editorial System).

Article entitled ("Work" or "Article"):
Image Encryption and Restoration Based on a Bimodal Isomorphic Dynamical System

Author/s: (also referred to as "Licensor/s")
Qian Xiong, Zaifang Xi, Jia Duan, Wenxin Yu

Corresponding author: (if more than one author)
Zaifang Xi

Journal Name
Bulletin of the Polish Academy of Sciences Technical Sciences

Journal Owner
Polish Academy of Sciences

1. License

The use of the article will be governed by the Creative Commons Attribution license CC BY 4.0 as currently displayed on https://creativecommons.org/licenses/by/4.0/.

2. Author's Warranties

The author warrants that the article is original, written by stated author/s, has not been published before, contains no unlawful statements, does not infringe the rights of others, is subject to copyright that is vested exclusively in the author and free of any third party rights, and that any necessary written permissions to quote from other sources have been obtained by the author/s. The undersigned also warrants that the manuscript (or its essential substance) has not been published other than as an abstract or doctoral thesis and has not been submitted for consideration elsewhere, for print, electronic or digital publication.

3. User Rights

Under the Creative Commons Attribution license, the author(s) and users are free to share (copy, distribute and transmit the contribution) under the following conditions:
1. They must attribute the contribution in the manner specified by the author or licensor,
2. They may use this contribution for commercial purposes,
3. They may alter, transform, or build upon this work.

4. Rights of Authors

Authors retain the following rights:
– copyright, and other proprietary rights relating to the article, such as patent rights,
– the right to use the substance of the article in future own works, including lectures and books,
– the right to reproduce the article for own purposes, provided the copies are not offered for sale,
– the right to self-archive the article,
– the right to supervision over the integrity of the content of the work and its fair use.

5. Co-Authorship

If the article was prepared jointly with other authors, the signatory of this form warrants that he/she has been authorized by all co-authors to sign this agreement on their behalf, and agrees to inform his/her co-authors of the terms of this agreement.

6. Termination

This agreement can be terminated by the author or the Journal Owner upon two months' notice where the other party has materially breached this agreement and failed to remedy such breach within a month of being given the terminating party's notice requesting such breach to be remedied. No breach or violation of this agreement will cause this agreement or any license granted in it to terminate automatically or affect the definition of the Journal Owner. The author and the Journal Owner may agree to terminate this agreement at any time. This agreement or any license granted in it cannot be terminated otherwise than in accordance with this section 6. This License shall remain in effect throughout the term of copyright in the Work and may not be revoked without the express written consent of both parties.

7. Royalties

This agreement entitles the author to no royalties or other fees. To such extent as legally permissible, the author waives his or her right to collect royalties relative to the article in respect of any use of the article by the Journal Owner or its sublicensee.

8. Miscellaneous

The Journal Owner will publish the article (or have it published) in the Journal if the article's editorial process is successfully completed and the Journal Owner or its sublicensee has become obligated to have the article published. Where such obligation depends on the payment of a fee, it shall not be deemed to exist until such time as that fee is paid. The Journal Owner may conform the article to a style of punctuation, spelling, capitalization and usage that it deems appropriate. The author acknowledges that the article may be published so that it will be publicly accessible, and such access will be free of charge for the readers. The Journal Owner will be allowed to sublicense the rights that are licensed to it under this agreement. This agreement will be governed by the laws of Poland.

By signing this License, Author(s) warrant(s) that they have the full power to enter into this agreement. This License shall remain in effect throughout the term of copyright in the Work and may not be revoked without the express written consent of both parties.

Author's (Corresponding Author's) Signature (to be signed only by the corresponding Author):

Name printed:

Zaifang Xi

Date:

6 July 2026