Int. J. Appl. Math. Comput. Sci., 2025, Vol. 35, No. 3, 417–428
DOI: 10.61822/amcs-2025-0029

DESIGN OF A NEW CHAOTIC SYSTEM BY A NON–SMOOTH CONTROLLER AND ITS APPLICATION

JIANBIN HE [a,*], KUN ZHAO [a], SHIYA WANG [a]

[a] School of Mathematics and Statistics
Minnan Normal University
Zhangzhou 363000, China
e-mail: jbh2012yml@126.com

Chaos theory constitutes a fundamental discipline within nonlinear science. Chaotic systems, leveraging their sensitive dependence on initial conditions, have found extensive applications in information security. While numerous chaotic systems have been developed via continuous control methodologies in recent years, the design of such systems under non-smooth control regimes remains challenging due to the lack of systematic theoretical frameworks. Under what conditions can non-smooth control schemes induce deterministic chaos in nonlinear systems? What systematic methodology enables the construction of non-smooth controllers that guarantee chaotic dynamics generation while maintaining system stabilizability? Building upon the principles of chaos theory, this study introduces a novel chaotic system developed via a non-smooth control design methodology. The newly developed chaotic system is analyzed through its complex attractors and equilibrium points. Additionally, an image encryption algorithm based on this system is investigated, combining block scrambling and diffusion techniques in its design. The feasibility of the proposed encryption algorithm is validated through numerical simulations, demonstrating an expansive key space and robust security characteristics as evidenced by comprehensive security analyses.

Keywords: chaotic system, non-smooth control, pseudo-random sequence, image encryption.

1. Introduction

With the progress of the Internet, the transmission of multimedia information is very popular in our daily life, such as the information of video and image. The security of information is very important for our privacy. As the information is sent by the public network, and it may be attacked and cracked. Therefore, it is very necessary to protect information and ensure confidentiality of data (Gao and Gao, 2019).

Chaos-based encryption algorithm is one of useful technologies to ensure information security. Chaos is hailed as the third revolution in 20th century in physics (Fu *et al*., 2018). Researchers have found that there are many connections between cryptography and chaos. As chaotic system has the characteristics of pseudo-randomness, unpredictability and sensitivity, it can be used to the information encryption. Many scholars have done much research based on chaotic systems (Song *et al*., 2019; Xiao *et al*., 2019; Chen *et al*., 2020; Peechara and Sucharita, 2021; Singh *et al*., 2021; Ramakrishnan *et al*., 2024).

An encryption algorithm with high text sensitivity by chaotic map and the Hilbert quantum scrambling algorithm for encryption is proposed, and the experiments show the method is robust and efficient (Rajakumaran and Kavitha, 2020). According to Tent chaotic map, an image encryption algorithm is investigated by Khaitan *et al*. (2020). The encryption key is generated by an optimized Salp Swarm algorithm, and the algorithm can resist violent attacks, differential cryptanalysis and key sensitivity analysis attacks. Based on chaotic attractor in the frequency domain, and an encryption algorithm is studied by means of substitution, encoding, complementation and decoding (Banu S and Amirtharajan, 2020). A novel image encryption is investigated by a Sine chaotic map and the Logistic map, and it expands the key space and exhibits significant resistance to well-known attacks (ul Haq and Shah,

*Corresponding author

2020). An encryption algorithm is investigated for digital images, and the pixels of image are circularly encrypted to enhance the system security, such as differential attack (Ravichandran *et al*., 2021). Based on the block scrambling encryption, an algorithm is studied to improve the degree of scrambling of image pixel (Li and Han, 2021). By the combination of Tent map, Logistics chaotic map and Sine map, an algorithm with large key space is given by diffusion encryption. The encryption algorithm is investigated by shifting bit-levels of the plaintext image, and the diffusion encryption of image is designed by the integrated chaos map combined with Sine, Tent and Logistic maps (Riyahi *et al*., 2021).

In order to improve the security, an image encryption algorithms is proposed, and the algorithm can resist to the chosen-plaintext and chosen-ciphertext attacks (Zhang, 2021). By the enhanced Thorp mixing and sawtooth scan convolution, an image encryption algorithm is investigated (Huang *et al*., 2022). An encryption algorithm is investigated based on Lorenz systems and Logistic chaotic map for many kinds of digital images (Zhang *et al*., 2022). The chaotic map is used to control the generation of random sequences for an image encryption technology, several statistics and security tests show that the scheme can improve the encryption efficiency and has certain ability to resist common attacks (Mondal and Singh, 2022).

The significance of studying non-smooth chaos anti-control (i.e., intentionally inducing or amplifying chaos via non-smooth controllers) lies in its unique applications and theoretical insights. The non-smooth strategies efficiently destabilize equilibria to generate chaos through abrupt nonlinear interventions, aligning with real-world non-idealities. Chaotic unpredictability is valuable for secure communication, encryption, and optimizing complex dynamics. Therefore, this research advances the understanding of non-smooth dynamics and chaos generation mechanisms, offering novel paradigms for controlling complex systems.

Current chaotic encryption studies predominantly rely on smooth or continuous systems, overlooking the potential of non-smooth sawtooth wave dynamics in enhancing chaos complexity and anti-attack capabilities, particularly in expanding key spaces and optimizing resistance to cropping attacks. The proposed sawtooth wave controller employs a non-continuous piecewise slope mutation mechanism, disrupting equilibrium in traditional smooth systems. This enhances ergodicity and initial value sensitivity. The image encryption algorithm based on this non-smooth chaotic system utilizes pixel-key bidirectional diffusion, expanding the key space to 10^{575}. An block-wise encryption strategy improves resistance to cropping attacks.

Usually, the dynamic characteristics of hyperchaotic system are more complex than the chaotic system with one positive Lyapunov exponent (Wu *et al*., 2016; Al Solami *et al*., 2018; Xiao *et al*., 2022).

Drawing on chaos theory, this study presents a controlled system capable of generating complex chaotic attractors through non-smooth control. Building upon this foundation, we develop a novel encryption algorithm leveraging higher-dimensional chaotic dynamics, subsequently demonstrating its effectiveness through practical image encryption applications. The principal contributions of this work are threefold: (i) a new chaotic system is constructed by introducing a single non-smooth controller to a stable linear nominal system, enabling controlled chaotic behavior, (ii) a dual-stage encryption framework is proposed, integrating Z-shaped block scrambling with pixel-value diffusion encryption, where cryptographic sequences are derived directly from the state variables of the developed chaotic system, (iii) comprehensive cryptanalysis is conducted through statistical evaluations (including NIST SP 800-22 tests) and resistance verification against differential cryptanalysis and cropping attacks.

2. Design of a higher-dimensional new chaotic system and equilibrium analysis

2.1. Design of higher-dimensional new chaotic systems. Based on the design method of chaotic system (He and Yu, 2019; Zhao and He, 2022), the linear system is

$$\dot{\boldsymbol{x}} = \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}\boldsymbol{x}, \tag{1}$$

where

$$\boldsymbol{A} = \begin{pmatrix} A_1 & 0 & 0 & 0 & 0 \\ 0 & \boldsymbol{A}_2 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A_{m-1} & 0 \\ 0 & 0 & \cdots & 0 & A_m \end{pmatrix}_{n\times n}, \tag{2}$$

when n is even, $m = \frac{n}{2}$, and the block matrix

$$\boldsymbol{A}_d = \begin{pmatrix} \lambda_d & \psi_{d1} \\ \psi_{d2} & \lambda_d \end{pmatrix}, \psi_{d1} \times \psi_{d2} < 0.$$

By designing a controller $\boldsymbol{f}(\sigma\boldsymbol{x}, \varepsilon)$ and controlling matrix $\boldsymbol{C}$, one can obtain a controlled system, i.e.,

$$\dot{\boldsymbol{x}} = \boldsymbol{P}\boldsymbol{A}\boldsymbol{P}^{-1}\boldsymbol{x} + \boldsymbol{C}\boldsymbol{f}\left(\sigma\boldsymbol{x}, \varepsilon\right), \tag{3}$$

where $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)^T$, $\boldsymbol{P}$ is a non-singular matrix, and $\boldsymbol{A}$ is a block matrix with negative eigenvalues.

The controller generates a sawtooth wave, which is defined as follows:

$$\boldsymbol{f}\left(\sigma\boldsymbol{x}, \varepsilon\right) = \begin{cases} \varepsilon\text{sawtooth}(\sigma x_1), \\ \varepsilon\text{sawtooth}(\sigma x_2), \\ \vdots \\ \varepsilon\text{sawtooth}(\sigma x_n), \end{cases} \tag{4}$$

where

$$\varepsilon\text{sawtooth}(\sigma x_i) = \frac{\varepsilon\sigma}{\pi}(x_i - \frac{\pi}{\sigma}i), x_i \in [\frac{2\pi}{\sigma}i, \frac{2\pi}{\sigma}(i+1)],$$
$$i = \cdots, -1, 0, 1 \cdots.$$

The set $\{\varepsilon, \sigma\}$ constitutes the controller parameters, and the controller's position matrix is defined as

$$\boldsymbol{C} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 1_{(i,j)} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}_{n\times n}. \tag{5}$$

Let matrix $\boldsymbol{A}$ be defined as

$$\boldsymbol{A} = \begin{pmatrix} -1 & -6 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -0.1 & -14 \\ 0 & 0 & 8 & -0.3 \end{pmatrix}, \tag{6}$$

with the parameter matrices

$$\boldsymbol{P} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \boldsymbol{C} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{7}$$

The dynamical system governed by Eqn. (3) is controlled by the function $\boldsymbol{f}(\sigma\boldsymbol{x}, \varepsilon)$ with parameters $\varepsilon = 2.3$ and $\sigma = 4.1$, where the control input is applied at the position $(i, j) = (4, 3)$. The system dynamics are formulated as follows:

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{pmatrix} = \begin{pmatrix} 6.9667 & -6.9333 & -0.0333 & -7.0333 \\ 0.5333 & -7.7667 & 7.2333 & 0.2333 \\ 9.8333 & -12.3667 & 1.5333 & -3.4667 \\ 12.1667 & -10.0333 & -1.1333 & -3.1333 \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2.3\text{sawtooth}(4.1x_3) \end{bmatrix}, \tag{8}$$

where the controller $\boldsymbol{f}(\sigma\boldsymbol{x}, \varepsilon)$ is a sawtooth wave function $y = f(x_3) = 2.3\text{sawtooth}(4.1x_3)$.

Since the controller $\boldsymbol{f}(\sigma\boldsymbol{x}, \varepsilon)$ is continuous and uniformly bounded, the controlled systems (3) and (8) are also bounded. The chaotic attractors corresponding to the initial conditions

$$\boldsymbol{x}(0) = (0.2, 0.1, 0.2, 0.5)^T \tag{9}$$

are shown in Fig. 1.

Distinct initial values can generate different sequences that produce unique attractor phase diagrams.

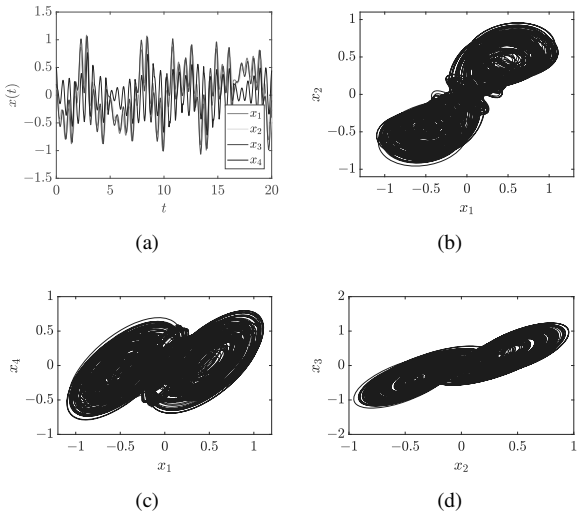


Fig. 1. Chaotic attractors of the system (8): time series of variables $x(t)$ (a), x_1 vs. x_2, (c) x_1 vs. x_4, (d) x_2 vs. x_3 (b).

The system variables remain bounded within the range $[-1.5, 1.5]$, while the generated sequences exhibit pseudo-random behavior characterized by non-periodicity, non-convergence, and non-divergence.

Note 1. The matrix $\boldsymbol{A}$ must satisfy the negative definiteness criterion, requiring all its eigenvalues to possess negative real parts. The parameters $\{\varepsilon, \sigma\}$ and positions $\boldsymbol{C}$ of controller (4) must be judiciously selected to ensure effective stabilization of the asymptotically stable system, thereby inducing characteristic value transformations through sign reversal in their real parts, for instance, generating multiple eigenvalues with positive real components in the controlled system.

Note 2. The non-smooth controller in Eqn. (4) and Fig. 2 is both non-differentiable and discontinuous at zero and other periodic points, and it employs discontinuous or non-differentiable control laws to enforce finite-time convergence, offering strong robustness against model inaccuracies and disturbances. However, it may induce high-frequency chattering. Non-smooth controllers excel in chaotic systems or underactuated scenarios, while smooth controllers are preferred for conventional stabilization tasks requiring simplicity and smooth operation.

2.2. Equilibrium analysis. The equilibrium point of the system (1) is only zero, and the corresponding eigenvalues of the Jacobi matrix are given by

$$\lambda_{1,2} = -0.2 \pm 10.5824\text{i}, \lambda_{3,4} = -1 \pm 2.4496\text{i}. \tag{10}$$

Thus, the system (1) is asymptotically stable.

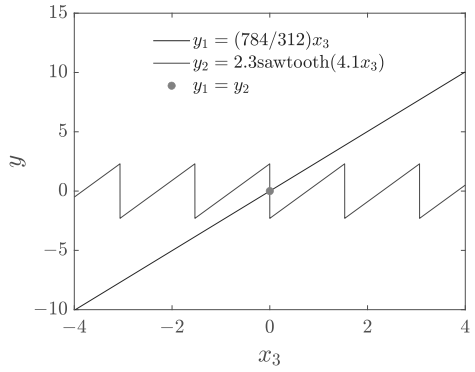


Fig. 2. Equilibrium point of the system (8).

The equilibrium point x_i of the system (8) is satisfied following equations, i.e.,

$$x_i = (-1)^{(4+i)} \frac{f(\sigma x_3, \varepsilon)}{|\boldsymbol{H}|} |\boldsymbol{G}_i|, \quad i = 1, 2, 3, 4, \quad (11)$$

where matrix $\boldsymbol{H} = \boldsymbol{PAP}^{-1}$, $\boldsymbol{G}_i$ is equal to $\boldsymbol{H}$ except the i-th column is a column vector $[0, 0, 0, f(\sigma x_3, \varepsilon)]^T$, and $|*|$ is the determinant of matrix $*$. As the sawtooth wave function $f(\sigma x_3, \varepsilon) = -2.3\text{sawtooth}(4.1x_3)$, and the determinant of $\boldsymbol{A}$ is $|\boldsymbol{H}| \approx 784$, then one has

$$\begin{cases} x_1 = \dfrac{-2.3\text{sawtooth}(4.1x_3)}{784}(-368), \\ x_2 = \dfrac{-2.3\text{sawtooth}(4.1x_3)}{784}317, \\ x_3 = \dfrac{-2.3\text{sawtooth}(4.1x_3)}{784}(-312), \\ x_4 = \dfrac{-2.3\text{sawtooth}(4.1x_3)}{784}50. \end{cases} \quad (12)$$

According to equation $x_3 = \frac{-2.3\text{sawtooth}(4.1x_3)}{784}(-312)$, one can get $\frac{784}{312}x_3 = 2.3\text{sawtooth}(4.1x_3)$.

The functions y_1 and y_2, defined as

$$y_1 = \frac{784}{321}x_3, y_2 = 2.3\text{sawtooth}(4.1x_3),$$

are graphically presented in Fig. 2. Analysis reveals that the system solution satisfies $x_3 = 0$. Consequently, the controlled system (8) possesses a unique equilibrium point located at the origin.

The Jacobian matrix of the system (8) evaluated at the equilibrium point is given by

$$\boldsymbol{J} = \begin{pmatrix} 6.9667 & -6.9333 & -0.0333 & -7.0333 \\ 0.5333 & -7.7667 & 7.2333 & 0.2333 \\ 9.8333 & -12.3667 & 1.5333 & -3.4667 \\ 12.1667 & -10.0333 & 1.8684 & -3.1333 \end{pmatrix},$$

and the eigenvalues are given by

$$\lambda_{1,2} = 0.7396 \pm 11.0144\text{i},$$
$$\lambda_{3,4} = -1.9396 \pm 3.2198\text{i}.$$

The controlled system exhibits two eigenvalues with positive real parts at the equilibrium point. Therefore, the equilibrium is unstable.

3. Design of a chaos encryption algorithm

3.1. Chaotic pseudo-random sequence preprocessing. According to the chaotic system (8), the encryption algorithm is investigated for image information. Firstly, the fourth-order Runge–Kutta algorithm is applied to discretization of chaotic system with step $h = 0.001$ and time $T = 2000$.

The initial values are given in Eqn. (9), the sum of the plaintext image pixel values is divided by 100, and it is added to the initial value x_4. Based on Matlab R2020b and the chaotic system (8), four chaotic sequences are given by

$$\boldsymbol{X} = (\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3, \boldsymbol{X}_4). \quad (13)$$

In order to obtain the sequences $\boldsymbol{X}_i$ $(i = 1, 2, 3, 4)$, chaotic sequences (13) are preprocessed as follows:

Step 1. The sequences $\boldsymbol{X}_i$ $(i = 1, 2, 3, 4)$ are removed with a length of Ts + fix $(\text{s}/\sigma M)$ to reduce the transient effect of chaotic system, where the value of Ts is given by the designer, s is the sum of pixel values of the plaintext image, M is the number of lines of the plaintext image, σ is the parameter in Eqn. (8), and fix is a function of integral. The sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$ are obtained by

$$\begin{cases} \boldsymbol{R}_1 = \text{fix}(\text{mod}(\boldsymbol{X}_1 \times 100\sigma\varepsilon, 1) \times 10^6), \\ \boldsymbol{R}_2 = \text{fix}(\text{mod}(\boldsymbol{X}_2 \times 100\dfrac{\sigma}{\varepsilon}, 1) \times 10^6), \\ \boldsymbol{R}_3 = \text{fix}(\text{mod}(\boldsymbol{X}_3 \times 100\dfrac{\varepsilon}{\sigma}, 1) \times 10^6), \\ \boldsymbol{R}_4 = \text{fix}(\text{mod}(\boldsymbol{X}_4 \times 100\dfrac{1}{\sigma\varepsilon}, 1) \times 10^6), \end{cases} \quad (14)$$

where mod are functions of modular. So, the sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$ can pass the NIST test.

Step 2. The sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$ are further processed by the operation of mod, i.e., sequences $\boldsymbol{Z}_i$ $(i = 1, 2, 3)$ are obtained by

$$\begin{cases} \boldsymbol{Z}_1 = \text{mod}(\boldsymbol{R}_1, 64) + 1, \\ \boldsymbol{Z}_2 = \text{mod}(\boldsymbol{R}_2, 64) + 1, \\ \boldsymbol{Z}_3 = \text{mod}(\boldsymbol{R}_1 \times \boldsymbol{R}_2 - \boldsymbol{R}_3 - \boldsymbol{R}_4, 256). \end{cases} \quad (15)$$

The sequences $\boldsymbol{Z}_i$ $(i = 1, 2, 3)$ can also pass NIST test, and it is applied to the scrambling and diffusion encryption.

3.2. Design of an encryption algorithm. The encryption process combines block-wise row/column scrambling with Z-shaped XOR diffusion encryption.

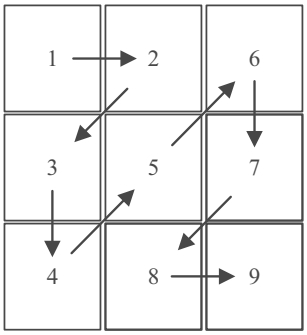


Fig. 3. New sequence obtained by sorting in "Z" shape.

Given a plaintext image matrix $\boldsymbol{P}$ of dimensions $M \times N$, the encryption procedure consists of the following sequential steps:

(i) Row scrambling of blocks.

Step 1. The plaintext image is divided into blocks of size 8×8, and the number of blocks is $\frac{MN}{64}$.

Step 2. The sequence $\boldsymbol{Z}_1$ is used for row scrambling of blocks. In the horizontal direction, the i-th and $\boldsymbol{Z}_1(i)$-th blocks are exchanged, where $i = 1, 2, \cdots, \frac{M}{8}$. According to the row scrambling of blocks, then encrypted image P_1 is obtained by

$$\boldsymbol{P}_1(i) = \boldsymbol{P}(\boldsymbol{Z}_1(i)), \quad i = 1, 2, \cdots, \frac{M}{8}. \tag{16}$$

(ii) Column scrambling of blocks.

Similarly, the sequence $\boldsymbol{Z}_2$ is used to encrypt the scrambled image $\boldsymbol{P}_1$. In the vertical direction, the i-th and $\boldsymbol{Z}_2(i)$-th blocks of scrambled image $\boldsymbol{P}_1$ are exchanged from 1 to $\frac{N}{8}$, and scrambled image $\boldsymbol{P}_2$ is given by

$$\boldsymbol{P}_2(i) = \boldsymbol{P}_1(\boldsymbol{Z}_2(i)), \quad i = 1, 2, \cdots, \frac{N}{8}. \tag{17}$$

(iii) XOR diffusion encryption in "Z" shape.

Step 1. A sequence $\boldsymbol{P}_3'$ with a length of MN is obtained by sorting the scrambled image $\boldsymbol{P}_2$ in "Z" shape. For example, the sorting result in "Z" shape for 3×3 matrix is shown in Fig. 3.

Step 2. The sequence $\boldsymbol{Z}_3$ is applied to the XOR diffusion encryption, and the first value of sequence $\boldsymbol{P}_3'$ is encrypted by

$$\boldsymbol{P}_3(1) = \boldsymbol{P}_3'(1) \oplus \boldsymbol{Z}_3(1). \tag{18}$$

Step 3. The rests of $\boldsymbol{P}_3'$ are ciphered by $\boldsymbol{Z}_3$ and the previous pixel value of $\boldsymbol{P}_3'$. By the reverse operation of "Z" shape in Fig. 3, then encrypted image $\boldsymbol{P}_3$ is obtained by

$$\begin{aligned} \boldsymbol{P}_3(i) = \boldsymbol{P}_3'(i) \oplus \boldsymbol{P}_3'(i-1) \oplus \boldsymbol{Z}_3(i), \\ i = 2, 3, \cdots, MN. \end{aligned} \tag{19}$$

3.3. Design of decryption algorithm. The steps of the decryption algorithm are shown below.

Step 1. The encrypted image $\boldsymbol{P}_3$ is decrypted by the $\boldsymbol{Z}_3(1)$, i.e.,

$$\boldsymbol{P}_3'(1) = \boldsymbol{P}_3(1) \oplus \boldsymbol{Z}_3(1). \tag{20}$$

Step 2. The rests of encrypted image $\boldsymbol{P}_3$ is recovered by the sequence $\boldsymbol{Z}_3$ and the previous value of the sequence $\boldsymbol{P}_3'$, then the sequence $\boldsymbol{P}_3'$ is obtained by

$$\begin{aligned} \boldsymbol{P}_3'(i) = \boldsymbol{P}_3(i) \oplus \boldsymbol{Z}_3(i) \oplus \boldsymbol{P}_3'(i-1), \\ i = 2, 3, \ldots, MN. \end{aligned} \tag{21}$$

Step 3. The sequence $\boldsymbol{P}_3'$ is rearranged into a matrix according to the inverse operation of "Z" shape, so the block scrambled image P_2 is obtained.

Step 4. The block scrambled image $\boldsymbol{P}_2$ is divided into $\frac{M}{8} \times \frac{N}{8}$ according to the block size of 8×8. In the vertical direction, the i-th and $\boldsymbol{Z}_2(i)$-th blocks of matrix $\boldsymbol{P}_2$ are exchanged from $\frac{N}{8}$ to 1, then the block scrambled image $\boldsymbol{P}_1$ is decrypted by

$$\boldsymbol{P}_1(i) = \boldsymbol{P}_2(\boldsymbol{Z}_2(i)), \quad i = \frac{N}{8}, \frac{N}{8} - 1, \ldots, 1. \tag{22}$$

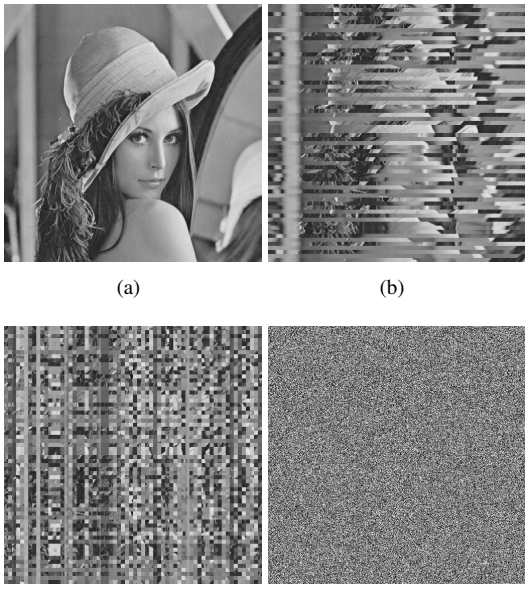
Step 5. In the horizontal direction, the i-th and $Z_1(i)$-th blocks of scrambled image $\boldsymbol{P}_1$ are exchanged from $\frac{M}{8}$ to 1, and plaintext image $\boldsymbol{P}$ is obtained by

$$\boldsymbol{P}(i) = \boldsymbol{P}_1(\boldsymbol{Z}_1(i)), \quad i = \frac{M}{8}, \frac{M}{8} - 1, \ldots, 1. \tag{23}$$

3.4. Results of experimental simulation. The Lena image is selected for the encryption experiments, the size $M = N = 512$, s = 32515895, Ts = 100, the controller parameters are $\varepsilon = 4.1$ and $\sigma = 2.3$, control positions $(i, j) = (4, 3)$, initial values in Eqn. (9). The experiments of encryption and decryption are based on Matlab R2020b software, and the results are shown in Fig. 4. Obviously, the information of the original image has been encrypted effectively, and the decrypted image can accurately restore by the correct key.

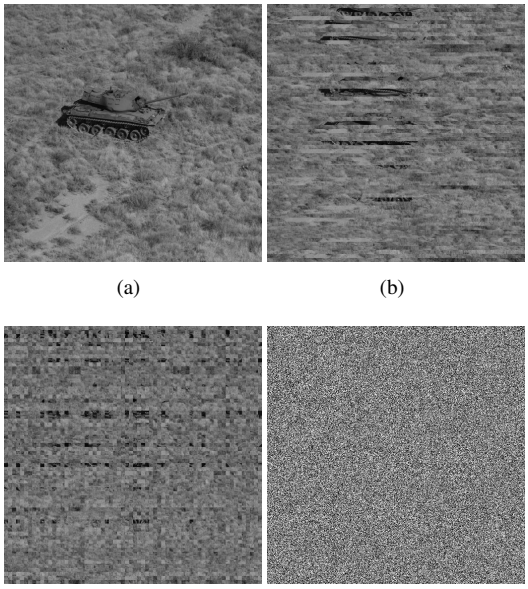
Similarly, the Tank image is selected for the encryption experiments, the size $M = N = 512$, s = 28374107, Ts = 100, the controller parameters are $\varepsilon = 4.1$ and $\sigma = 2.3$, control positions $(i, j) = (4, 3)$, initial values in Eqn. (9), and the results are shown in Fig. 5.

Initial observation indicates that the scrambling and encryption processes achieve thorough disruption of the original image's structural information, though residual discernible fragments persist. Following complete encryption, no original visual information remains recognizable in the processed image. Subsequent statistical analysis will systematically evaluate the cryptographic effectiveness and security robustness of the encryption methodology.



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

Fig. 4. Experimental results of encryption and decryption: Lena image (a), block scrambled image in the horizontal direction (b), block scrambled image (c), encrypted image with XOR diffusion (d).



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

Fig. 5. Experimental results of encryption and decryption: tank image (a), block scrambled image in the horizontal direction (b), block scrambled image (c), encrypted image with XOR diffusion (d).

Table 1. Key space.

Methods	KS
Proposed method	$\gg 2^{997}$
He *et al.*, 2023	2^{436}
Wang and He, 2024	2^{734}

4. Security analysis

4.1. Key space and key sensitivity. Generally, the encryption algorithm is considered secure if the key space (abbreviated as KS) KS $\geqslant 2^{128}$ (Alli and Dinesh Peter, 2021). The KS of proposed algorithm is mainly related to the parameters of $\{\boldsymbol{A}, \varepsilon, \sigma, X(0)\}$, and it is calculated by

$$\begin{aligned} \text{KS} &= (10^{15})^{16} \times (10^{15})^{16} \times (10^{15})^2 \times (10^{16})^3 \times 10^{17} \\ &= 10^{575} \gg 10^{300} \approx 2^{997} \gg 2^{128}. \end{aligned} \tag{24}$$

Meanwhile, the encryption algorithm has good key sensitivity if the ciphertext cannot be restored successfully by a key with minor errors (Wang *et al.*, 2021).

In Fig. 4, the decrypted image with the correct key is clearly restored for the ciphertext image. However, the decryption results obtained with the small key errors are shown in Fig. 6, and one cannot see any useful information.

Similarly, decrypted images obtained under minor parametric variations exhibit comparable characteristics to those shown in Fig. 6, with no discernible useful information identifiable in the reconstructed outputs.

Table 2. Key sensitivity.

Key errors	Recovered successfully
$\lvert x_1 - x_1' \rvert \geqslant 10^{-16}$	No
$\lvert x_2 - x_2' \rvert \geqslant 10^{-17}$	No
$\lvert x_3 - x_3' \rvert \geqslant 10^{-16}$	No
$\lvert x_4 - x_4' \rvert \geqslant 10^{-16}$	No
$\lvert \sigma - \sigma' \rvert \geqslant 10^{-15}$	No
$\lvert \varepsilon - \varepsilon' \rvert \geqslant 10^{-15}$	No
$\lVert \boldsymbol{A} - \boldsymbol{A'} \rVert \geqslant 10^{-15}$	No
$\lVert \boldsymbol{P} - \boldsymbol{P'} \rVert \geqslant 10^{-15}$	No

In Table 2, the key sensitivity of some keys is discussed by experiments, and the results show that a slight change of the key cannot recover the original image. The decrypted images by the key with small error are completely different.

4.2. Histogram and χ^2 tests. The encrypted images have uniformly distributed histogram for a good encryption algorithm (Sun *et al.*, 2021). The histogram of the Lena image and ciphertext is given in Fig. 7, the histogram distribution of the plain text image is uneven, but the ciphertext image is uniform.

Furthermore, Chi-square test χ^2 is a method of non-parametric hypothesis test, and it is used to calculate the fitting degree. The χ^2 test can further show that the cryptosystem has good diffusion effects, and it is given as

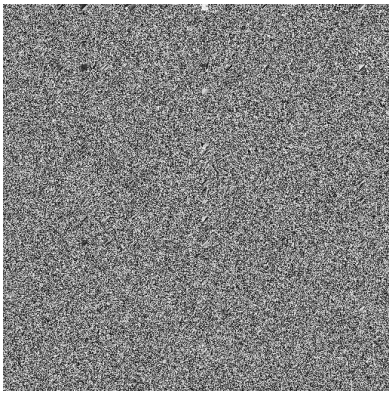


Fig. 6. Decrypted Lena image by the key x_1 with error 10^{-16}.

Table 3. Results of χ^2 test.

Images	Lena	Baboon	Peppers
Plaintext	1.5835×10^5	1.8760×10^5	1.3884×10^5
Ciphertext	286.6738	261.5820	256.9414

(Zhu *et al.*, 2018)

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - g_i)}{g_i}, \tag{25}$$

where f_i is the frequency of pixels (0 to 255), g_i is the ideal frequency. If the freedom degree of χ^2 test is 255 and the significance level is 0.05, then ${\chi^2}_{0.05}(255) = 293.25$.

The χ^2 test analysis in Table 3 reveals distinct statistical characteristics: original images exhibit χ^2 values significantly exceeding the critical value at $\alpha = 0.05$ (293.25), while encrypted images demonstrate compliant values below this threshold. This statistical divergence confirms the ciphertext's effective concealment of plaintext statistical patterns, achieving χ^2 distribution alignment with theoretical randomness requirements.

4.3. Information entropy. The distribution of pixel values in an image can be shown by the information entropy, and it is calculated as (Alli and Dinesh Peter, 2021)

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i, \tag{26}$$

where p_i is the probability of i.

In information theory, when an 8-bit grayscale image achieves uniform pixel distribution (i.e., all 256 intensity levels occur with equal probability), the information entropy attains its theoretical maximum of 8 bits. This upper bound implies that encrypted images approaching this entropy limit exhibit enhanced resistance to statistical cryptanalysis, with the proposed encryption scheme demonstrating superior security preservation through entropy maximization.

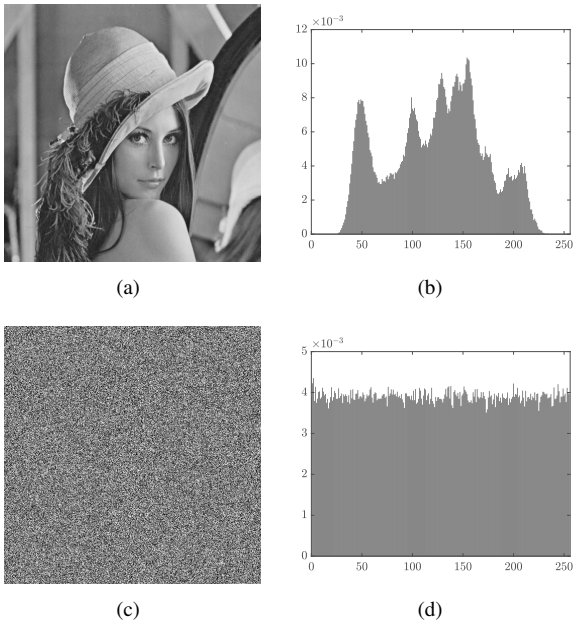


Fig. 7. Histogram analysis of images: original image (a), histogram of original image (b), encrypted image P_3 (c), histogram encrypted image (d).

Table 4. Information entropy.

Images	Plaintext	Ciphertext
Lena	7.4456	7.9914
Baboon	7.3579	7.9918
Peppers	7.5715	7.9915
Kaur *et al.*, 2022	7.4456	7.9768
Folifack Signing *et al.*, 2021	7.5925	7.9757

As quantitatively demonstrated in Table 4, the measured entropy values of encrypted images (ranging from 7.991 to 7.999 bits) closely approach the theoretical maximum of 8 bits. This near-optimal entropy distribution confirms that the proposed encryption scheme demonstrates strong resistance against statistical cryptanalysis attacks, particularly in defeating frequency analysis and histogram-based deciphering attempts.

4.4. Correlation coefficient analysis. Usually, an original image has strong correlation. The correlation coefficient of vectors for the gray values of an image is given by Sethi *et al.* (2022) as well as Zhao and He (2022).

Figure 8 presents directional correlation analyses demonstrating significant reduction in pixel interdependence, with spatial correlation coefficients approaching ideal random distribution levels across horizontal, vertical, and diagonal orientations.

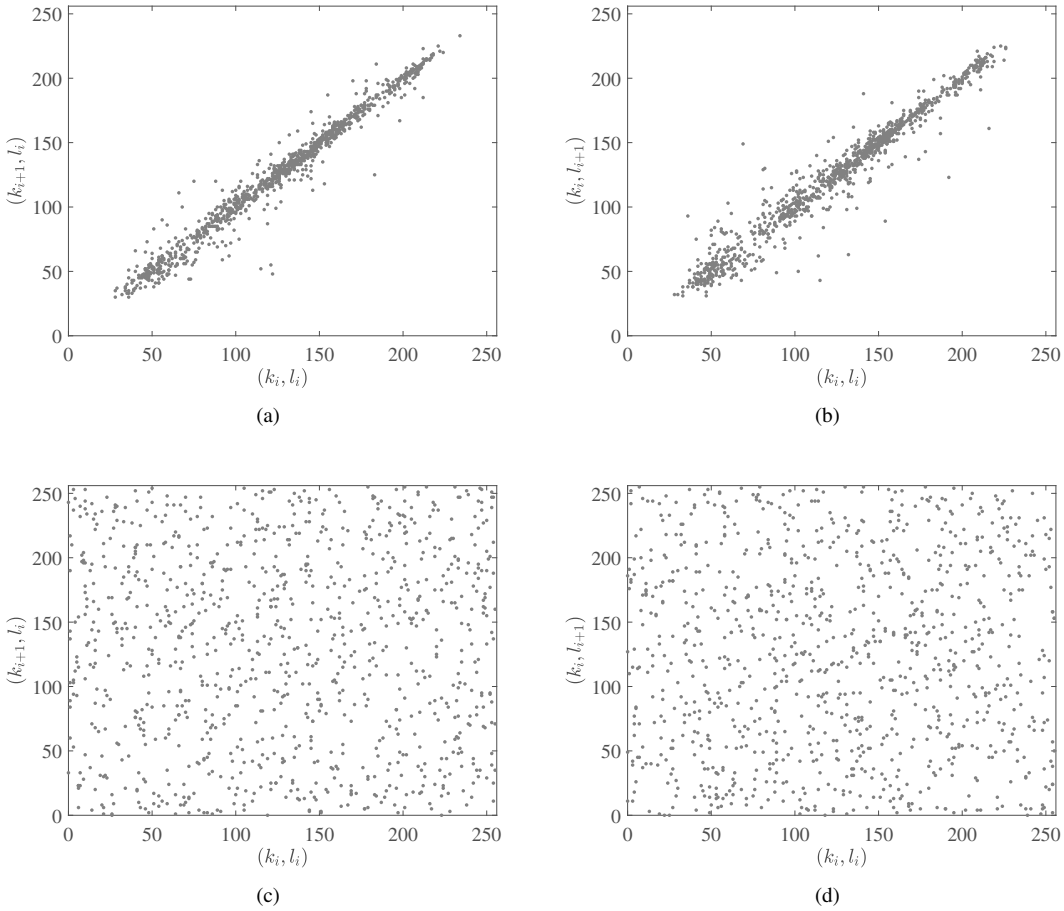


Fig. 8. Correlation analysis of Lena image: horizontal direction (a), vertical direction (b), horizontal direction of the encrypted image (c), vertical direction of the encrypted image (d).

Quantitative analysis of pixel correlation was performed by sampling 1000 pairs of adjacent pixels across horizontal, vertical, and diagonal directions. The correlation coefficients demonstrate significant reduction from pre-encryption values $(0.9831, 0.9737, 0.9666)$ to post-encryption levels $(0.0069, 0.0033, -0.0052)$, effectively approximating ideal random distribution characteristics. This substantial decrease (average reduction $> 95\%$) in spatial correlation confirms the algorithm's successful disruption of pixel relationships, meeting essential criteria for secure image encryption.

4.5. Differential attack. Obviously, two different encrypted images can be obtained if one pixel value of original image is slightly changed. The difference between two encrypted images is given by NPCR and UACI (Musanna *et al*., 2020; Zhao and He, 2022).

A ciphered image P_3 is given by the encryption algorithm, and a new ciphered image CP_3 can be obtained when one pixel value of the plaintext image is changed.

Table 5. Results of NPCR and UACI (%).

Images	NPCR	UACI
Lena	99.6136	33.5126
Baboon	99.6220	33.5074
Peppers	99.6216	33.4875
Akkasaligar and Biradar, 2020	99.8700	33.2900
Lone *et al.*, 2021	99.2400	33.3873

For example, the 100th pixel values of images (Lena, Baboon and Peppers) are changed from (90, 64,13) to (91, 65,14), then three new encrypted images are obtained by the proposed encryption method. The results of the encrypted images are shown in Table 5, and they approach to the expected values 99.6094 and 33.4635, respectively.

Note 3. The initial values are related to the original image. For example, if the initial values are given in Eqn. (9), and s $= 32515895$, one has $(3 + 2 + 5 + 1 + 5 + 8 + 9 + 5) \times 10^{-2} = 0.38$, then the new initial values are $X_0' = (0.2, 0.1, 0.2, 0.1 + 0.38)$. So, the initial values will

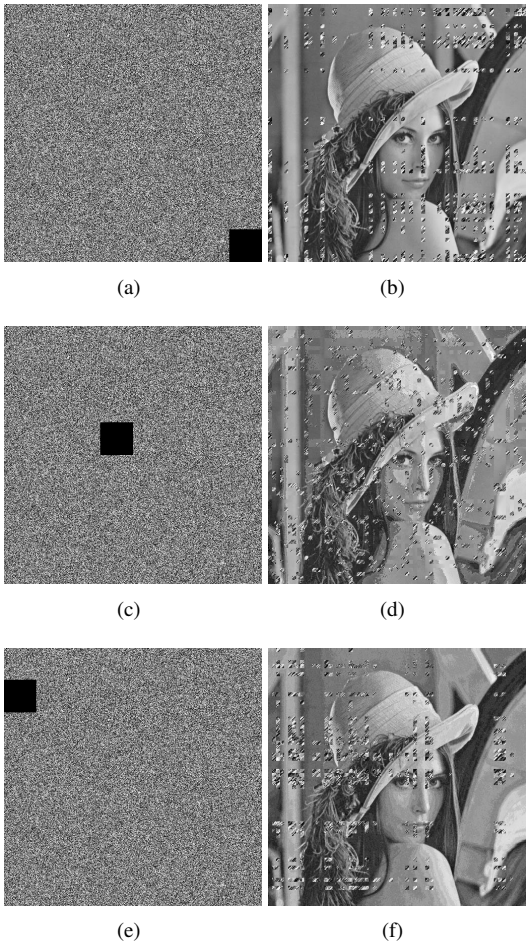


Fig. 9. Results of a crop attack: cropped 1/64 in top-left corner of Fig. 4(d) (a), decrypted image of Fig. 9(a) (b), cropped 1/64 in the middle of Fig. 4(d) (c), decrypted image of Fig. 9(c) (d), cropped 1/64 in the bottom-right corner of Fig. 4(d) (e), decrypted image of Fig. 9(e) (f).

be changed by the different images.

4.6. Crop attack. There also exists crop attack during the transmission process, so the ciphered image should be restored when part of the data is lost (Wang *et al.*, 2020). Therefore, if the encrypted images are cut in different positions, i.e., the pixel values of these blocks are changed to 0, then these images are decrypted by the correct keys.

In Fig. 9, the decrypted images are shown when the encrypted images are cropped in upper-left, center and lower-right corner with size of 1/64, respectively. Obviously, the original images can be recovered with some error. Similarly, the original image may be recovered roughly if the encrypted images are cropped by 1/64, so the proposed algorithm can resist to the crop attack to some extent.

To evaluate the algorithm's resilience against cropping attacks, a comparative analysis of recovery accuracy using statistical evaluation is presented in Table 6, the average relative error (ARE) serves as the key metric for quantifying reconstruction quality.

Table 6. Errors of recovered image by crop attack.

Image	Size	Position	ARE	Proportion of different pixels
Lena	1/64	Upper-left	0.07	50.34%
	1/64	Center	0.34	29.35%
	1/64	Lower-right	0.29	6.39%
Benoon	1/64	Upper-left	0.24	55.65%
	1/64	Center	0.16	27.48%
	1/64	Lower-right	0.30	5.77%

Note 4. The proposed encryption algorithm in Eqn. (19) exhibits reduced noise resistance capability due to its dependency on adjacent plaintext pixels. During decryption, the iterative reliance on preceding plaintext information causes error propagation where pixel restoration errors accumulate sequentially along the encryption order. This phenomenon is empirically validated in Table 6, i.e., images cropped at earlier positions demonstrate significantly higher error ratios in restoration $(50\% - 60\%)$, while those cropped at later positions maintain lower pixel error rates $(1\% - 10\%)$. The progressive error mitigation confirms the algorithm's position-sensitive error propagation characteristics.

4.7. NIST test. NIST tests include 15 kinds of tests, and the sequences are random if $P_{\text{value}} \geqslant 0.01$ (Kumar *et al.*, 2022).

According to the chaotic sequences in Eqns. (13) and (14), the sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$ are obtained. One gets the sequences $\boldsymbol{Z}_i$ $(i = 1, 2, 3)$ by Eqn. (15). In Tables 7 and 8, the sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$ and $\boldsymbol{Z}_i$ $(i = 1, 2, 3)$ can all pass NIST tests.

5. Conclusions

A new four-dimensional chaotic system is constructed based on a stable linear system with a non-smooth controller. Through modulus and multiplication operations applied to this chaotic system, novel sequences are generated that successfully pass the NIST statistical tests. An image encryption algorithm is developed using block scrambling combined with Z-shaped XOR diffusion encryption. The proposed algorithm demonstrates high sensitivity to parameters of the four-dimensional chaotic system while maintaining a sufficiently large key space to resist brute-force attacks. Security analysis validates its robustness against various attacks including differential cryptanalysis and cropping attacks. Experimental results confirm that chaotic

Table 7. Test results of NIST for sequences $\boldsymbol{R}_i$ $(i = 1, 2, 3, 4)$.

Items	$\boldsymbol{R}_1$	$\boldsymbol{R}_2$	$\boldsymbol{R}_3$	$\boldsymbol{R}_4$
Frequency	0.6371	0.8677	0.1453	0.9463
Block frequency	0.5544	0.3041	0.8165	0.9114
Cumulative sums	0.7639	0.8207	0.3999	0.8376
Runs	0.9114	0.1816	0.8165	0.3345
Longest Run	0.8165	0.4944	0.5141	0.6371
Rank	0.7981	0.7399	0.9241	0.5955
FFT	0.9835	0.6993	0.5955	0.5749
Non-overlapping template	0.4990	0.4658	0.4485	0.4640
Overlapping template	0.2622	0.0205	0.2897	0.0457
Universal	0.4559	0.1816	0.3345	0.2622
Approximate entropy	0.2757	0.6371	0.4559	0.2927
Random excursions	0.5492	0.4216	0.4224	0.2927
Random excursions variant	0.5328	0.4074	0.4353	0.4696
Serial	0.3882	0.6495	0.3999	0.0618
Linear complexity	0.9114	0.3505	0.0192	0.3669

Table 8. Test results of NIST for sequences $\boldsymbol{Z}_i$ $(i = 1, 2, 3)$.

Items	$\boldsymbol{Z}_1$	$\boldsymbol{Z}_2$	$\boldsymbol{Z}_3$
Frequency	0.6371	0.8677	0.1538
Block frequency	0.5544	0.3041	0.5544
Cumulative sums	0.7639	0.8207	0.4808
Runs	0.9114	0.1816	0.5749
Longest run	0.7399	0.5955	0.5955
Rank	0.3191	0.3838	0.9717
FFT	0.9835	0.6993	0.7792
Non-overlapping template	0.4990	0.4658	0.5050
Overlapping template	0.5141	0.2622	0.3345
Universal	0.4559	0.1816	0.5749
Approximate entropy	0.2757	0.6371	0.2023
Random excursions	0.5492	0.4216	0.4946
Random excursions variant	0.5328	0.4074	0.4972
Serial	0.3882	0.6495	0.3245
Linear complexity	0.4012	0.7197	0.5955

behavior persists in non-smooth controlled systems, and the developed chaos-based encryption algorithm exhibits superior security characteristics. This demonstrates its strong potential for future applications in information security and cryptographic systems.

Acknowledgment

This work is supported by the Natural Science Foundation of Fujian Province (no. 2022J01895), the Digital Fujian Meteorological Big Data Research Institute, the Key Laboratory of Data Science and Statistics, and the Fujian Key Laboratory of Granular Computing and Applications (Minnan Normal University), China.

References

Akkasaligar, P.T. and Biradar, S. (2020). Selective medical image encryption using DNA cryptography, *Information Security Journal: A Global Perspective* **29**(2): 91–101.

Al Solami, E., Ahmad, M., Volos, C., Doja, M.N. and Beg, M.M.S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes, *Entropy* **20**(7): 525.

Alli, P. and Dinesh Peter, J. (2021). A novel auto-encoder induced chaos based image encryption framework aiding DNA computing sequence, *Journal of Intelligent & Fuzzy Systems* **41**(1): 181–198.

Banu S, A. and Amirtharajan, R. (2020). A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach, *Medical & Biological Engineering & Computing* **58**(7): 1445–1458.

Chen, L., Yin, H., Huang, T., Yuan, L., Zheng, S. and Yin, L. (2020). Chaos in fractional-order discrete neural networks with application to image encryption, *Neural Networks* **125**: 174–184.

Folifack Signing, V., Fozin Fonzin, T., Kountchou, M., Kengne, J. and Njitacke, Z.T. (2021). Chaotic jerk system with hump structure for text and image encryption using DNA coding, *Circuits, Systems, and Signal Processing* **40**(9): 4370–4406.

Fu, X.-Q., Liu, B.-C., Xie, Y.-Y., Li, W. and Liu, Y. (2018). Image encryption-then-transmission using DNA encryption algorithm and the double chaos, *IEEE Photonics Journal* **10**(3): 1–15.

Gao, H. and Gao, T. (2019). Double verifiable image encryption based on chaos and reversible watermarking algorithm, *Multimedia Tools and Applications* **78**(6): 7267–7288.

He, J., Qiu, W. and Cai, J. (2023). Synchronization of hyperchaotic systems based on intermittent control and its application in secure communication, *Journal of Advanced Computational Intelligence and Intelligent Informatics* **27**(2): 292–303.

He, J. and Yu, S. (2019). Construction of higher-dimensional hyperchaotic systems with a maximum number of positive Lyapunov exponents under average eigenvalue criteria, *Journal of Circuits, Systems and Computers* **28**(09): 1950151.

Huang, H., Chen, Y. and Cheng, D. (2022). Plaintext-related image encryption scheme based on chaos and game of life, *Journal of Electronic Imaging* **31**(1): 013031.

Kaur, G., Agarwal, R. and Patidar, V. (2022). Color image encryption scheme based on fractional Hartley transform and chaotic substitution-permutation, *The Visual Computer* **38**(3): 1027–1050.

Khaitan, S., Sagar, S. and Agarwal, R. (2020). Public key cryptosystem based on optimized chaos-based image encryption, *Journal of Computational and Theoretical Nanoscience* **17**(12): 5217–5223.

Kumar, V., Rayappan, J.B.B., Amirtharajan, R. and Praveenkumar, P. (2022). Quantum true random number

generation on IBM's cloud platform, *Journal of King Saud University—Computer and Information Sciences* **34**(8): 6453–6465.

Li, G. and Han, X. (2021). A color image encryption algorithm with cat map and chaos map embedded, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **29**(Supp01): 73–87.

Lone, P.N., Singh, D. and Mir, U.H. (2021). A novel image encryption using random matrix affine cipher and the chaotic maps, *Journal of Modern Optics* **68**(10): 507–521.

Mondal, B. and Singh, J.P. (2022). A lightweight image encryption scheme based on chaos and diffusion circuit, *Multimedia Tools and Applications* **81**(24): 34547–34571.

Musanna, F., Dangwal, D., Kumar, S. and Malik, V. (2020). A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor, *Imaging Science Journal* **68**(1): 24–40.

Peechara, R.R. and Sucharita, V. (2021). A chaos theory inspired, asynchronous two-way encryption mechanism for cloud computing, *PeerJ Computer Science* **59**(3): e628.

Rajakumaran, C. and Kavitha, R. (2020). Chaos based encryption of quantum images, *Multimedia Tools and Applications* **79**(33): 23849–23860.

Ramakrishnan, A., Ramalingam, R., Ramalingam, P., Ravi, V., Alahmadi, T.J. and Maidin, S.S. (2024). A novel chaotic binary butterfly optimization algorithm based feature selection model for classification of autism spectrum disorder, *International Journal of Applied Mathematics and Computer Science* **34**(4): 647–660, DOI: 10.61822/amcs-2024-0043.

Ravichandran, D., Banu S, A., Murthy, B., Balasubramanian, V., Fathima, S. and Amirtharajan, R. (2021). An efficient medical image encryption using hybrid DNA computing and chaos in transform domain, *Medical & Biological Engineering & Computing* **59**(3): 589–605.

Riyahi, M., Kuchaki Rafsanjani, M. and Motevalli, R. (2021). A novel image encryption scheme based on multi-directional diffusion technique and integrated chaotic map, *Neural Computing and Applications* **33**(21): 14311–14326.

Sethi, J., Bhaumik, J. and Chowdhury, A.S. (2022). Chaos-based uncompressed frame level video encryption, *Proceedings of the 7th International Conference on Mathematics and Computing: ICMC 2021, Shibpur, India,* pp. 201–217.

Singh, R.K., Kumar, B., Shaw, D.K. and Khan, D.A. (2021). Level by level image compression-encryption algorithm based on quantum chaos map, *Journal of King Saud University—Computer and Information Sciences* **33**(7): 844–851.

Song, Y., Zhu, Z., Zhang, W., Guo, L., Yang, X. and Yu, H. (2019). Joint image compression–encryption scheme using entropy coding and compressive sensing, *Nonlinear Dynamics* **95**(3): 2235–2261.

Sun, Y., Zhang, H., Wang, X. and Wang, M. (2021). Bit-level color image encryption algorithm based on coarse-grained logistic map and fractional chaos, *Multimedia Tools and Applications* **80**(8): 12155–12173.

ul Haq, T. and Shah, T. (2020). Algebra-chaos amalgam and DNA transform based multiple digital image encryption, *Journal of Information Security and Applications* **54**: 102592.

Wang, M., Wang, X., Wang, C., Xia, Z., Zhao, H., Gao, S., Zhou, S. and Yao, N. (2020). Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption, *Chaos, Solitons & Fractals* **139**: 110028.

Wang, M., Wang, X., Zhao, T., Zhang, C., Xia, Z. and Yao, N. (2021). Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme, *Information Sciences* **544**: 1–24.

Wang, S. and He, J. (2024). Design of chaotic systems with multiple scrolls via anti-control method and its encryption application, *IAENG International Journal of Applied Mathematics* **54**(12): 2636–2644.

Wu, J., Wang, L., Chen, G. and Duan, S. (2016). A memristive chaotic system with heart-shaped attractors and its implementation, *Chaos, Solitons & Fractals* **92**: 20–29.

Xiao, Y., Cao, J., Wang, Z., Long, C., Liu, Y. and He, J. (2019). Polar coded optical OFDM system with chaotic encryption for physical-layer security, *Optics Communications* **433**: 231–235.

Xiao, Y., Tong, X., Zhang, M. and Wang, Z. (2022). Image lossless encoding and encryption method of EBCOT Tier1 based on 4D hyperchaos, *Multimedia Systems* **28**(3): 727–748.

Zhang, Y. (2021). A new unified image encryption algorithm based on a lifting transformation and chaos, *Information Sciences* **547**: 307–327.

Zhang, Y., He, Y., Zhang, J. and Liu, X. (2022). Multiple digital image encryption algorithm based on chaos algorithm, *Mobile Networks and Applications* **27**(4): 1349–1358.

Zhao, K. and He, J. (2022). Design of higher-dimensional hyperchaotic system based on combined control and its encryption application, *International Journal of Advanced Computer Science and Applications* **13**(7): 869–879.

Zhu, S., Zhu, C. and Wang, W. (2018). A new image encryption algorithm based on chaos and secure hash SHA-256, *Entropy* **20**(9): 716.

Jianbin He received his PhD degree from the Guangdong University of Technology, China, in 2017. He was a lecturer at the School of Mathematics and Statistics, Minnan Normal University, China, in the years 2017–2020. He is currently an associate professor there. His research interests include chaos theory and its application, chaos-based cryptography.

Kun Zhao received his BS degree from Heze University, China, in 2020. He is currently studying for an MS degree at the School of Mathematics and Statistics, Minnan Normal University, China. His research interests include higher-dimensional chaotic system and their encryption application.

Shiya Wang received her BS degree from Heze University, China, in 2022. She is currently studying for an MS degree at the School of Mathematics and Statistics, Minnan Normal University, China. Her research interests include multi-scrolls attractors and their encryption application.

Received: 5 January 2025
Revised: 9 April 2025
Accepted: 13 May 2025