Nonlinear Dyn (2023) 111:20425–20446
https://doi.org/10.1007/s11071-023-08866-0

ORIGINAL PAPER

Construction of new 5D Hamiltonian conservative hyperchaotic system and its application in image encryption

Xiangyang Ning · Qing Dong · Shihua Zhou · Qiang Zhang · Nikola K. Kasabov

Received: 24 April 2023 / Accepted: 14 August 2023 / Published online: 7 September 2023

Abstract While the Internet has made great progress in facilitating modern life, the importance of protecting information security becomes increasingly prominent. In this research, a novel image encryption method depending on the five-dimensional (5D) Hamiltonian conservative hyperchaotic system has been put forward. And the hyperchaotic system is constructed based on the theoretical foundation of Euler equation and energy analysis. Unlike dissipative chaotic systems, conservative chaotic systems have better ergodicity because there is no attractor. Moreover, there are two or greater Lyapunov exponents above zero in hyperchaotic systems, which leads to higher complexity. Therefore, the new 5D Hamiltonian conservative hyperchaotic system has stronger randomness, and it has more advantages in image encryption. In addition, we designed a new bit-plane segmentation method that combines bit diffusion to strengthen the diffusion effect and encryption reliability. Encryption experiments and the performance analyses illustrate that this proposed encryption method is provided with strong security and practicability.

Keywords Information security · Image encryption · 5D Hamiltonian conservative hyperchaotic system · Bit-plane segmentation

X. Ning · Q. Dong · S. Zhou (✉) · Q. Zhang (✉)
Key Laboratory of Advanced Design and Intelligent Computing, Ministry of Education, School of Software Engineering, Dalian University, Dalian 116622, People's Republic of China
e-mail: zhoushihua@dlu.edu.cn

Q. Zhang
e-mail: zhangq@dlu.edu.cn

X. Ning
e-mail: ningxiangyang@s.dlu.edu.cn

Q. Dong
e-mail: dongqing@s.dlu.edu.cn

Q. Zhang
School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, People's Republic of China

N. K. Kasabov
Knowledge Engineering and Discovery Research Institute, Auckland University of Technology, Auckland 1010, New Zealand
e-mail: nkasabov@aut.ac.nz

N. K. Kasabov
Intelligent Systems Research Center, Ulster University, Londonderry BT52 1SA, UK

N. K. Kasabov
Auckland Bioengineering Institute (ABI), The University of Auckland, Auckland 1010, New Zealand

1 Introduction

Along with the rapid development of 5G network transmission technology, digital images have become the major carrier of information in the network. However, while Internet technology has facilitated communication, it has also brought security risks that cannot be ignored. Therefore, how to ensure the secure transmission of image information in the network has become a hot research direction of scholars.

Encrypting images through encryption algorithms is one of the effective methods to safeguard the image security. However, because of the features of digital images, for instance, large amount of information, high correlation and data redundancy, classical encryption algorithms DES, AES, IDEA, etc., fail to satisfy the requirements of digital image encryption commendably [1]. For this reason, the exploration of new encryption methods to encrypt image data is absolutely necessary. So far, scholars have designed many different types of image encryption methods, which are mostly on the basis of chaos [2,3], DNA encoding [4,5], compressed sensing [6–8] and other theories [9–12]. In the above schemes, chaotic systems have strong initial value sensitivity, ergodicity and unpredictability, which make chaotic systems naturally related to encryption in cryptography [13]. Therefore, encryption algorithms combined with chaotic systems have become an important research topic.

Friedrich [14] utilized the chaotic system to image encryption firstly and proposed the general structure of image encryption, "permutation and diffusion." With the deepening of research, a variety of image encryption methods based on chaos have been proposed. To reduce the computational complexity of the algorithm calculations and elevate the effectiveness of the permutation process, Wang et al. [15] constructed an encryption method for colorful images through applying piecewise linear chaotic map to perform random permutation on heterogeneous planes. Li et al. [16] improved the tent map to make its initial conditions and parameters very sensitive to subtle changes, enhancing the encryption safety. Wang et al. [17] devised a novel encryption scheme by combining DNA coding rules and the improved logistic map, while the fact that this scheme increases the key space, its efficiency of encryption is reduced. Zheng et al. [18] invented a modified 2D logistic sine map and proposed a unique encryption algorithm that combined with dynamic DNA sequence, which increases the complexity and security of this encryption scheme. Based on 3D chaotic maps, Qian et al. [19] designed an efficient color image encryption scheme, but this encryption scheme has certain requirements on the magnitude of original images.

The encryption schemes mentioned above are all proposed based on low-dimensional chaotic systems. Although they can achieve the purpose of image encryption, with the advancement of chaos research, disadvantages of low-dimensional chaotic systems have been gradually exposed [20]. Because the state space of the low-dimensional chaotic system is small, its system behavior is simpler and easier to analyze than the high-dimensional chaotic system, which leads to the poor security of image encryption algorithm based on low-dimensional chaos. Therefore, the research hotspot now gradually shifts to the study of new image encryption methods based on high-dimensional chaotic systems. Currently, there have been some encryption algorithms proposed based on high-dimensional dissipative chaotic systems [21–23]. However, dissipative chaotic systems are also not very secure when applied to encryption. Since dissipative systems have attractors, its trajectory cannot reach most of the space near the attractors; the ergodicity is poor. And the risk of the attacker cracking the encryption scheme by reconstructing the attractors is greatly increased.

In contrast to dissipative chaotic systems, for conservative chaotic systems, there are no attractors and no risk of being attacked by reconstructed attractors, and its trajectory can almost traverse the entire phase space. Especially for the Hamiltonian conservative chaotic system, in addition to phase space conservation, its Hamiltonian energy is always conserved, so that Hamiltonian conservative chaotic systems have stronger ergodicity than dissipative systems. In addition, hyperchaotic systems have at least two LEs greater than 0, which exhibit higher randomness compared to other systems. Therefore, we design a novel 5D Hamiltonian conservative hyperchaotic system by constructing the Euler rotation equation, and the energy analysis of the system proves that chaos can be generated. With this as a framework, we construct a novel image encryption scheme, which can realize the secure encryption of any gray and color images. Moreover, we also propose a new bit-plane segmentation method and a bit-plane diffusion operation to enhance the effect of image diffusion. Simulation results and security analysis show that our algorithm is more secure than other algorithms.

The subsequent parts of this paper are constituted as described in the following. In Sect. 2, the design and construction of a novel 5D Hamiltonian conservative hyperchaotic system is recommended, and its Hamiltonian energy and Casimir energy are analyzed. Section 3 explores the fundamental features of this new system. Section 4 designs a new image encryption method using this novel chaotic system. Section 5 simulates the devised encryption method and compares the safety and reliability analysis results with other encryption methods. Finally, Sect. 6 summarizes this paper.

2 System design and model construction

2.1 Prerequisites

Maschke et al. [24] constructed a generalized Hamiltonian system to study the stability of forced Hamiltonian system with dissipation. It can be described as

$$\begin{cases} \dot{\mathbf{x}} = [J(\mathbf{x}) - R(\mathbf{x})]\nabla H(\mathbf{x}) + g(\mathbf{x})u \\ y = g^T(\mathbf{x})\nabla H(\mathbf{x}) \end{cases} \tag{1}$$

where $\mathbf{x}$ is the state variable vector, and $\mathbf{x} = [x_1, \ldots, x_n]^T$; $J(\mathbf{x})$ is a symplectic matrix and satisfies $J(\mathbf{x}) = -J^T(\mathbf{x})$, which represents the conservative part of the system; $R(\mathbf{x})$ is a positive semi-definite matrix, which satisfies $R(\text{x}) = R^T(\text{x})$, represents the energy dissipation part of the system. $H(\mathbf{x})$ represents the Hamiltonian energy function of the system; $g(\mathbf{x})$ and u represent the input gain vector and the input of the generalized force received by the system, respectively; and y is the output of the system.

The variation of the Hamiltonian energy $H(\mathbf{x})$ is related to the internal dissipation and the external energy exchange of the system, which can be expressed as

$$\frac{\mathrm{d}H}{\mathrm{d}t} = -\nabla H^T(\mathbf{x})R(\mathbf{x})\nabla H(\mathbf{x}) + u^T y \tag{2}$$

When the external input and the energy dissipation term in Eq. (2) are 0, the Hamiltonian energy of the system is conserved. In this case, the system is called the generalized Hamiltonian conservative system, and its differential equation can be described as:

$$\dot{\mathbf{x}} = J(\mathbf{x})\nabla H(\mathbf{x}) \tag{3}$$

2.2 Construct the 5D Euler equation

The Euler rotation equation is often used to describe the motion of rotating rigid bodies and incompressible fluids [25], which has great value in the field of classical mechanics. According on the theory of [26–28], Euler rotation equation can be used to describe dissipative chaotic systems, its corresponding Hamiltonian vector field conforms to the generalized Hamiltonian system shown in Eq. (1). And the generalized Hamiltonian conservative system can be derived by constructing the Euler equation of rigid body without external force. Then, by adding external constants to break the Casimir energy conservation, it is possible to create a Hamiltonian conservative chaotic system [27–30]. Furthermore, the dynamic specifics of this chaotic system can be validated through analyzing the Casimir energy and Hamiltonian energy.

According to the above theory, a 5D Euler rotation equation describing the motion of a rigid body without external force is designed, which is denoted as system Σ_5, and its Hamiltonian vector field satisfies the generalized Hamiltonian conservative system shown in Eq. (3).

And the Hamiltonian energy function $H(\mathbf{x})$ of system Σ_5 can be obtained as

$$H(\mathbf{x}) = \frac{1}{2}\sum_{i=1}^{5} \Pi_i {x_i}^2 \tag{4}$$

where x_i expresses the rotational angular momentum, $i = 1, 2, 3, 4, 5$. $\Pi_i = I_i^{-1}$, and I_i is the principal moment of inertia. In addition, the gradient function of $H(\mathbf{x})$ is $\nabla H(\mathbf{x}) = [\Pi_1 x_1, \Pi_2 x_2, \Pi_3 x_3, \Pi_4 x_4, \Pi_5 x_5]^T$.

Moreover, $J(\mathbf{x})$ is a symplectic matrix, which is defined as

$$J(\mathbf{x}) = \begin{bmatrix} 0 & x_4 & 0 & -x_2 & 0 \\ -x_4 & 0 & -x_5 & x_1 & x_3 \\ 0 & x_5 & 0 & 0 & -x_2 \\ x_2 & -x_1 & 0 & 0 & 0 \\ 0 & -x_3 & x_2 & 0 & 0 \end{bmatrix} \tag{5}$$

The variation of Hamiltonian energy for system Σ_5 can be denoted as the differential of the Hamiltonian energy with time. Since $J(\mathbf{x})$ of system Σ_5 is a symplectic matrix, $J(\mathbf{x}) = -J^T(\mathbf{x})$, and $\dot{H}(\mathbf{x})$ can be calculated from Eq. (6).

$$\dot{H}(\mathbf{x}) = \nabla H(\mathbf{x})^T J(\mathbf{x})\nabla H(\mathbf{x}) = 0 \tag{6}$$

Within the rigid body dynamic realm, Casimir energy function C plays a significant role, and is a powerful means of describing dynamic systems and analyzing their stability conditions. According to reference [27–30], it is found that Casimir energy has an important relationship with whether the system can produce chaos. Chaos cannot occur in a system when both its Hamiltonian energy and Casimir energy are conservative. Analyzing the Casimir energy of system Σ_5, the function of Casimir energy changing with time is known as the Casimir power $\dot{C}$, which is defined as

$$\dot{C} = \{C, H\} = \nabla C(\mathbf{x})^T \cdot \dot{\mathbf{x}} \tag{7}$$

And the Casimir energy gradient function is $\nabla C(\mathbf{x}) = [x_1, x_2, x_3, x_4, x_5]^T$; thus, the Casimir power can be obtained as

$$\dot{C} = \nabla C(\mathbf{x})^T J(\mathbf{x}) \nabla H(\mathbf{x}) = 0 \tag{8}$$

According to Eqs. (6) and (8), both the Hamiltonian energy and Casimir energy remain conservative for system Σ_5, so the system Σ_5 cannot generate chaotic behavior. However, it can be regarded as the basic framework for constructing Hamiltonian conservative chaotic system.

2.3 Modeling the 5D Hamiltonian conservative hyperchaotic system

From reference [30], it can be concluded that breaking the conservation of Casimir energy is a crucial element in the formation of chaotic behavior within the system. In order to construct a 5D Hamiltonian conservative chaotic system, we need to break the Casimir energy conservation within system Σ_5. By adding an external nonzero parameter c to $J(\mathbf{x})$ can obtain System Σ_5^H. And $J_C(\mathbf{x})$ can be obtained as

$$J_C(\mathbf{x}) = \begin{bmatrix} 0 & x_4 & 0 & -x_2 & 0 \\ -x_4 & 0 & -x_5 & x_1 & x_3 \\ 0 & x_5 & 0 & 0 & -x_2 \\ x_2 & -x_1 & 0 & 0 & -c \\ 0 & -x_3 & x_2 & c & 0 \end{bmatrix} \tag{9}$$

System Σ_5^H is denoted as

$$\dot{\mathbf{x}} = J_C(\mathbf{x}) \nabla H(\mathbf{x}) \tag{10}$$

For system Σ_5^H, its mathematical model is expressed by

$$\begin{cases} \dot{x}_1 = (\Pi_2 - \Pi_4)x_2x_4 \\ \dot{x}_2 = (\Pi_4 - \Pi_1)x_1x_4 + (\Pi_5 - \Pi_3)x_3x_5 \\ \dot{x}_3 = (\Pi_2 - \Pi_5)x_2x_5 \\ \dot{x}_4 = (\Pi_1 - \Pi_2)x_1x_2 - c\Pi_5x_5 \\ \dot{x}_5 = (\Pi_3 - \Pi_2)x_2x_3 + c\Pi_4x_4 \end{cases} \tag{11}$$

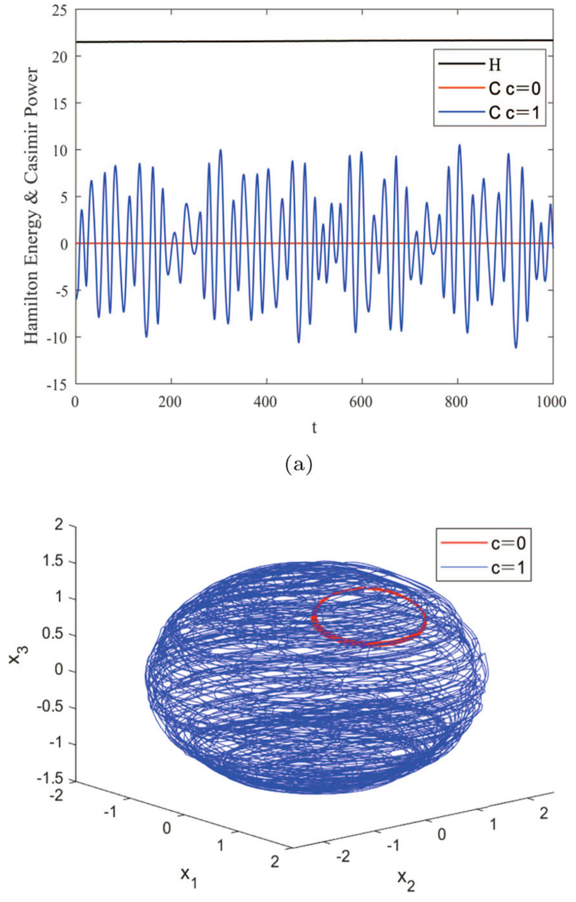
By analyzing the Hamiltonian energy of new system Σ_5^H, the result can be obtained that $\dot{H}(\mathbf{x}) = \nabla H(\mathbf{x})^T J_C(\mathbf{x}) \nabla H(\mathbf{x}) = 0$; hence, its Hamiltonian energy is conservative. However, for system Σ_5^H, its Casmir power can be calculated as

$$\begin{aligned} \dot{C} &= \nabla C^T(\mathbf{x}) J_C(\mathbf{x}) \nabla H(\mathbf{x}) \\ &= c(\Pi_4 - \Pi_5)x_4x_5 \end{aligned} \tag{12}$$

As can be seen from Eq. (12), when $c(\Pi_4 - \Pi_5)x_4x_5 \neq 0$, that is, $c \neq 0$ and $\Pi_4 \neq \Pi_5$, the Casimir energy is not conservative, and system Σ_5^H can produce chaotic behavior.

Furthermore, the above results can also be confirmed through simulation experiments. Set the system control parameters as $(\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5) = (9, 7, 5, 4, 8)$, the initial values $(x_{10}, x_{20}, x_{30}, x_{40}, x_{50}) = (1, 1, 1, 1, 1.5)$. And choose MATLAB ode45 as the solver, the time step is $T = 0.01$. When the parameter c is set to 0, it is equivalent to system Σ_5, and when $c = 1$, it represents to system Σ_5^H. The energy analysis results of system Σ_5 and system Σ_5^H are shown in Fig. 1a. And the black line indicates the Hamiltonian energy of the two systems, indicating that under this parameter, the Hamiltonian energy is always 21.54, which is conserved. Red represents the Casimir power trajectory of system Σ_5, which is always zero, indicating the conservation of Casimir energy. Blue represents the Casimir power trajectory of system Σ_5^H. It can be seen that the trajectory presents irregular oscillation, indicating that its Casimir energy is not conservative. And the phase trajectories of both systems are depicted in Fig. 1b, where the red represents system Σ_5 and the blue represents system Σ_5^H. As Fig. 1b shows, system Σ_5 shows periodic motion, while the trajectory of system Σ_5^H is unstable aperiodic orbits.

The above analysis results demonstrate that the system Σ_5^H with Hamiltonian energy conservation can generate chaos.



(a)

(b)

Fig. 1 System Σ_5 and System Σ_5^H. **a** Energy analysis diagram; **b** the $x_1 - x_2 - x_3$ space phase diagram

3 System analysis

Unless otherwise noted, the default parameters and initial values for this section are $(\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5, c) = (9, 7, 5, 4, 8, 1)$ and $(x_{10}, x_{20}, x_{30}, x_{40}, x_{50}) = (1, 1, 1, 1, 1.5)$, respectively.

3.1 Dynamics analysis

3.1.1 Conservative analysis

For the vector field F, its phase space volume change rate can be expressed by divergence $\nabla \cdot F$ [31]. According to the magnitude of the divergence $\nabla \cdot F$, whether the chaotic system is conservative or dissipative can be distinguished. In the case of $\nabla \cdot F$ being negative, the system is dissipative, and the trajectories gradually gather near the attractor. When $\nabla \cdot F$ equals zero, the system is conservative and has a constant phase volume. For system Σ_5^H, its divergence $\nabla \cdot F$ can be obtained as

$$\begin{aligned} \nabla \cdot F &= \frac{\partial F_{x_1}}{\partial x_1} + \frac{\partial F_{x_2}}{\partial x_2} + \frac{\partial F_{x_3}}{\partial x_3} + \frac{\partial F_{x_4}}{\partial x_4} + \frac{\partial F_{x_5}}{\partial x_5} \\ &= 0 \end{aligned} \tag{13}$$

It can be confirmed from the above equation that system Σ_5^H is conservative.

3.1.2 LEs and bifurcation diagram analysis

Sensitivity to control parameters and initial values is one of the most basic characteristics of chaotic systems. This is usually analyzed by Lyapunov exponents diagram and bifurcation diagram. And in this section, Fig. 2 illustrates the LEs diagram and bifurcation diagram varying with initial value x_{20}.

From Fig. 2a, it can be found that the sum of LEs is always 0, and there are always two positive LEs greater than 0 within a wide initial value range, indicating that system Σ_5^H has high stability and complexity. Moreover, Fig. 2b manifests that as the initial values increase, the phase space traversal range expands. Furthermore, the unpredictability of sequences produced by system Σ_5^H is also stronger.

Specifically, when $x_{20} = 1$, the LEs of system Σ_5^H are calculated to be $(0.6030, 0.0037, 0.0001, -0.0050, -0.6018)$, the sum of all LEs is 0, and there are two positive LEs $LE_1 = 0.6030$ and $LE_2 = 0.0037$, which satisfy the characteristics of conservative hyperchaotic systems. And the Lyapunov dimension of system Σ_5^H can also be given by the Kaplan–Yorke form:

$$\begin{aligned} D &= 4 + \frac{0.6030 + 0.0037 + 0.0001 - 0.0050}{0.6018} \\ &= 5 \end{aligned} \tag{14}$$

As Eq. (14) shows, the Lyapunov dimension of system Σ_5^H is an integer dimension, which conforms to the characteristics of conservative systems.

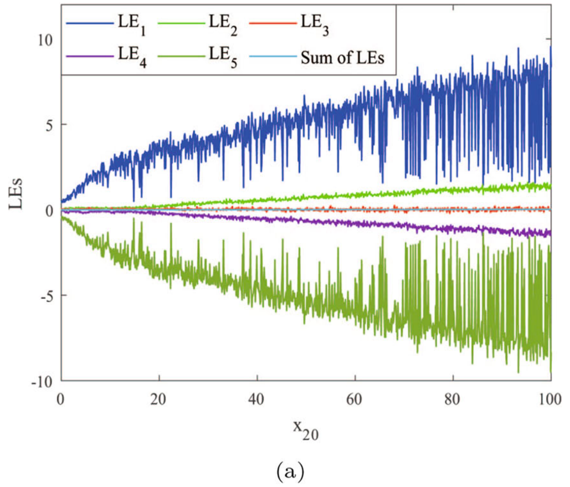


Fig. 2 System Σ_5^H. **a** LEs with initial value x_{20}; **b** bifurcation diagram with initial value x_{20}

3.1.3 *Phase diagram and Poincaré section diagram analysis*

Phase diagram is a relatively intuitive method to observe the movement trajectory of chaotic system. Figure 3 displays the partial phase diagrams of system Σ_5^H. The motion trajectory of system Σ_5^H fills almost the entire phase space, which proves that system Σ_5^H has strong ergodicity and high complexity.

Poincaré section diagram is a common method to analyze the motion state of the system. Figure 4 shows the Poincaré section diagrams of a partial plane for system Σ_5^H. The Poincaré section of system Σ_5^H covers almost the entire trajectory and has no stable line or closed loop, which proves the chaos of the system.

3.1.4 *Initial value sensitivity analysis*

The system parameters sensitivity and initial values sensitivity to chaotic systems are two crucial properties that ensures the safety of encryption applications. To observe the effect of various initial values on system Σ_5^H, we selected different initial values and obtained the corresponding chaotic sequences within the time $t \in [0, 100]$, and the sampling time is 0.5. The results are shown in Fig. 5.

As depicted in Fig. 5, minor differences in the initial values lead to significant variations in the resulting chaotic sequences, highlighting the extreme sensitivity to initial conditions of system Σ_5^H.

3.2 Pseudo-randomness analysis

The safety of chaotic encryption applications is directly associated with the randomness of chaotic sequences. In an effort to confirm the randomness of system Σ_5^H, we apply the United States National Institute of Standards and Technology (NIST) SP80022 standard [32] to appraise the test data, which is the chaotic sequence produced by system Σ_5^H. NIST offers 15 statistical tests to appraise the stochasticity of random sequences or pseudo-random number generators. Each statistical test is given a P value, and by judging the P values, it is determined whether the sequence is random. For a pseudo-random sequence, its NIST test results should satisfy three conditions:

(1) Select the default significance level $\alpha = 0.01$, and for each test item, the P value cannot be less than α;
(2) Select the test sequence data length as l million bits, and divide the data into s groups equally, and the confidence interval can be calculated by $\hat{p} \pm 3\sqrt{\hat{p}(1-\hat{p})/s}$, where $\hat{p} = 1 - \alpha$. Set $l = 100$, $s = 100$, the proportion of P values that are greater than or equal to α should be within the confidence interval [0.9602, 1] [33];
(3) P values distribution obeys uniformity.

Set the parameters as $(\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5, c) = (9, 7, 5, 4, 8, 1)$, and the initial values as $(x_{10}, x_{20}, x_{30}, x_{40}, x_{50}) = (1, 1, 1, 1, 1.5)$. Select the time interval $t \in [0, 200]$ and the sample time $T = 10^{-5}$ to generate chaotic sequences x_1, x_2, x_3, x_4, x_5. Then, the chaotic sequence X with a length of 100 million bits can be obtained, and $X = [x_1, x_2, x_3, x_4, x_5]$.

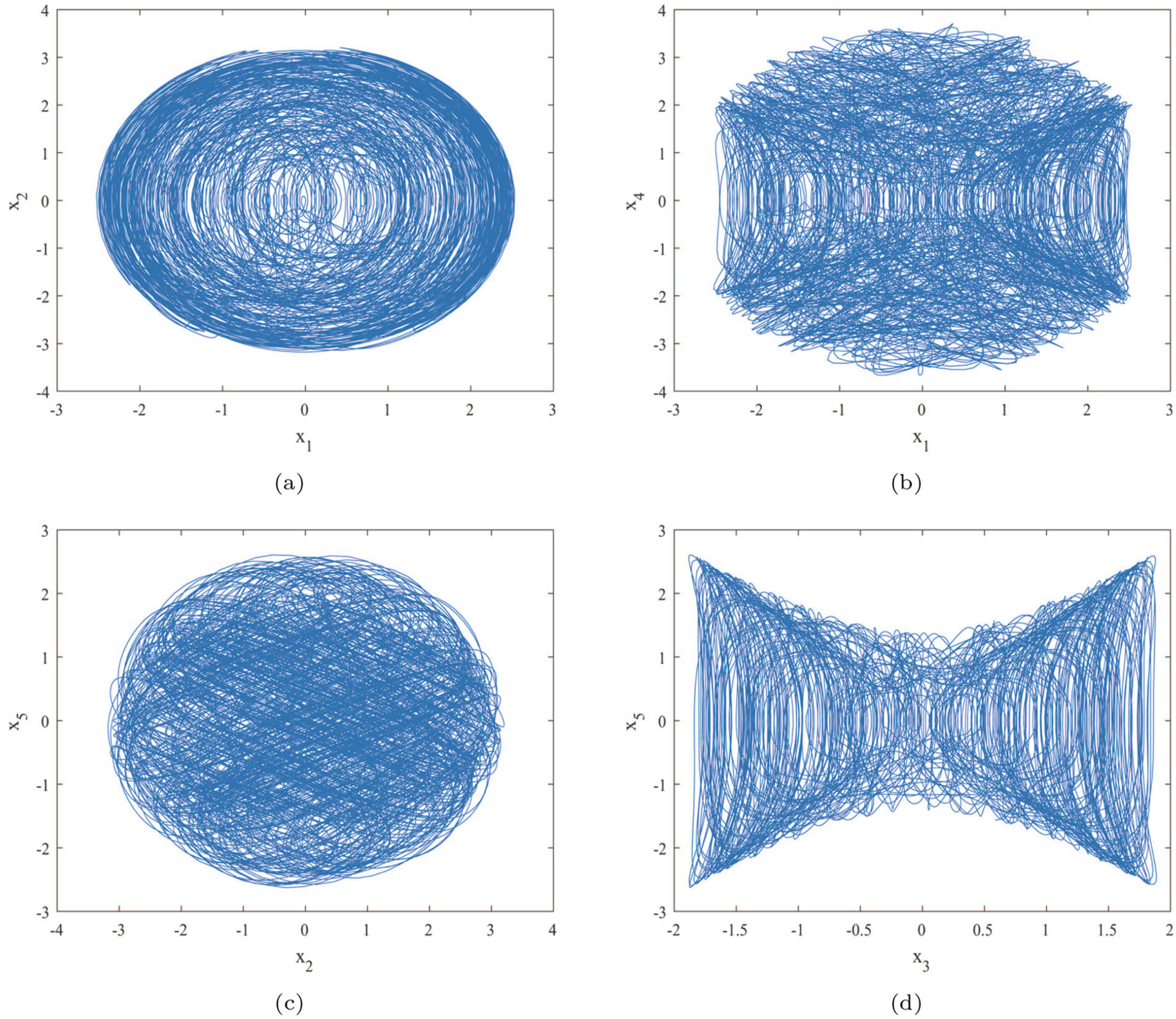


Fig. 3 Results of phase diagram. **a** Plane $x_1 - x_2$; **b** Plane $x_1 - x_4$; **c** Plane $x_2 - x_5$; **d** Plane $x_3 - x_5$

Further, as shown in Eq. (15), convert the chaotic sequence X into test data composed of 0 and 1, and divide it into 100 groups for NIST testing.

$$X = \mathrm{mod}(floor(X \times 10^{15}), 2) \tag{15}$$

where mod() is the modulus operation, and $floor()$ represents rounding down operation.

Table 1 explicates the outcomes of the test; for items with multiple sub-tests, the average value is selected as result.

In accordance with Table 1, the test sequence passes all test items, and all pass rates are greater than or equal to 0.9602, which satisfies conditions (1) and (2). In addition, the uniformity of P values distribution can be verified by a histogram. By dividing the range from 0 to 1 into 10 equidistant sub-ranges, the quantities of P values are illustrated in each sub-range of the histogram. Histogram analysis is performed with the non-overlapping test item, and the result is drawn in Fig. 6. The P values are evenly distributed, satisfying condition (3).

As the above results indicate, the test sequence produced by system Σ_5^H meets all the test standards, and the chaotic test sequence has good pseudo-randomness. Therefore, system Σ_5^H has the capability to be a secure pseudo-random number generator.

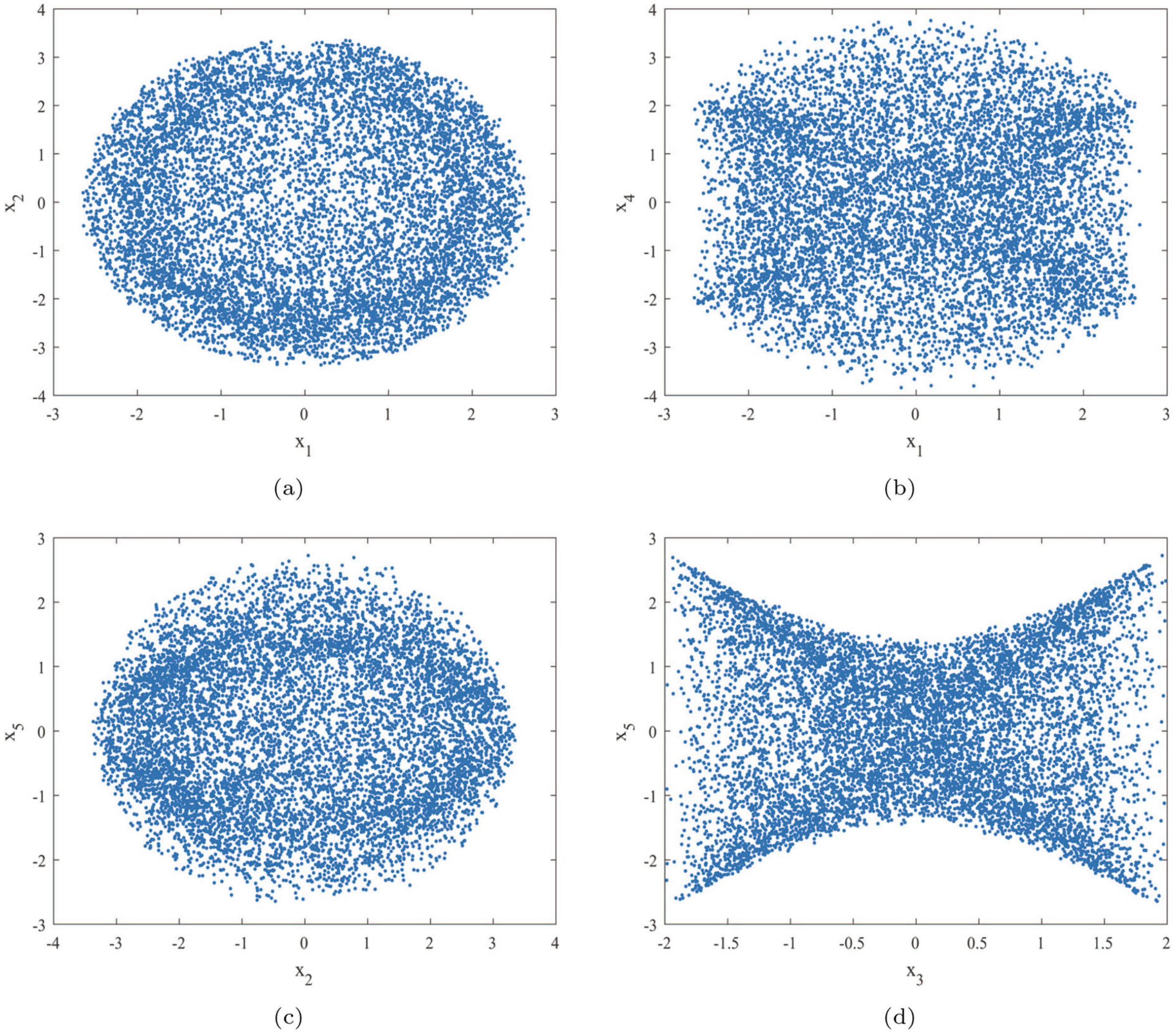


Fig. 4 Results of Poincare section diagram. **a** Plane $x_1 - x_2$; **b** Plane $x_1 - x_4$; **c** Plane $x_2 - x_5$; **d** Plane $x_3 - x_5$

4 Design of the image encryption algorithm

A novel diffusion method based on the bit-plane segmentation is designed in this part. And on this basis, an image encryption scheme based on the 5D Hamiltonian conservative hyperchaotic system is proposed. Figure 7 shows the encryption process. The scheme can encrypt both gray and color images of any size, which consists of two parts, namely, key production and plaintext image encryption.

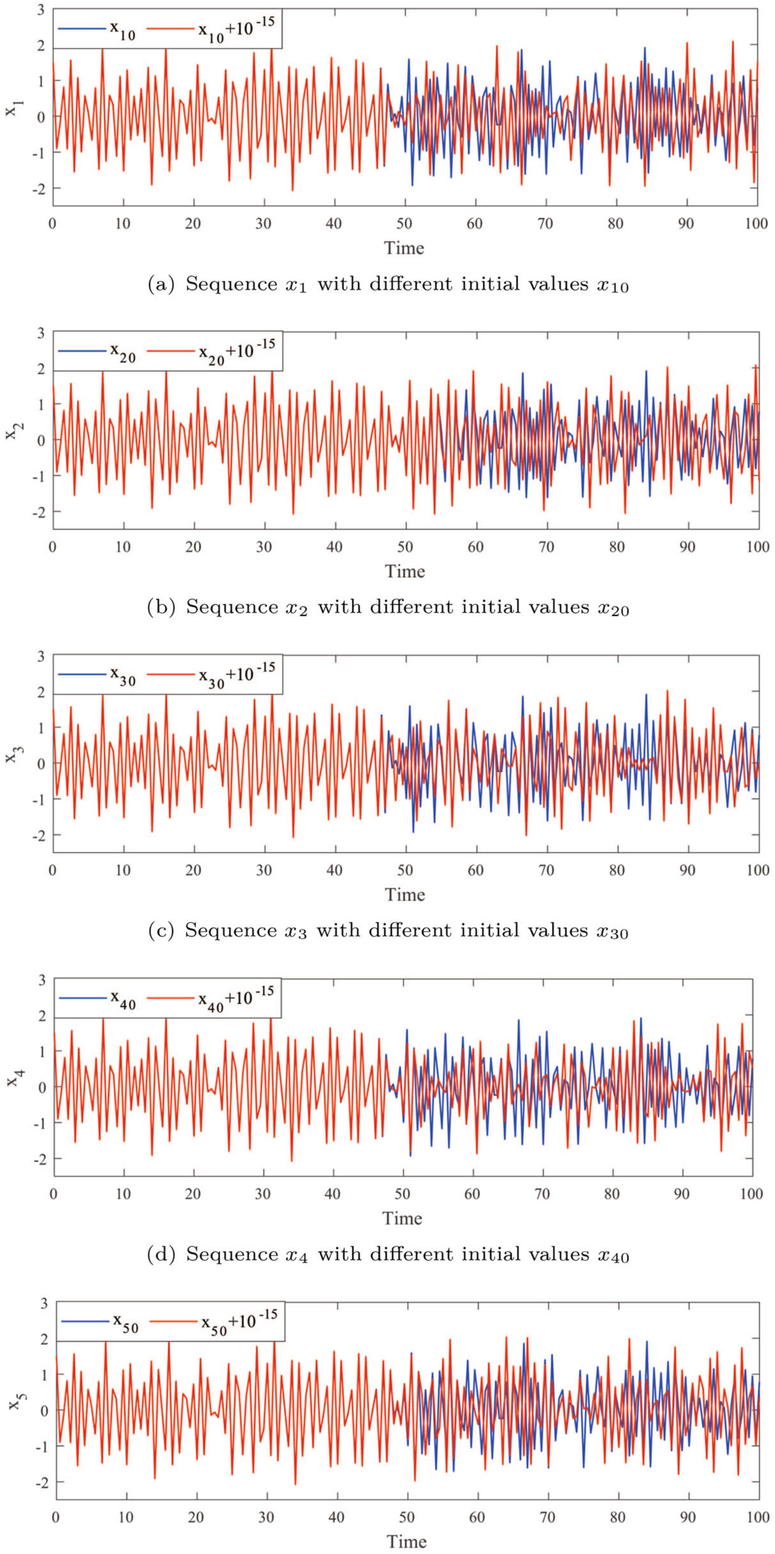
4.1 Initial key production

The initial key is constructed of two segments, namely the SHA-256 sequence HK of the original image, where HK is a hexadecimal sequence with a length of 64, and the initial values of the chaotic system $(x_0, y_0, z_0, u_0, v_0)$. In addition, the encryption key K can be generated by the following process.

Step 1 Convert the hash code HK into a string;

$$HK = num2str(HK) \tag{16}$$

Fig. 5 Results of initial value sensitivity analysis



(a) Sequence x_1 with different initial values x_{10}

(b) Sequence x_2 with different initial values x_{20}

(c) Sequence x_3 with different initial values x_{30}

(d) Sequence x_4 with different initial values x_{40}

(e) Sequence x_5 with different initial values x_{50}

Table 1 NIST test results of system Σ_5^H

No.	Statistical test	P values	Pass rate
1	Rank	0.3505	1
2	Runs	0.4750	1
3	FFT	0.5544	1
4	Frequency	0.8514	1
5	Cumulative sums	0.4677	0.99
6	Block frequency	0.3041	0.99
7	Longest run	0.2493	0.99
8	Universal	0.8831	0.99
9	Non-overlapping template	0.5014	0.99
10	Random excursions variant	0.4475	0.99
11	Random excursions	0.5533	0.99
12	Serial	0.3528	0.98
13	Linear complexity	0.3505	0.98
14	Approximate entropy	0.4750	0.97
15	Overlapping template	0.1816	0.97

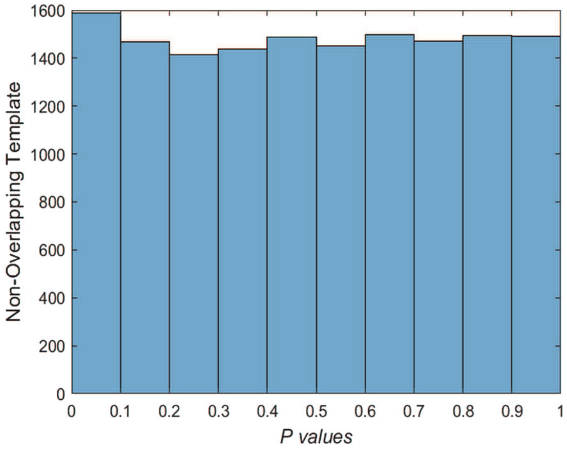


Fig. 6 The non-overlapping template P value histogram

where $num2str()$ is the number-to-string function.

Step 2 Divide HK into six parts and calculate to obtain $hk_0, hk_1, hk_2, hk_3, hk_4, hk_5$;

$$\begin{cases} hk_0 = sum(HK) \\ hk_1 = sum(HK(1:12))/hk_0 \\ hk_2 = sum(HK(13:24))/hk_0 \\ hk_3 = sum(HK(25:36))/hk_0 \\ hk_4 = sum(HK(37:48))/hk_0 \\ hk_5 = sum(HK(49:60))/hk_0 \end{cases} \tag{17}$$

where $sum()$ represents the summation operation.

Step 3 Add the processed hash values to the initial values to obtain the encryption key K.

$$K = (x_0+hk_1, y_0+hk_2, z_0+hk_3, u_0+hk_4, v_0+hk_5) \tag{18}$$

4.2 Encryption algorithm description

To enhance the effect of high-dimensional chaotic systems on encryption algorithms and improve the diffusion effect, a new bit-plane segmentation operation is designed. The encryption algorithm includes one scrambling and two times diffusion operations, which improve the encryption strength.

4.2.1 Bit-plane segmentation

Figure 8 shows the bit-plane segmentation operation process. The original image is converted into an 8-bit binary array; next, the image array is divided into four groups according to the pattern of two-bit binary numbers. Further processing can produce four sub-images with pixels ranging from 0 to 3. Subsequently, the pseudo-random sequences generated by chaotic system Σ_5^H are used for bit-level diffusion, which make

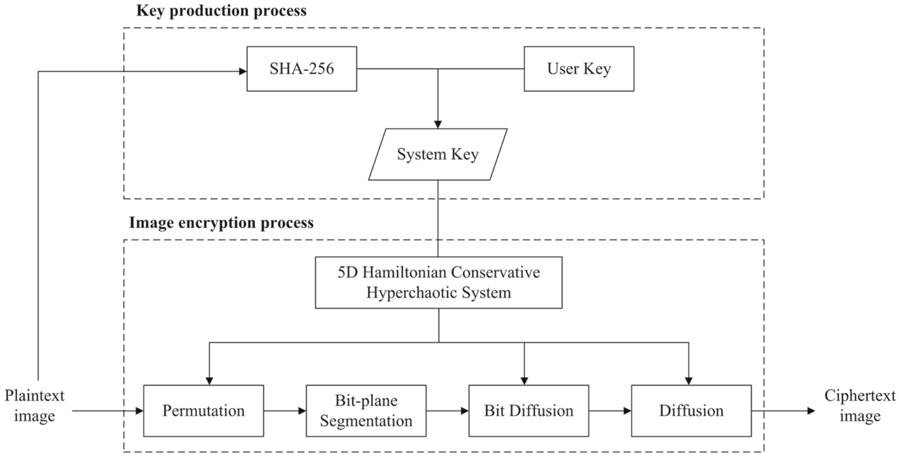


Fig. 7 Encryption algorithm flowchart

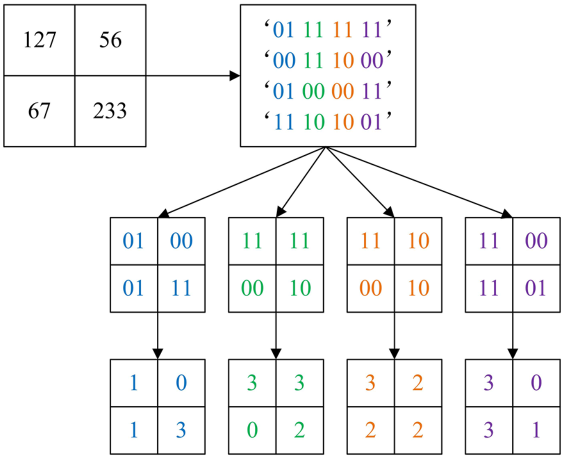


Fig. 8 The bit-plane segmentation process

the diffusion more sufficient and improve the security of the encryption algorithm.

4.2.2 Encryption process

Encrypt the original image P with size $M \times N \times A$, and A represents the quantity of channels of the image, RGB color images correspond to $A = 3$, gray images correspond to $A = 1$. And the following is the detailed encryption process.

Step 1 Take the encryption key K into the 5D conservative hyperchaotic system as initial values to produce chaotic sequences $X0$, $Y0$, $Z0$, $U0$ and $V0$ with the length of $M \times N \times A + len$, where len is the discarded length to prevent the implication of transient data, and it is set to 1000. Then, $X1$, $X2$, $Y1$, $Z1$, $U1$ and $V1$ with a size of $M \times N \times A$ can be calculated by processing as follows:

$$\begin{cases} [\sim, X1] = sort(X0) \\ X2 = \mathrm{mod}(round(X0 \times 10^{15}), 256) \\ Y1 = \mathrm{mod}(round(Y0 \times 10^{15}), 4) \\ Z1 = \mathrm{mod}(round(Z0 \times 10^{15}), 4) \\ U1 = \mathrm{mod}(round(U0 \times 10^{15}), 4) \\ V1 = \mathrm{mod}(round(V0 \times 10^{15}), 4) \end{cases} \tag{19}$$

where $sort()$ is the function for sorting, and $round()$ denotes the rounding function.

Step 2 Transform image P into an array with one dimension. Then, perform a permutation operation on P and the index sequence $X1$ to acquire $P1$;

$$P = reshape(P, M \times N \times A, 1) \tag{20}$$

$$P1(k) = P(X1(k)) \tag{21}$$

where $reshape()$ is the function to reshape the array, $k = 1, 2, \ldots, M \times N \times A$.

Step 3 Implement the bit-plane segmentation operation on $P1$. Firstly, convert $P1$ into 8-bit binary matrix S, and S is divided into four subsequences $s1$, $s2$, $s3$, $s4$ by bit-plane segmentation.

$$S(:, :) = dec2bin(P1, 8) \tag{22}$$

$$\begin{cases} s1 = bin2dec(s(:, 1 : 2)) \\ s2 = bin2dec(s(:, 3 : 4)) \\ s3 = bin2dec(s(:, 5 : 6)) \\ s4 = bin2dec(s(:, 7 : 8)) \end{cases} \tag{23}$$

where $dec2bin()$ is the decimal to binary conversion function and $bin2dec()$ is the binary-to-decimal function.

Step 4 Perform XOR processing on subsequences $s1, s2, s3, s4$ and pseudo-random sequences $Y1, Z1, U1, V1$, respectively. And the processed results are transformed into binary form to obtain sequence $d1, d2, d3, d4$;

$$\begin{cases} d1 = dec2bin(bitxor(s1, Y1), 2) \\ d2 = dec2bin(bitxor(s2, Z1), 2) \\ d3 = dec2bin(bitxor(s3, U1), 2) \\ d4 = dec2bin(bitxor(s4, V1), 2) \end{cases} \tag{24}$$

where $bitxor()$ is a bitwise XOR function.

Step 5 Merge the sequences $d1, d2, d3$ and $d4$, to get the 8-bit binary sequence D. And by converting D into decimal, the preliminary diffusion result $P2$ is obtained;

$$\begin{cases} D = \left[d1\ d2\ d3\ d4 \right] \\ P2 = dec2bin(D) \end{cases} \tag{25}$$

Step 6 Perform XOR processing on $P2$ and sequence $X2$ to complete secondary diffusion to obtain $P3$, and finally restore $P3$ to the $M \times N \times A$ array to get the encrypted result E.

$$\begin{cases} P3 = bitxor(P2, X2) \\ E = reshape(P3, M, N, A) \end{cases} \tag{26}$$

4.3 Decryption algorithm description

The decryption algorithm is the inverse operation of the encryption algorithm, and the decryption steps of ciphertext image C with the size of $M \times N \times A$ are briefly introduced as follows:

Step 1 Calculate the decryption key based on the hash sequence and initial values in the initial key. The decryption key generation process is shown in Sect. 4.1.

Step 2 Take the decryption key into the 5D conservative hyperchaotic system as initial values to produce chaotic sequences, and further processing to get the index sequence and pseudo-random sequences. The detailed process is shown in step 1 of Sect. 4.2.

Step3 Decrypt the ciphertext image C according to the reverse process of the encryption process from step 2 to step 6 in Sect. 4.2, and get the plaintext image P.

5 Simulation results and security analysis

For the purpose of validating the security of our proposed image encrypting method, we choose grayscale images sized 256 × 256, such as Cameraman and Lena, and several images in the image dataset USC-SIPI with varying sizes, including color images and gray images, for testing the constructed image encryption algorithm. And the security efficacy of the encryption method is assessed by the factors such as information entropy, correlation, and anti-attack. We use MATLAB R2020a to carry out simulation experiments under Windows 10 system. The computer hardware is set to Intel Core i5-1135G7 CPU (2.40 GHz), 16.0 GB RAM memory. The computer precision is set to 15, and the initial values are $x_0 = 1$, $y_0 = 1$, $z_0 = 1.5$, $u_0 = 1$, $v_0 = 1$.

5.1 Simulation results

The color image House (4.1.05) and the gray image alarm Clock (5.1.12) with a size of 256 × 256 and the gray image Bridge (5.2.10) with a size of 512 × 512 are encrypted with the proposed encryption method. Figure 9 exhibits the results of simulation.

5.2 Safety performance analysis

5.2.1 Key sensitivity analysis

The reliability of encryption algorithms is largely affected by the sensitivity of the key, any minor alteration to the key must generate entirely distinct encryption and decryption results. To confirm the sensitivity of our encryption method to the key, we perform encryption and decryption to the plaintext Lena with the correct key, then change only one initial value of the key from x_0 to $x_0 + 10^{-15}$, and the rest is unchanged, the modified key is applied for decryption. Figure 10 shows the outcome of decryption.

As Fig. 10 illustrates, changing the key results in the inability to decrypt the plaintext from the ciphertext, which explicates that our proposed encryption scheme possesses strong key sensitive.

5.2.2 Analysis of key space

Encryption methods that possess a larger key space are more resistant to violent attacks, and Alvarez et

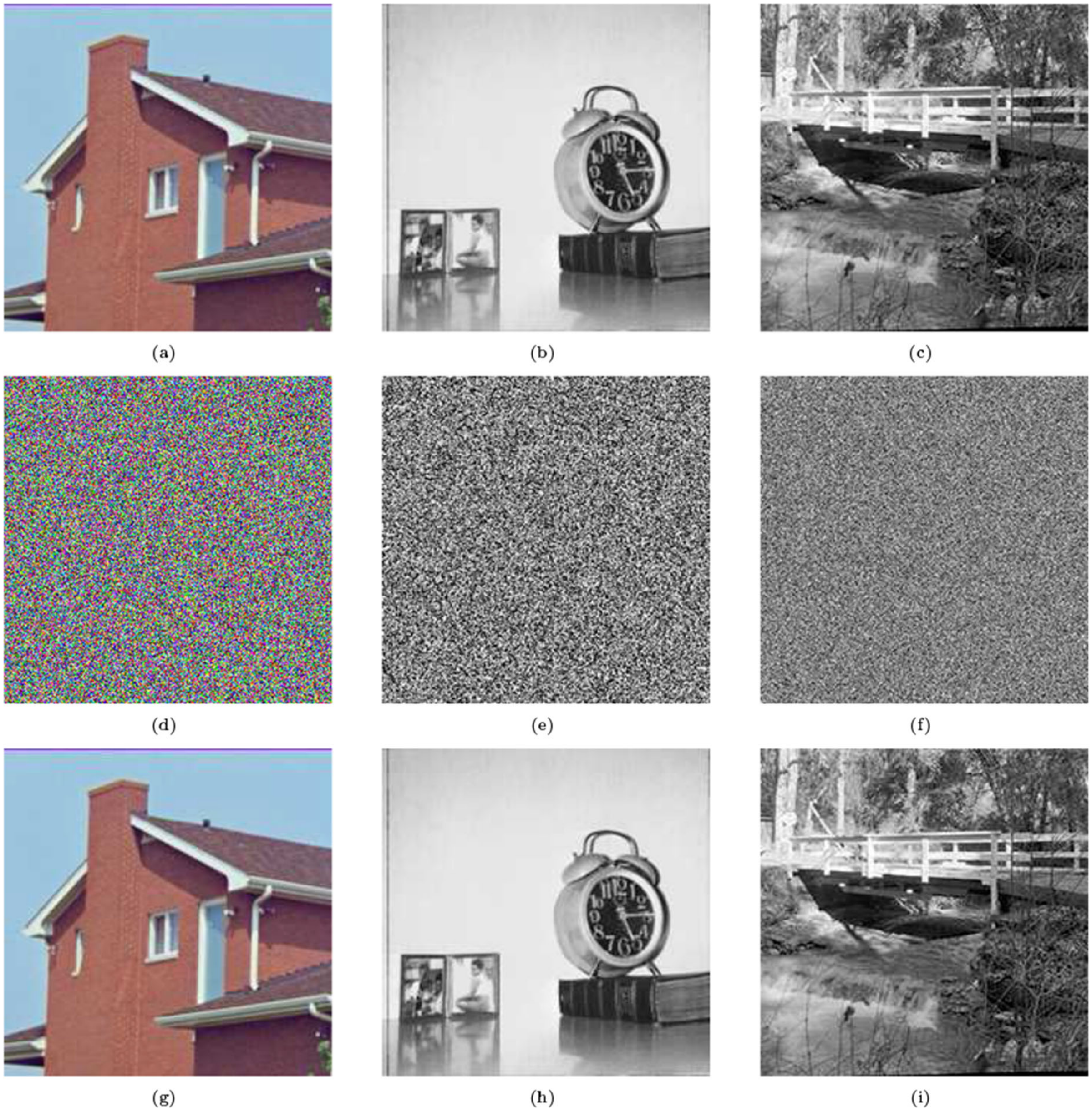


Fig. 9 Results of simulation experiments. **a**–**c** Source images; **d**–**f** ciphertext; **g**–**i** decrypted results

al. [34] suggested that minimum size of the key space must be no smaller than 2^{100} for secure encryption algorithms. For our proposed encryption method, the key consists the SHA-256 sequence and initial values $(x_0, y_0, z_0, u_0, v_0)$. When calculation precision of the operating environment is 10^{-15}, the key space can be calculated as $2^{256} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \approx 2^{505}$. And the result of comparing the key space in our encryption scheme with that in other schemes is expressed in Table 2; bold represents the best results.

As determined in Table 2, our method owns a wider key space; it has a greater capacity to withstand violent attacks.

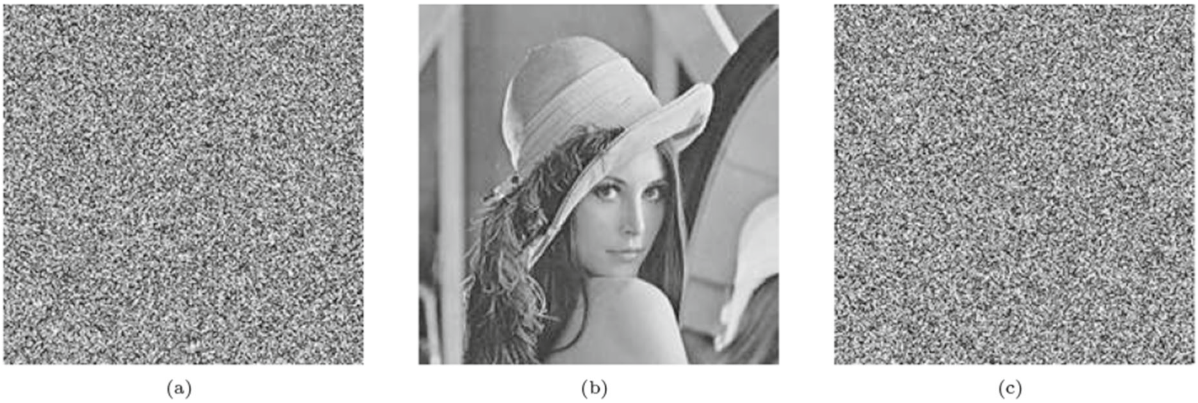


Fig. 10 Results of key sensitivity analysis. **a** Ciphertext; **b** decrypted outcome by the initial key; **c** decrypted outcome by the changed key

Table 2 Key space comparison

Schemes	Key space
Ours	$\mathbf{2^{505}}$
[35]	2^{399}
[36]	2^{465}
[37]	2^{312}
[38]	1.677×2^{341}
[39]	$0.4 \times 2^{189.7}$

Bold indicates the results with better performance in the comparison schemes

5.2.3 Analysis of histogram

The pixel distribution of images can be accurately displayed on the histogram. And the more even distribution of the histogram indicates that the safety of the encryption scheme is greater. For the grayscale image Lena, Fig. 11 reveals its plaintext histogram and corresponding ciphertext histogram.

It is evident that the pixel values of the encrypted image are uniformly distributed, which makes it hard for attackers to extract valuable information from the histogram of the encrypted image. To further validate the evenness of pixel distribution in ciphertext images, we perform the Chi-square test to appraise encrypted images. And the Chi-square test result χ^2 can be derived as

$$\chi^2 = \sum_{k=0}^{255} \frac{(p_k - p)^2}{p} \tag{27}$$

where k is the pixel value, p_k is the quantity of pixel k, and p denotes the expected quantity of pixel k, $p = (M \times N \times A)/256$.

Set the confidence level is 95%, i.e., the significance level $\alpha = 0.05$, the χ^2 value satisfying the test criteria should be less than 293.24783. Moreover, the results of Chi-square test for source images and their ciphertexts are manifested in Table 3. All encryption results of test images are far below 293, indicating that the ciphertext pixels are uniformly distributed, and it proves that our encryption method exhibits good resistance to statistical attacks.

5.2.4 Information entropy analysis

As a conventional index to judge the effectiveness of image encryption methods, information entropy can reflect the disorder and randomness of image information. Information entropy can be obtained as

$$E(x) = -\sum_{i=0}^{2^N-1} P(x_i)\log_2 P(x_i) \tag{28}$$

where x_i is the pixel value, N represents the bits quantity of x_i, and $P(x_i)$ denotes the probability of pixel x_i. And for the 256 grayscale ciphertext image, which N equals 8, its information entropy theory value is 8.

We have compared the information entropy of the ciphertexts between our scheme and other algorithms, and the results are presented in Table 4; bold indicates the optimal value. It demonstrates that our encryption algorithm produces ciphertext with information

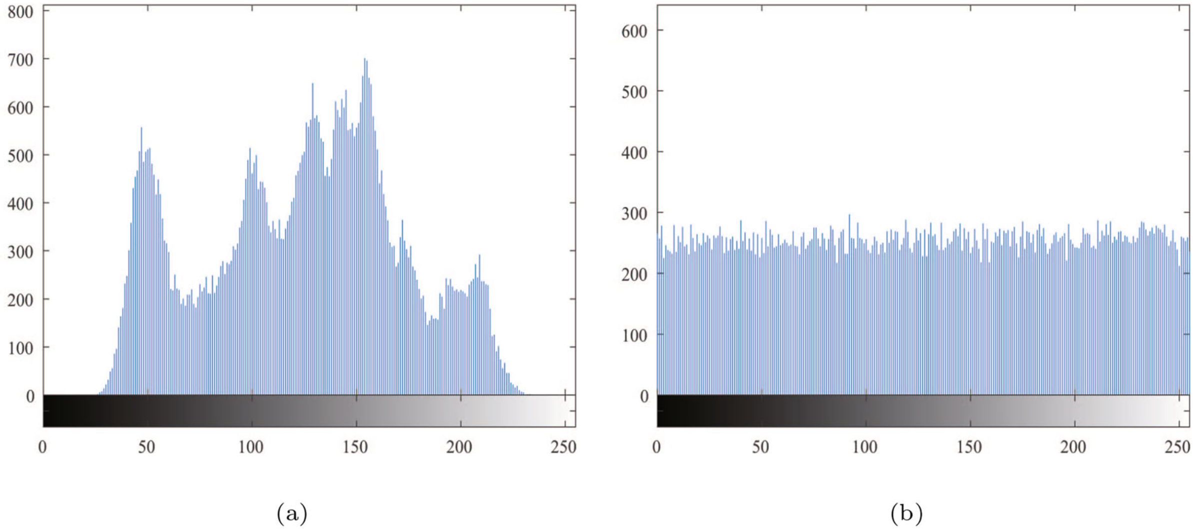


Fig. 11 Results of histogram analysis. **a** Plaintext; **b** ciphertext

Table 3 Results of Chi-square test

Images	Lena	Cameraman	White	Black	Average
Plaintext	39868.7266	110973.3047	16711680	16711680	–
Ciphertext	274.7344	255.4063	266.8438	231.7344	258.6775

entropy that are closer to 8, and it signifies the designed method possesses a greater level of security.

5.2.5 Correlation analysis

Adjacent pixels in meaningful images display a noticeable correlation, and encryption algorithms should minimize the adjacent pixels correlation in order to provide better protection for the security of encrypted images. The evaluation of correlation analysis ordinarily involves the analyses of horizontal correlation, vertical correlation and diagonal correlation. And correlation coefficient can be derived by Eq. (32).

$$E(p) = \frac{1}{Q}\sum_{i=1}^{Q} p_i \tag{29}$$

$$V(p) = \frac{1}{Q}\sum_{i=1}^{Q} (x_p - E(p))^2 \tag{30}$$

$$\text{cov}(p,q) = \frac{1}{Q}\sum_{i=1}^{Q} ((p_i - E(p))(q_i - E(q))) \tag{31}$$

$$\text{corr}_{xy} = \frac{cov(p,q)}{\sqrt{V(p)}\sqrt{V(q)}} \tag{32}$$

where (p, q) is a set of adjacent pixels, $V(p)$ and $E(p)$ represent the variance and expectation of pixel p, respectively, and Q denotes the quantity of adjacent pixel pairs selected.

We select 10,000 sets of adjacent pixels randomly, and correlation coefficients in three various aspects are calculated. Figure 12 shows the analysis results of source images and their corresponding ciphertexts. And the source images have a significant correlation. However, the ciphertexts have a low correlation, close to 0. Moreover, Figs. 13 and 14 specifically display the correlation analysis results of grayscale and color images separately.

In addition, Table 5 illustrates the correlation analysis comparison results between our encryption scheme and other schemes, where bold represents the optimal value. And the correlation coefficients of ciphertext are significantly smaller than original images, which signifies that our encryption method exhibits a strong capability to prevent statistical attacks.

Table 4 Informatica entropy of ciphertext images

Images	Plaintext	Ciphertext			
		Ours	[40]	[41]	[42]
5.1.09 (256 × 256)	6.7093	**7.9977**	7.9971	7.9972	7.9966
5.1.10 (256 × 256)	7.3118	**7.9974**	7.9974	7.9971	7.9971
5.1.11 (256 × 256)	6.4523	7.9970	7.9969	7.9970	**7.9972**
5.1.12 (256 × 256)	6.7057	**7.9974**	7.9972	7.9973	7.9974
5.2.09 (512 × 512)	6.9940	7.9992	**7.9993**	7.9993	7.9992
5.2.10 (512 × 512)	5.7056	**7.9994**	7.9993	7.9992	7.9991
5.3.01 (1024 × 1024)	7.5237	7.9998	7.9998	7.9998	7.9998
5.3.02 (1024 × 1024)	6.8303	7.9998	7.9998	7.9998	7.9996
7.1.01 (512 × 512)	6.0274	**7.9993**	7.9991	7.9992	7.9990
7.1.02 (512 × 512)	4.0045	**7.9993**	7.9992	7.9992	7.9991
7.2.01 (1024 × 1024)	5.6115	7.9998	7.9998	**7.9999**	7.9996
Mean of 256 × 256	–	**7.9974**	7.9972	7.9972	7.9971
Mean of 512 × 512	–	**7.9993**	7.9992	7.9992	7.9991
Mean of 1024 × 1024	–	7.9998	7.9998	7.9998	7.9997

Bold indicates the results with better performance in the comparison schemes

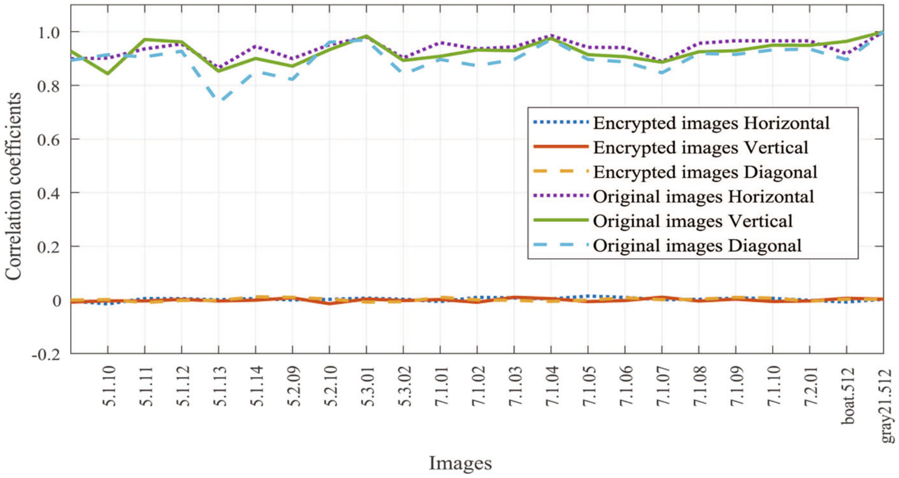


Fig. 12 Analysis results of correlation coefficients

5.2.6 Differential attack resistance analysis

Resistance to differential attack is also a crucial metric for evaluating the effectiveness of encryption schemes. Differential attack, also known as plaintext sensitivity analysis, refers to the attacker changing specific pixels of the source image, analyzing discrepancies in the ciphertext, then using obtained data to crack ciphertext. Therefore, a secure image encryption scheme must be sensitive to the plaintext information, even if there is a tiny difference in the plaintext, the encryption result should be significantly different from that before, so as to resist differential attack. And the number of pixels change rate (NPCR) and unified averaged changed intensity (UACI) are performed to represent the capability of encryption schemes to oppose differential attack, which can be obtained by Eqs. (33) and (34).

$$\mathrm{NPCR} = \sum_{m=1}^{M}\sum_{n=1}^{N}\frac{D(m,n)}{M\times N}\times 100\% \tag{33}$$

$$\mathrm{UACI} = \sum_{m=1}^{M}\sum_{n=1}^{N}\frac{|E_1(m,n)-E_2(m,n)|}{M\times N\times 255}\times 100\% \tag{34}$$

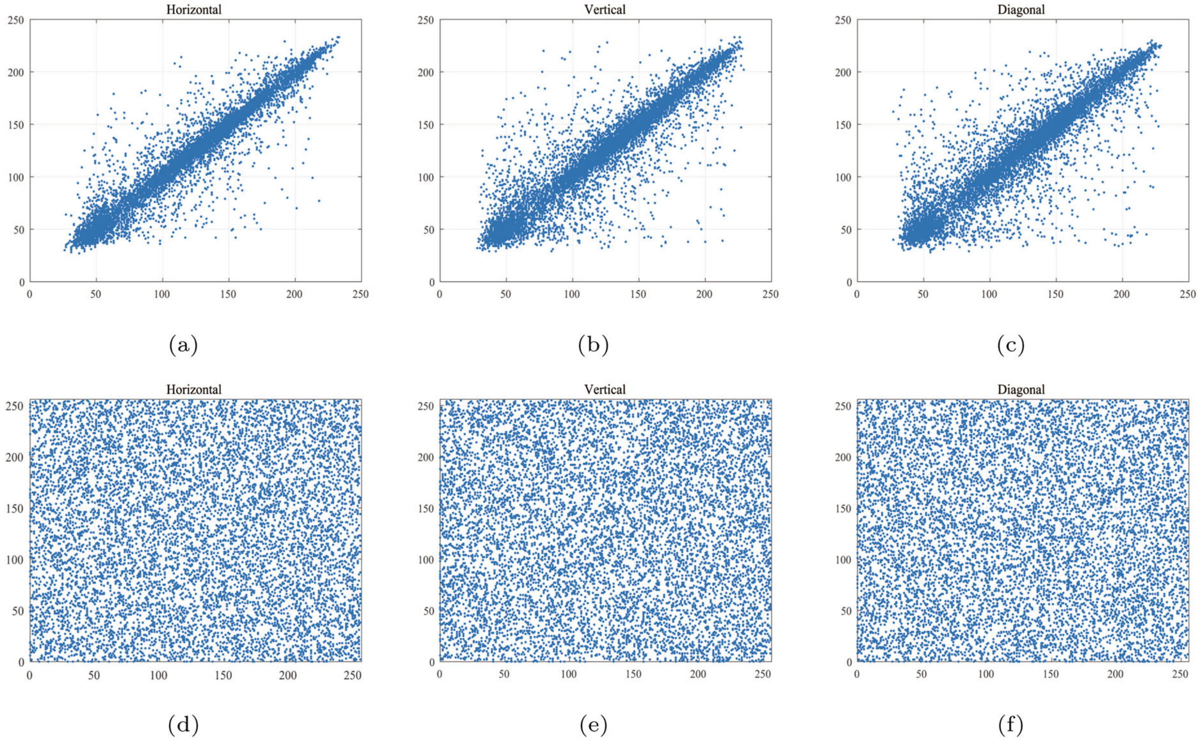


Fig. 13 Analysis of correlation for Lena. **a**–**c** Plaintext; **d**–**f** ciphertext

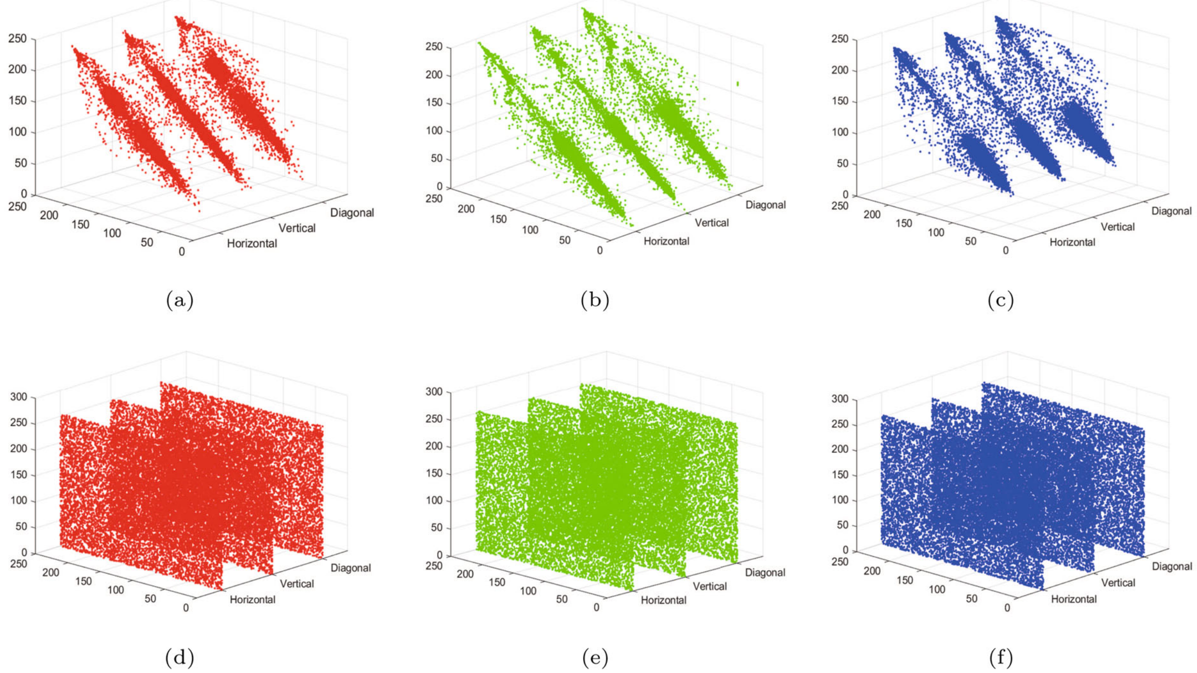


Fig. 14 Analysis of correlation for House. **a**–**c** Red, green and blue channels of the source image; **d**–**f** Red, Green and Blue channels of the ciphertext. (Color figure online)

Table 5 Correlation analysis results under different encryption schemes

Schemes	Horizontal	Vertical	Diagonal
Plaintext Lena	0.9285	0.9609	0.9133
Ours	**0.0056**	**−0.0054**	**−0.0058**
[43]	0.0085	0.0054	0.0049
[44]	−0.0230	**0.0019**	**−0.0034**
[45]	−0.0081	0.0035	−0.0368
[18]	0.0241	−0.0222	0.0169

Table 6 Theoretical values of NPCR (%) and UACI (%) with various image sizes

Image sizes	NPCR	UACI	
		UACI$^-$	UACI$^+$
256 × 256	99.5693	33.2824	33.6447
512 × 512	99.5893	33.3730	33.5541
1024 × 1024	99.5994	33.4183	33.5088

where E_1 and E_2 are two encrypted images sized $M \times N$, and their source images are only a difference of one pixel. $D(i, j)$ is the quantity of pixel values that differ between ciphertexts E_1 and E_2.

$$D(i, j) = \begin{cases} 1 & \text{for} \quad E_1(i, j) \neq E_2(i, j) \\ 0 & \text{otherwise} \end{cases} \tag{35}$$

Set the default significance level $\alpha = 0.05$, and Table 6 reveals the NPCR and UACI theoretical values of multiple image sizes [46].

Table 7 shows the differential attack analysis results of several test images encrypted with our proposed encryption method and other encryption schemes, respectively. The conclusion can be drawn that the resistance capability of the designed encryption algorithm against differential attacks is strong.

5.2.7 Analysis of robustness

The secure image encryption schemes are considered to have strong robustness, especially for data loss and noise that may occur during network transmission of images. The effect of varieties in ciphertext images on the decryption results should be minimized. For the purpose of assessing the robustness of the designed encryption solution, we analyze the capacity of encryption algorithms to defend against cropping and noise attacks, and the peak signal-to-noise ratio (PSNR) is performed to express the robustness strength, which can be obtained by Eq. (37).

$$\text{MSE} = \sum_{m=1}^{M} \sum_{n=1}^{N} \frac{\|P(m, n) - D(m, n)\|^2}{M \times N} \tag{36}$$

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{255 \times 255}{\text{MSE}} \right) \tag{37}$$

where P represents the source image sized $M \times N$ and D represents the decrypted result, and MSE is the mean square error of images P and D.

Figure 15 shows the ciphertext images and decryption results of Lena (256×256) under different clipping intensities. And the PSNR results under different clipping attack degrees is shown in Table 8, where bold represents the optimal value. All the results demonstrate that our encryption method possesses good resistance to cropping attacks.

Moreover, for the purpose of appraising the capability of this designed encryption method to withstand noise attacks, we apply various intensities of noise to the ciphertext Lena. And Fig. 16 manifests the decryption images of encrypted images with noise. Furthermore, Table 9 explicates the PSNR of deciphered images under different noise intensities and compares it with some existing encryption schemes. From the results obtained through the analyses, our image encryption algorithm also exhibits strong resistance to noise attacks.

The analyses presented above illustrate that our encryption method is capable of effectively defending against cropping attacks and noise attacks and possesses strong robustness.

6 Conclusion

In this work, we construct a novel 5D Hamiltonian conservative hyperchaotic system based on Euler rigid body equation and energy analysis. Compared with other chaotic systems, the 5D conservative hyperchaotic system has more complicated dynamic behavior and chaotic sequences generated by it have stronger pseudo-randomness. Depending on this novel hyperchaotic system and the new designed bit-plane segmentation method, we construct a secure image encryption method. Simulation experiments and performance

Table 7 Results of resistance to differential attack

Images	NPCR (%)			UACI (%)		
	Ours	[47]	[48]	Ours	[47]	[48]
5.1.09 (256 × 256)	99.5834	99.6064	99.603	33.5605	33.4456	33.552
5.1.10 (256 × 256)	99.6078	99.6154	99.636	33.4193	33.4946	33.453
5.1.11 (256 × 256)	99.6201	99.6244	99.942	33.3567	33.5541	33.586
5.1.12 (256 × 256)	99.6124	99.5703	99.792	33.5581	33.4302	33.453
5.2.08 (512 × 512)	99.6189	**99.5870**	99.960	33.4461	33.4008	**33.692**
5.2.09 (512 × 512)	99.5979	99.6260	99.876	33.3965	33.4804	33.548
5.2.10 (1024 × 1024)	99.6067	99.6124	99.654	33.4334	33.4563	33.454
5.3.01 (1024 × 1024)	99.6045	**99.5931**	99.950	33.5004	33.4585	33.508
5.3.02 (1024 × 1024)	99.6039	99.6128	99.982	33.4696	33.4605	**33.514**
7.1.01 (512 × 512)	99.6140	99.5992	99.957	33.5162	33.5037	**33.648**
7.1.02 (512 × 512)	99.6140	99.6075	99.918	33.4925	33.4480	33.465
7.2.01 (1024 × 1024)	99.6107	99.6156	99.980	33.4659	33.4556	33.487
Mean	99.6055	99.6058	99.8542	33.4679	33.4637	33.5300
Std	0.0114	0.0154	0.1385	0.0593	0.0389	0.0756
Pass/All	12/12	10/12	12/12	12/12	12/12	9/12

Bold indicates values that do not meet the test criteria

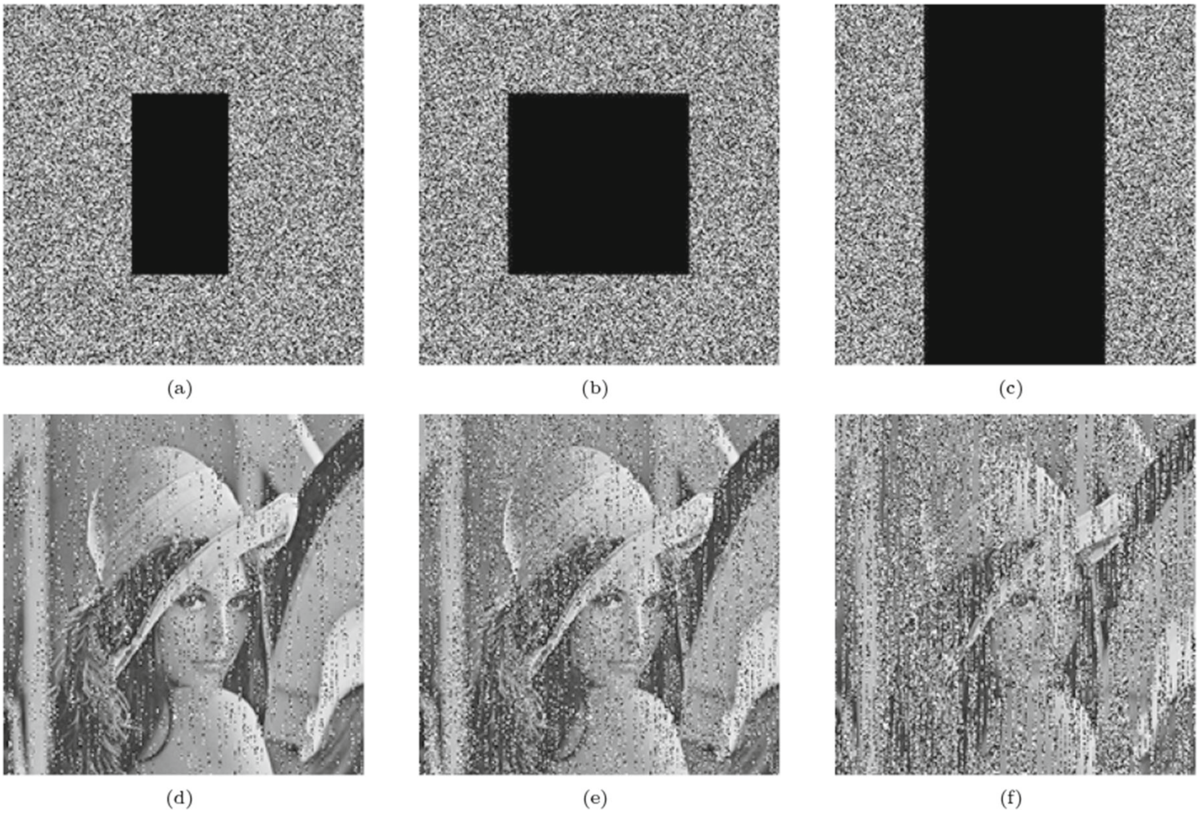


Fig. 15 Analysis of robustness against cropping attack. **a** 1/8 trimming; **b** 1/4 trimming; **c** 1/2 trimming; **d**–**f** decrypted images of **a**–**c**

Table 8 PSNR under cropping attack

Cropping size	1/8	1/4	1/2
Ours	**17.96**	**15.15**	**12.19**
[49]	16.45	12.29	8.13
[50]	8.80	8.50	8.10

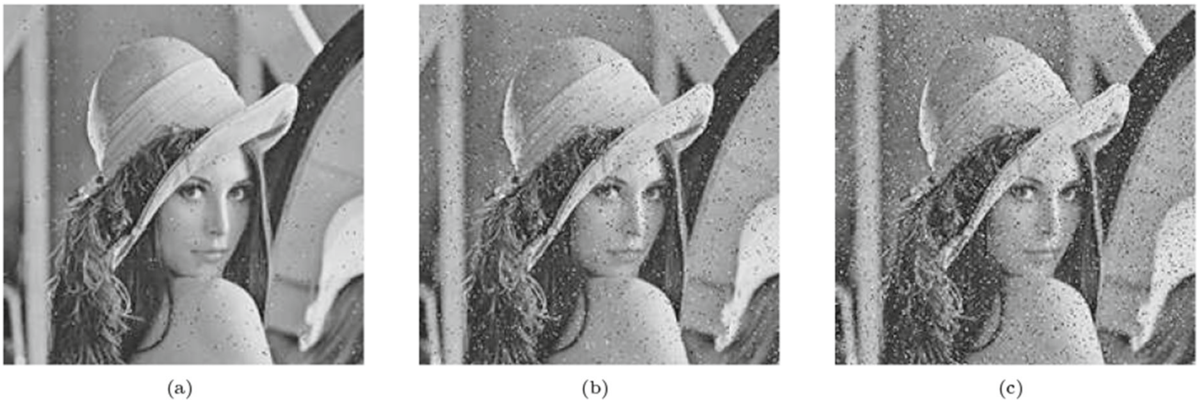


Fig. 16 Analysis of robustness against salt and pepper noise attacks. **a**–**c** Decrypted images under different noise level

Table 9 PSNR under noise attack

Noise level	0.01	0.05	0.10
Ours	**29.52**	**22.24**	**19.21**
[49]	27.12	20.57	17.50
[51]	27.80	21.20	18.03

analysis results illustrate that our encryption scheme possesses strong key sensitivity, wide key space, high plaintext sensitivity and robustness. Moreover, the ciphertext image has low correlation and uniform histogram distribution. All analyses indicate that our designed image encryption algorithm effectively ensures security and meets the needs of practical applications. In future, we intend to deeply study the secure transmission of encryption algorithm keys, so as to further protect the security of image information.

Funding This work was supported by 111 Project (No. D23006), the National Natural Science Foundation of China (Nos. 62272079, 61972266), the Liaoning Revitalization Talents Program (No. XLYC2008017), the Natural Science Foundation of Liaoning Province (Nos. 2021-MS-344, 2021-KF-11-03, 2022-KF-12-14), the Postgraduate Education Reform Project of Liaoning Province (No. LNYJG2022493) and the Dalian Outstanding Young Science and Technology Talent Support Program (No. 2022RJ08).

Data availability The data that support the findings of this study are available within the article.

Declarations

Conflict of interest The authors declare that they have no conflict of interests.

References

1. Usama, M., Khan, M.K., Alghathbar, K., Lee, C.: Chaos-based secure satellite imagery cryptosystem. Comput. Math. Appl. **60**(2), 326–337 (2010)
2. Wang, X., Liu, C., Jiang, D.: A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3d DCT. Inf. Sci. **574**, 505–527 (2021)
3. Liu, X., Tong, X., Wang, Z., Zhang, M.: Construction of controlled multi-scroll conservative chaotic system and its application in color image encryption. Nonlinear Dyn. **110**(2), 1897–1934 (2022)

4. Liang, Q., Zhu, C.: A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. Opt. Laser Technol. **160**, 109033 (2023)
5. Chai, X., Chen, Y., Broyde, L.: A novel chaos-based image encryption algorithm using DNA sequence operations. Opt. Lasers Eng. **88**, 197–213 (2017)
6. Ye, G., Liu, M., Wu, M.: Double image encryption algorithm based on compressive sensing and elliptic curve. Alex. Eng. J. **61**(9), 6785–6795 (2022)
7. Huang, X., Dong, Y., Zhu, H., Ye, G.: Visually asymmetric image encryption algorithm based on sha-3 and compressive sensing by embedding encrypted image. Alex. Eng. J. **61**(10), 7637–7647 (2022)
8. Chai, X., Fu, J., Gan, Z., Lu, Y., Zhang, Y.: An image encryption scheme based on multi-objective optimization and block compressed sensing. Nonlinear Dyn. **108**(3), 2671–2704 (2022)
9. Lv, W., Chen, J., Chai, X., Fu, C.: A robustness-improved image encryption scheme utilizing life-liked cellular automaton. Nonlinear Dyn. **111**(4), 3887–3907 (2023)
10. Liu, P., Zhou, S., Yan, W.Q.: A 3d cuboid image encryption algorithm based on controlled alternate quantum walk of message coding. Mathematics **10**(23), 4441 (2022)
11. Naz, F., Shoukat, I.A., Ashraf, R., Iqbal, U., Rauf, A.: An ASCII based effective and multi-operation image encryption method. Multimed. Tools Appl. **79**, 22107–22129 (2020)
12. Raza, S.F., Satpute, V.: A novel bit permutation-based image encryption algorithm. Nonlinear Dyn. **95**, 859–873 (2019)
13. Kocarev, L.: Chaos-based cryptography: a brief overview. IEEE Circ. Syst. Mag. **1**(3), 6–21 (2001)
14. Fridrich, J.: Image encryption based on chaotic maps. In: 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, vol. 2, pp. 1105–1110 (1997)
15. Wang, X., Zhang, H.-L.: A color image encryption with heterogeneous bit-permutation and correlated chaos. Opt. Commun. **342**, 51–60 (2015)
16. Li, C., Luo, G., Qin, K., Li, C.: An image encryption scheme based on chaotic tent map. Nonlinear Dyn. **87**, 127–133 (2017)
17. Wang, X., Du, X.: Chaotic image encryption method based on improved zigzag permutation and DNA rules. Multimed. Tools Appl. **81**(30), 43777–43803 (2022)
18. Zheng, J., Liu, L.: Novel image encryption by combining dynamic DNA sequence encryption and the improved 2d logistic sine map. IET Image Process. **14**(11), 2310–2320 (2020)
19. Qian, X., Yang, Q., Li, Q., Liu, Q., Wu, Y., Wang, W.: A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. IEEE Access **9**, 61334–61345 (2021)
20. Ponomarenko, V., Prokhorov, M.: Extracting information masked by the chaotic signal of a time-delay system. Phys. Rev. E **66**(2), 026215 (2002)
21. Yuan, H.-M., Liu, Y., Lin, T., Hu, T., Gong, L.-H.: A new parallel image cryptosystem based on 5d hyper-chaotic system. Signal Process. Image Commun. **52**, 87–96 (2017)
22. Arthi, G., Thanikaiselvan, V., Amirtharajan, R.: 4d hyperchaotic map and DNA encoding combined image encryption for secure communication. Multimed. Tools Appl. **81**(11), 15859–15878 (2022)
23. Kar, M., Kumar, A., Nandi, D., Mandal, M.: Image encryption using DNA coding and hyperchaotic system. IETE Tech. Rev. **37**(1), 12–23 (2020)
24. Maschke, B., Ortega, R., Van Der Schaft, A.J.: Energy-based Lyapunov functions for forced Hamiltonian systems with dissipation. IEEE Trans. Autom. control **45**(8), 1498–1502 (2000)
25. Roe, P.L.: Characteristic-based schemes for the Euler equations. Annu. Rev. Fluid Mech. **18**(1), 337–365 (1986)
26. Qi, G., Zhang, J.: Energy cycle and bound of Qi chaotic system. Chaos Solitons Fractals **99**, 7–15 (2017)
27. Qi, G., Hu, J., Wang, Z.: Modeling of a Hamiltonian conservative chaotic system and its mechanism routes from periodic to quasiperiodic, chaos and strong chaos. Appl. Math. Model. **78**, 350–365 (2020)
28. Qi, G., Hu, J.: Modelling of both energy and volume conservative chaotic systems and their mechanism analyses. Commun. Nonlinear Sci. Numer. Simul. **84**, 105171 (2020)
29. Qi, G., Liang, X.: Mechanism and energy cycling of the Qi four-wing chaotic system. Int. J. Bifurcat. Chaos **27**(12), 1750180 (2017)
30. Qi, G.: Modelings and mechanism analysis underlying both the 4d Euler equations and Hamiltonian conservative chaotic systems. Nonlinear Dyn. **95**(3), 2063–2077 (2019)
31. Nave, G.K., Nolan, P.J., Ross, S.D.: Trajectory-free approximation of phase space structures using the trajectory divergence rate. Nonlinear Dyn. **96**, 685–702 (2019)
32. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Preprint at https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final (2010)
33. Dong, Q., Zhou, S., Zhang, Q., Kasabov, N.K.: A class of 5d Hamiltonian conservative hyperchaotic systems with symmetry and multistability. Nonlinear Dyn. **110**, 2889–2912 (2022)
34. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos **16**(08), 2129–2151 (2006)
35. Zhou, M., Wang, C.: A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. Signal Process. **171**, 107484 (2020)
36. Tresor, L.O., Sumbwanyambe, M.: A selective image encryption scheme based on 2d DWT, Henon map and 4d Qi hyper-chaos. IEEE Access **7**, 103463–103472 (2019)
37. Hu, G., Li, B.: Coupling chaotic system based on unit transform and its applications in image encryption. Signal Process. **178**, 107790 (2021)
38. Wang, M.-M., Zhou, N.-R., Li, L., Xu, M.-T.: A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank. Expert Syst. Appl. **207**, 118067 (2022)
39. Xiang, H., Liu, L.: A novel image encryption algorithm based on improved key selection and digital chaotic map. Multimed. Tools and Appl. **80**, 22135–22162 (2021)
40. Xian, Y., Wang, X.: Fractal sorting matrix and its application on chaotic image encryption. Inf. Sci. **547**, 1154–1169 (2021)

41. Rani, N., Mishra, V., Sharma, S.R.: Image encryption model based on novel magic square with differential encoding and chaotic map. Nonlinear Dyn. **111**(3), 2869–2893 (2023)
42. Zhou, Y., Bao, L., Chen, C.P.: Image encryption using a new parametric switching chaotic system. Signal Process. **93**(11), 3039–3052 (2013)
43. Wang, T., Wang, M.-H.: Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. Opt. Laser Technol. **132**, 106355 (2020)
44. Xu, L., Li, Z., Li, J., Hua, W.: A novel bit-level image encryption algorithm based on chaotic maps. Opt. Lasers Eng. **78**, 17–25 (2016)
45. Zhu, H., Dai, L., Liu, Y., Wu, L.: A three-dimensional bit-level image encryption algorithm with Rubik's cube method. Math. Comput. Simul. **185**, 754–770 (2021)
46. Wu, Y., Noonan, J.P., Agaian, S., et al.: NPCR and UACI randomness tests for image encryption. Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. **1**(2), 31–38 (2011)
47. Hua, Z., Zhou, Y.: Image encryption using 2d logistic-adjusted-sine map. Inf. Sci. **339**, 237–253 (2016)
48. Alawida, M., Teh, J.S., Samsudin, A., et al.: An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Process. **164**, 249–266 (2019)
49. Zhou, S.: A real-time one-time pad DNA-chaos image encryption algorithm based on multiple keys. Opt. Laser Technol. **143**, 107359 (2021)
50. Karawia, A.A., Elmasry, Y.A.: New encryption algorithm using bit-level permutation and non-invertible chaotic map. IEEE Access **9**, 101357–101368 (2021)
51. Ali, T.S., Ali, R.: A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimed. Tools Appl. **79**(27–28), 19853–19873 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.