Nonlinear Dyn (2023) 111:2815–2839
https://doi.org/10.1007/s11071-022-07942-1

ORIGINAL PAPER

Quantum image encryption scheme based on 2D $Sine^2 - Logistic$ chaotic map

Miaoting Hu · Jinqing Li · Xiaoqiang Di

Received: 17 April 2022 / Accepted: 29 August 2022 / Published online: 23 October 2022

Abstract In recent years, quantum computing has made breakthrough progress. Due to the characteristics of qubits, image processing may be made more efficient and secure using quantum ciphers. Therefore, a qubit-level selective scrambling and overlapping feedback diffusion method based on a new 2D cross $Sine^2 - Logistic$ chaotic map is proposed. We propose a new type of cross two-dimensional chaotic map that combines Sine and Logistic chaotic systems. Compared with the traditional Sine and Logistic chaotic systems, the new chaotic system has a hyperchaotic state. Additionally, it solves the problem of periodic windows. With a broader parameter space and more chaotic performance, operational efficiency is improved. In the quantum image encryption scheme, based on a novel enhanced quantum representation model, the plaintext image is preprocessed, and the pixel value is changed by qubit level selective scrambling. At the same time, it can achieve the effect of diffusion and make the data more secure. Next, the pixel value position of the image is changed by chaos-based row/column cyclic shift and index scrambling, which greatly serves the purpose of confusion. A diffusion method of quantum overlapping feedback diffusion is proposed to improve the avalanche effect of the encryption algorithm, and finally, the encrypted image is obtained. The experimental results and performance analysis show that the quantum image encryption scheme proposed in this paper is highly secure and reliable.

Keywords 2D cross hyperchaotic system · Quantum image encryption · Quantum selective scrambling · Cycle row/column scrambling · Quantum overlapping feedback diffusion

1 Introduction

In recent years, with the rapid development of the Internet and modern communications, the quantity of data for multimedia transmission and sharing has increased significantly. Digital images are widely used in personal, social, national and other fields as an important multimedia resource. The question of how to ensure the safe transmission of images has piqued the interest of an increasing number of people. Since digital images are characterized by high data redundancy and large data volume, they are susceptible to various attack types throughout the transmission process. Therefore, image encryption algorithms have been extensively studied. However, due to the amount of information included in the image, classic encryption algorithms such as AES and DES [1,2] are no any longer applicable in the field of image encryption. For a large amount of

M. Hu · J. Li (✉) · X. Di
School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130033, China
e-mail: lijinqing@cust.edu.cn

M. Hu · J. Li · X. Di
Jilin Province Key Laboratory of Network and Information Security, Information Center, Changchun University of Science and Technology, Changchun 130033, China

information, the encryption speed will be very slow. Research on more applicable image encryption methods has become a more urgent need in real applications. In 1989, the mathematician Matthews introduced chaos into the encryption system for the first time, and proposed and explained the concept of chaotic cryptography [3]. Since then, various schemes have been developed for chaos-based image encryption, which show higher encryption efficiency compared with traditional image encryption methods. In 1998, Fridrich J was the first to propose an image encryption algorithm based on a chaotic system [4]. Then, some researchers continue to propose image encryption schemes that make considerable use of chaotic systems. Nezhad et al. proposed a chaos-based image encryption algorithm using Tent chaos map and DNA coding [5]. Moumen et al. proposed an image encryption method based on steganographic LSB, AES and RSA algorithms [6]. This algorithm eliminates the secret key sharing step in the encryption process. Ye et al. proposed a quantum logistic image encryption algorithm based on SHA-3 and RSA. The proposed algorithm is very suitable for secure communication in public cryptosystems [7]. Sun et al. [8] proposed an optical color image encryption scheme based on fingerprint keys, which can encrypt the primary color image hidden in the grayscale carrier image into three noise-like holograms. Li et al. introduced a two-dimensional smooth map and investigated its robustness to chaos in infinite parameter spaces [9]. At the same time, a chaos-based pseudo-random number generator is designed based on the optimized robust chaotic map. The analysis shows that the pseudo-random number generator has high randomness. Yu et al. [10] proposed an encryption separation algorithm using compressed sensing, which has the potential to greatly increase the key space while also significantly improving the algorithm's security. Moumen et al. proposed a new secure partial encryption method for medical images using the graph coloring problem, and experiments show that encrypted data have better security [11]. Huang et al. proposed a two-dimensional linear canonical transform for an optical multi-image encryption scheme [12], using two-dimensional LCT parameters and Logistic map as the master key to expanding the key space. Zhou et al. proposed an image encryption algorithm based on circle index table scrambling and partition diffusion [13]. Through experimental analysis, the superiority of this scheme is verified.

Because of their fast iteration speed and easy implementation, low-dimensional chaotic systems are commonly used in image encryption. Liu et al. proposed a digital image watermarking method based on Logistic and RSA encryption [14]. Li et al. proposed a chaos-based bit-level permutation encryption scheme for color images [15], using Tent chaotic map to generate control sequences, but because the Tent chaotic map parameters are relatively singular, the chaotic space is small, and it is insecure and easy to predict. With continuous research, many scholars have discovered that low-dimensional chaotic systems have a small number of variables and parameters, and the key space is small, which makes their structure simple and therefore insecure. High-dimensional chaotic systems are more complex, have more control parameters and have better randomness than low-dimensional chaotic systems. As a result, numerous researchers use high-dimensional chaotic systems for image encryption algorithms. Hosny et al. proposed a hyperchaotic image encryption algorithm [16]. The algorithm uses a six-dimensional hyperchaotic system and uses the Fibonacci Q-matrix to diffuse the image. Liu et al. proposed an encryption algorithm based on compressed sensing and nonlinear diffusion. The designers proposed a new five-dimensional chaotic system with a more complex key stream [17]. High-dimensional chaotic maps have more variables or parameters, so there is a larger chaotic space. However, this requires considerable time, so it is not suitable for real-time applications [18]. Therefore, in recent years, some scholars have proposed new chaotic systems and designed chaotic maps with more complex and rich dynamical behaviors. Teng et al. constructed a crossed 2D hyperchaotic map using a nonlinear function and two chaotic maps with crossed structures [19]. Additionally, the control parameter range is larger, and the chaotic system can have the complex chaotic trajectory phenomenon of a high-dimensional chaotic system, so complex chaotic behavior is easier to realize. Hua et al. proposed a chaotic 2D-LASM map with higher ergodicity [20], and the proposed new chaotic system has larger parameters scope. Li et al. propose a scheme for self-reproducing dynamics in a two-dimensional discrete map, to study self-reproducing dynamics in discrete-time systems by constructing a two-dimensional map with an infinite number of fixed points [21]. Ye et al. developed an elliptic curve public key cryptography algorithm and proposed a new ImproBsys chaotic system with better chaotic

behavior. It has two positive Lyapunov exponents to show hyperchaotic phenomena [22].

Generally, image processing algorithms are more complex and take much longer to calculate. Quantum computing has made breakthrough progress. Using the superposition characteristics of quantum states, computing efficiency can be greatly improved. Combining quantum images with classical image encryption is a safe and effective cryptographic system scheme. Some scholars have designed a variety of quantum image representation models [23–32]. Among them, flexible representation of quantum image (FRQI) and novel enhanced quantum representation (NEQR) models are frequently used because their coding modes are similar to classical images. The NEQR model can accurately restore the original information through measurement [33]. Zhou et al. used the NEQR representation model to propose a quantum image encryption method based on the Lorenz hyperchaotic system [34]. Hu et al. proposed a quantum image encryption algorithm based on Logistic map, using the generalized Arnold transform. It performs very well improving the efficiency of image encryption algorithms [35]. Liu et al. proposed a three-level quantum image encryption algorithm based on Logistic map [36]. Using Quantum Arnold Transform (QArT) to process qubits representing position information, the proposed encryption method has higher security. In addition, the processing efficiency is higher than that of the traditional encryption scheme. Dai et al. [37] proposed a novel quantum multi-image compression encryption algorithm based on the quantum discrete cosine transform and four-dimensional hyperchaotic Henon map. Luo et al. proposed an image encryption scheme based on hyperchaos and quantum coding [38]. It is performed by a bit-level adjacency swap operation, which has less complexity than a traditional bit-level swap operation.

In response to the above problems, we proposed a new 2D cross $Sine^2 - Logistic$ chaotic map, and proposed a quantum image encryption method based on the chaotic map. The simulation results derived from bifurcation diagrams, phase diagrams and Lyapunov exponents show that the 2D cross $Sine^2 - Logistic$ map has a hyperchaotic state and very good chaotic performance. The method proposed in this paper combines quantum images with classical encryption methods. Specifically, the novel enhanced quantum representation (NEQR) model is used to represent a traditional digital image as a quantum state. The key is related to the plaintext image; that is, different grayscale images generate different keys, which improves the resistance to the selected plaintext attack safety. The gray value of the quantum state is changed by the quantum selective scrambling method, and the diffusion effect can be achieved by scrambling the position level. A chaos-based row/column cyclic shift operation is used to change the position of the gray value. Moreover, in order to improve the security of the algorithm, a diffusion method of quantum overlapping feedback diffusion is proposed, which diffuses the scrambled image and finally obtains the encrypted image.

The main contributions of this paper are as follows:

1. A new type of two-dimensional cross hyperchaotic map is proposed, which solves the shortcomings of the small key space and simple structure of low-dimensional chaotic systems, and overcomes the obvious periodic window behavior of existing chaotic maps. It greatly improves the range of control parameters, solves the defects of slow iteration speed and high computational cost of high-dimensional chaotic systems, realizes the complexity of chaotic mapping, is easier to implement and shows very good chaotic behavior.
2. A quantum selection scrambling operation based on the NEQR model is proposed. By scrambling the qubit level, the pixel value can be changed, the effect of diffusion can be achieved at the same time, and the security of the data can be improved.
3. A chaos-based quantum overlapping feedback diffusion method is proposed, which further improves the security of the algorithm and improves the avalanche effect of the encryption algorithm. Even a small change in the original plaintext will cause a large difference in the ciphertext image.

The remaining sections of this article are organized as follows. Section 2 details the 2D cross $Sine^2 - Logistic$ hyperchaotic system and evaluates its chaotic behavior. Section 3 introduces the NEQR quantum image representation model. Section 4 introduces the quantum selective scrambling method in detail. Section 5 introduces the overlapping feedback diffusion method of the quantum image. Section 6 describes the proposed quantum image encryption scheme in detail. Section 7 describes the simulation results and performance analysis. Conclusions are provided in Sect. 8.

2 The proposed 2D hyperchaotic map

2.1 Definition of the 2D cross $Sine^2 - Logistic$ hyperchaotic system

In this paper, we propose a new 2D cross $Sine^2 - Logistic$ hyperchaotic system with two input states x_n, y_n and two cross outputs states x_{n+1}, y_{n+1}. The mathematical expression of this cross-system is shown in Eq. (1). Generally, functions f_1 and f_2 are two chaotic maps. The output is x_{n+1} when the input is y_n and y_{n+1} when the input is x_n.

$$\begin{cases} x_{n+1} = f_1(y_n) \\ y_{n+1} = f_2(x_n) \end{cases} \tag{1}$$

Here, we designed and improved the cross-chaotic system. The sine square chaotic system and the classic logistic chaotic system are introduced. In particular, it needs to be pointed out that the System (2) combines the characteristics of sine chaotic map and logistic chaotic map and retains the advantages of the low-dimensional chaotic system such as fast iteration speed and high operating efficiency. Additionally, our hyperchaotic system effectively avoids the security risks caused by the periodic window embedded in chaotic domain. Experimental analysis shows that this 2D system exhibits excellent hyperchaotic behavior. The state equations of the 2D cross $Sine^2 - Logistic$ hyperchaotic system are shown in Eq. (2).

$$\begin{cases} x_{n+1} = \sin^2(\mu * \arcsin\sqrt{y_n}) \\ y_{n+1} = \alpha * x_n * (1 - x_n) \end{cases} \tag{2}$$

where α, μ are control parameters. When $\alpha = 4, \mu \in [0.5, +\infty]$, the chaotic system has good hyperchaotic behavior. That is, there are two stable positive Lyapunov exponents.

2.2 Performance analysis

2.2.1 Bifurcation diagram

The chaotic behavior of the system may be determined using the bifurcation diagram of the chaotic sequence. To better describe the dynamic behavior and performance improvement of this 2D cross $Sine^2 - Logistic$ hyperchaotic system, we compare its bifurcation diagram with the bifurcation diagrams of the original Sine map and the Logistic map, as shown in Fig. 1.

From Fig. 1a, b, it is not difficult to find that the Sine map and Logistic map only exhibit chaotic properties in a small range of parameters and furthermore, manifest distinct periodic window behavior. Figure 1c, d shows bifurcations of the x-sequence and y-sequence in the $Sine^2 - Logistic$ hyperchaotic systems, respectively, when the initial conditions are $x_0 = 0.3538$ and $y_0 = 0.4262$ and the control parameter $\mu \in [0, 4]$. This hyperchaotic map has a larger parameter range and better stochasticity than the Sine and Logistic map and presents a full mapping state more quickly when entering chaotic behavior.

To better demonstrate the long-range validity of this hyperchaotic system parameter, we control the parameters μ to keep increasing, and the System (2) still has excellent chaotic behavior. Figure 1e, f shows the bifurcation results of $\mu \in [0, 50]$. As a result, the 2D cross $Sine^2 - Logistic$ hyperchaotic system has a larger range of control parameters and better stochasticity than the traditional Sine map and Logistic map.

2.2.2 Phase diagram

The phase diagram represents the distribution of chaotic attractors on the two-dimensional phase plane. The larger the area occupied in the phase diagram is, the better the chaotic performance of the chaotic system. The initial conditions are set to $x_0 = 0.3538$ and $y_0 = 0.4262$, and the phase diagram of system (2) is shown in Fig. 2. Figure 2a is the phase diagram of the 2D Logistic Map (2D-LM) [39], Fig. 2b is the phase diagram of the 2D Sine Logistic Modulation Map (2D-SLMM) [40], and Fig. 2c, d is the 2D cross $Sine^2 - Logistic$ phase diagrams when the parameters $\mu = 3.6239$ and $\mu = 6.9521$.

The results show that our system is more distributed, covering almost all areas, and not clustered in one region. In other words, the hyperchaotic sequence generated by system (2) is a uniform random sequence with good ergodic properties.

2.2.3 Lyapunov exponent

Using the Lyapunov exponent, it is possible to describe the sensitivity of chaotic systems to initial values. To determine whether a nonlinear system has chaotic motion, it is necessary to check whether its Lyapunov exponent λ is positive.

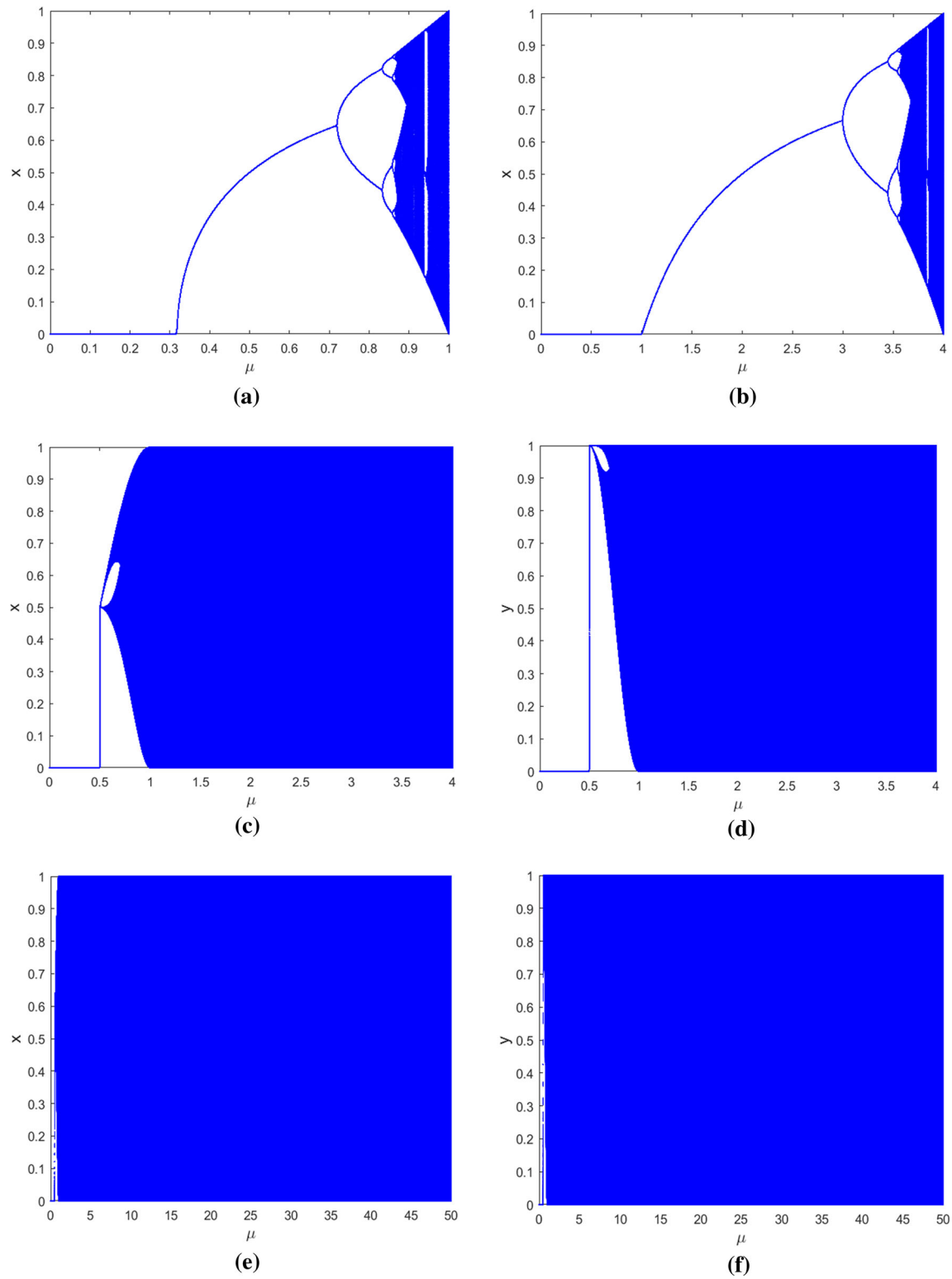

Fig. 1 **a** Sine map; **b** logisitc map; **c** $Sine^2 - Logistic$ map of x sequence for $\mu \in [0, 4]$; **d** $Sine^2 - Logistic$ map of y sequence for $\mu \in [0, 4]$; **e** $Sine^2 - Logistic$ map of x sequence for $\mu \in [0, 50]$; **f** $Sine^2 - Logistic$ map of y sequence for $\mu \in [0, 50]$

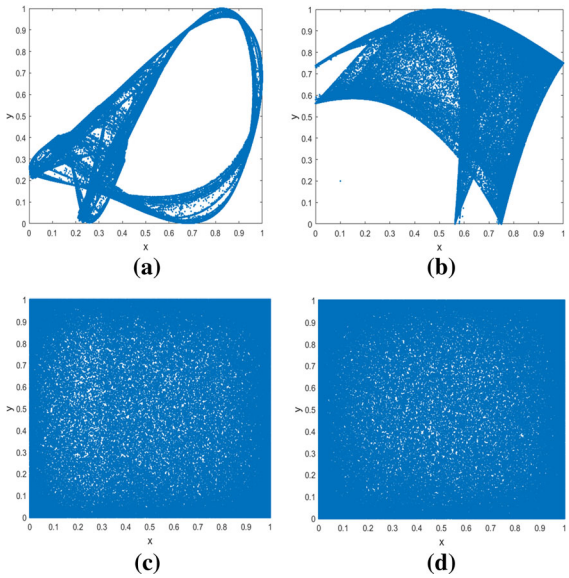

Fig. 2 **a** 2D-LM; **b** 2D-SLMM; **c** $Sine^2 - Logistic$ map phase diagram for $\mu = 3.6239$; **d** $Sine^2 - Logistic$ map phase diagram for $\mu = 6.9521$

There may be more than one Lyapunov exponent greater than zero in high-dimensional phase space, complicating the system's motion. Chaos with more than one positive exponent in the high-dimensional phase space has been called hyperchaos.

In a general sense, the higher the dimensionality is, the higher the possibility of hyperchaotic phenomena in nonlinear systems. However, high-dimensional chaotic systems usually have long iteration times and high computational complexity. This measurement uses the separation rate between infinitely close trajectories, as shown in Eq. (3).

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \mid f'(x_i) \mid \tag{3}$$

Figure 3a, b shows the Lyapunov of Sine and Logistic chaotic maps. As can be shown, the Lyapunov exponent value of the two is greater than 0 only over a small parameter range. As shown in Fig. 3c, when the parameters of our proposed chaotic system are greater than 0.5, the Lyapunov exponent values are all greater than 0. The lower right part of Fig. 3c is a zoomed-in local area picture. Literature [9] proposed a compound operation-based optimization control method of complexity. Theoretical analysis shows that the values of Lyapunov exponent will increase in logarithmic form when the control parameters vary in real space. Thus, the complexity of the chaotic sequence increases. From this, we can also clearly see that the Lyapunov exponent of the proposed chaotic map increases with the increase in the parameters. Meanwhile, the chaotic system has two positive Lyapunov exponent values, indicating that the chaotic system we proposed is a hyperchaotic system with more complex dynamics. The chaos performance is better. Meanwhile, literature [13] mentions that the applied map can keep robust hyperchaotic behaviors by selecting proper parameters. In fact, our proposed chaotic map, when the control parameter is increased to a larger positive number, the value of the Lyapunov exponent is still a positive number, maintaining robust hyperchaotic behavior. Compared with the Sine map and the Logistic map, the 2D $Sine^2 - Logistic$ chaotic system we proposed has a greater Lyapunov exponent value, a larger parameter range and exhibits good chaotic behavior.

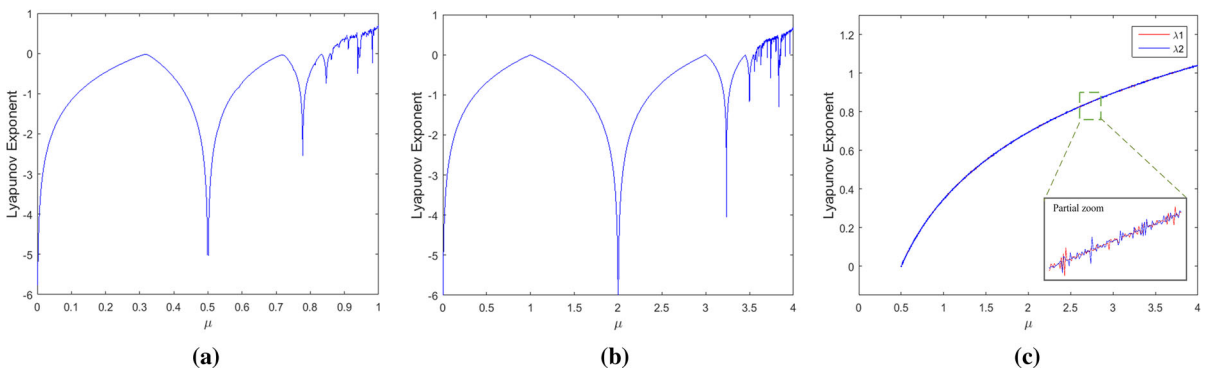

Fig. 3 **a** Sine map; **b** logisitc map; **c** $Sine^2 - Logistic$ map

2.2.4 The 0–1 test

The 0–1 test [41] is used to evaluate the chaotic performance of the proposed 2D cross $Sine^2 - Logistic$ system. For $c \in [0, \pi]$, the 0–1 test value K of chaotic sequence $\{W_j\}, j \in [1, 2, \ldots, n]$ is calculated as shown in Eq. (4):

$$K = \frac{\log M_c(n)}{\log n} \tag{4}$$

$$M_c(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{n} [p_c(j+n) - p_c(j)]^2 + [q_c(j+n) - q_c(j)]^2 \tag{5}$$

$$p_c(n) = \sum_{j=1}^{n} W_j \cos(ir) \tag{6}$$

$$q_c(n) = \sum_{j=1}^{n} W_j \sin(ir) \tag{7}$$

The closer K gets to 1, the more complex its dynamic behavior, and the faster it is equal to 1, the faster it enters into the chaotic state. Figure 4a presents the 0–1 test results of Sine, Logistic, and x, y sequences of the 2D cross $Sine^2 - Logistic$ chaotic map, $\mu \in [0, 4]$. Obviously, the proposed hyperchaotic system has more complex chaotic behavior than the other two systems.

To further demonstrate the long-range chaotic performance of this hyperchaotic system, we also calculated the K values, $\mu \in [0, 50]$, as shown in Fig. 4b, c. Experimental results show that our chaotic system exhibits good chaotic behavior over a wide range of parameters.

2.2.5 Sample entropy

Sample entropy is a measurement tool used to quantitatively measure the complexity of a dynamic system [42]. When sample entropy is positive, the nonlinear system behaves as chaos.

The two sequences x and y of the proposed hyperchaotic system demonstrate good chaotic performance. When μ is greater than 0.6, the sample entropies are significantly higher than 1, as shown by the red and blue lines in Fig. 5a. In contrast, neither traditional Sine nor Logistic map has a sample entropy greater than 1. In other words, the complexity of this 2D cross $Sine^2 - Logistic$ chaotic map is much higher than that of Sine map and Logistic map.

We tested the effect of increasing the parameter range on the sample entropy in this chaotic system in Fig. 5b, c. The results show that the system has consistently stable chaotic properties when the control parameter is extended. This means that if this proposed chaotic system is used as the random number generator of the cryptosystem, this cryptosystem will have a wider key space and can better resist brute-force attacks.

2.2.6 Sensitivity analysis of the initial value

Sensitivity to initial values is one of the important characteristics of chaotic systems. When the initial value changes slightly, completely different chaotic sequences will be generated.

We modified the initial values of Sine map and Logistic map as well as the proposed hyperchaotic system 10^{-16}. After about 55 iterations, the Sine and

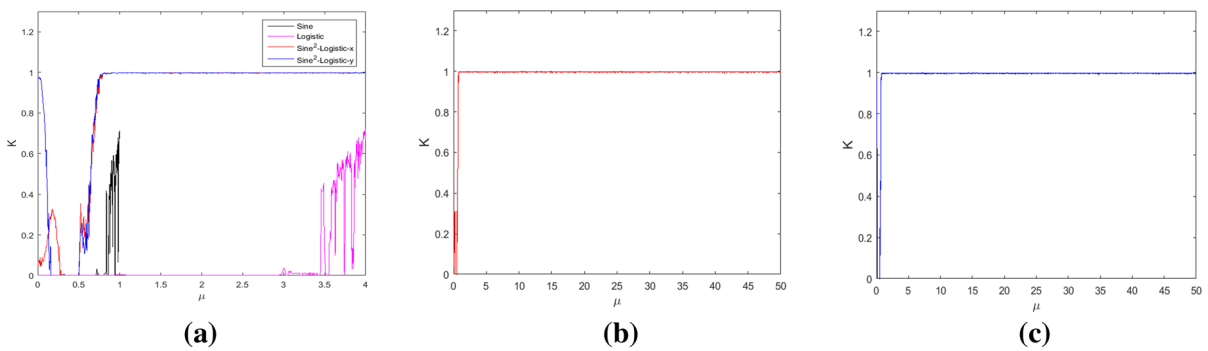

Fig. 4 **a** 0–1 test experiment comparison; **b** $Sine^2 - Logistic$ map of x sequence for $\mu \in [0, 50]$; **c** $Sine^2 - Logistic$ map of y sequence for $\mu \in [0, 50]$

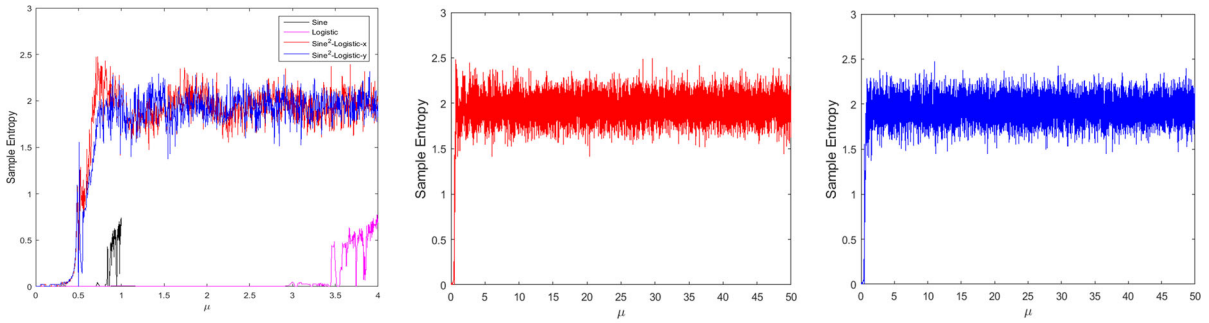

Fig. 5 **a** Sample entropy test comparison; **b** $Sine^2 - Logistic$ map of x sequence for $\mu \in [0, 50]$; **c** $Sine^2 - Logistic$ map of y sequence for $\mu \in [0, 50]$

Logisitc chaotic sequences are completely different from the original sequences, as shown in Fig. 6a, b. However, the 2D cross $Sine^2 - Logistic$ chaotic system requires only 25 iterations, and the generated chaotic sequences are completely different from the original, as shown in Fig. 6c, d. Therefore, the transient effects of chaotic systems can be effectively mitigated and the security of chaotic systems can be improved.

2.2.7 NIST test

The NIST test is a tool for evaluating the nonlinear properties of chaotic systems and the stochastic performance of data [43]. NIST random tests include 16 different test measures, and each test will produce a P value. Only when the P value is within the range of $[0.01, 1]$, the test be judged to have passed. We performed NIST random tests on the data sequences generated by the 2D cross $Sine^2 - Logistic$ hyperchaotic system, and the results are listed in Table 1. All results pass the tests, indicating that our chaotic sequences have measurable randomness.

In addition to the above performance analysis, we also analyze the complexity of the chaotic system. We iterate through different chaotic systems and compare them with our proposed chaotic system. Among them, the 2D Sine Logistic modulation graph is from the literature [40], as shown in Eq. (8). It can be found that the chaotic map also uses the sine function. Additionally, it is compared with other two-dimensional chaotic systems. Table 2 shows that the iteration time of the proposed chaotic system is longer than that of the same-dimensional chaotic system, but the iteration is generally fast. Furthermore, the proposed chaotic system still exhibits hyperchaotic behavior even with a two-dimensional chaotic map.

$$\begin{cases} x_{n+1} = \alpha(\sin(\pi y_n) + \beta) x_n (1 - x_n) \\ y_{n+1} = \alpha(\sin(\pi x_{n+1}) + \beta) y_n (1 - y_n) \end{cases} \tag{8}$$

The above performance analysis shows that our proposed chaotic system has a very large parameter range and has hyperchaotic behavior. At the same time, it exhibits good chaotic characteristics, and can generate more complex chaotic sequences. In applications, it is very suitable for encryption systems.

3 NEQR representation model

Zhang et al. [24] improved the FQRI model and proposed a novel enhanced quantum representation (NEQR) model for representing quantum images. A grayscale image I of $2^n \times 2^n$ is represented by the NEQR model as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |P_{YX}\rangle \otimes |yx\rangle \tag{9}$$

where $|P_{YX}\rangle = |p_{yx}^7 p_{yx}^6 \cdots p_{yx}^1 p_{yx}^0\rangle$ denotes the grayscale information of the pixel corresponding to the position $|yx\rangle$, and $|yx\rangle = |y\rangle|x\rangle = |y_{n-1} y_{n-2} \cdots y_0\rangle|x_{n-1} x_{n-2} \cdots x_0\rangle$ is the position coordinate; the symbol $\otimes$ represents the tensor product operation. Take a 2×2 sized quantum image as an example, as shown in Fig. 7, and its NEQR model is represented as Eq. (10):

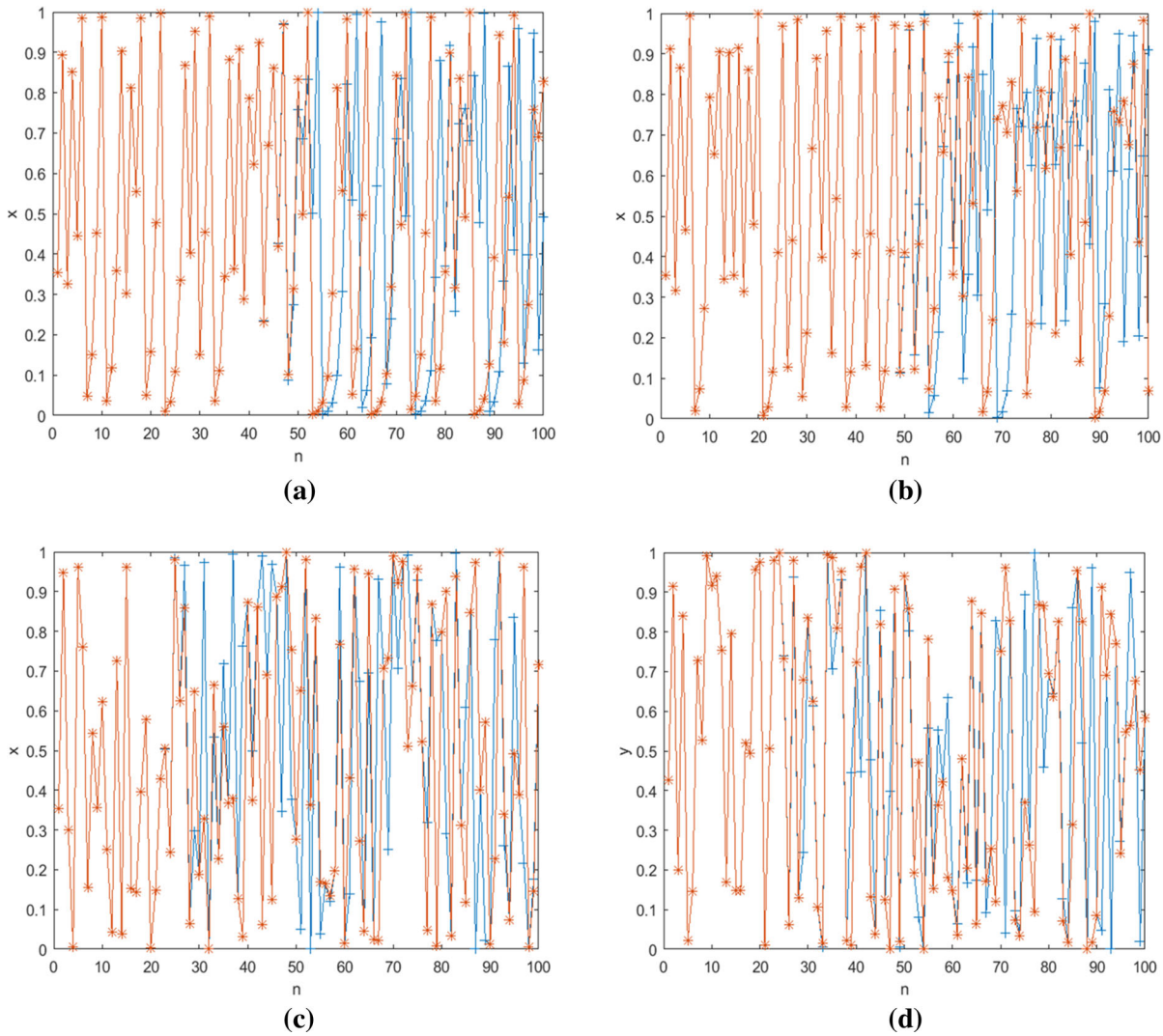

Fig. 6 **a** Sine map; **b** logisitc map; **c** $Sine^2 - Logistic$ map of x sequence; **d** $Sine^2 - Logistic$ map of y sequence

$$
\begin{aligned}
|I\rangle = & \frac{1}{2}(|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle \\
& + |255\rangle \otimes |11\rangle) \\
= & \frac{1}{2}(|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle \\
& + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle)
\end{aligned} \tag{10}
$$

4 Qubit-level selection scrambling

In this section, we propose a quantum selective scrambling method. The method consists of three functional modules: qubit-level shift operation, qubit-level cross-XOR-Shift operation and qubit-level cyclic shift operation. Qubits are selectively scrambled to alter the grayscale of a quantum image diffuse the image.

4.1 Qubit-level shift operation

We design a quantum circuit consisting of controlled swap gates. The value of each pixel (Y, X) is changed by using a qubit-level shift operation.

Taking the quantum circuit shown in Fig. 8 as an example, we perform a shift operation on the qubits, i.e., first swap the 7th qubit with the 3rd qubit, the 6th

Table 1 NIST statistical test results

Statistical test	X		Y	
	P value	State	P value	State
Frequency	0.909834	Pass	0.672582	Pass
Block frequency	0.236804	Pass	0.028836	Pass
Cumulative sums (forward)	0.992042	Pass	0.859177	Pass
Cumulative sums (reverse)	0.955606	Pass	0.482196	Pass
Runs	0.912010	Pass	0.596054	Pass
Longest run of ones	0.411378	Pass	0.427718	Pass
Non-overlapping template	0.991728	Pass	0.939401	Pass
Serial	0.889149	Pass	0.738474	Pass
Linear complexity	0.397492	Pass	0.101523	Pass
Random excursions	0.915301	Pass	0.989948	Pass
Random excursions variant	0.952246	Pass	0.909620	Pass
Approximate entropy	0.178595	Pass	0.438333	Pass
Universal	0.019175	Pass	0.792042	Pass
FFT	0.080739	Pass	0.541289	Pass
Rank	0.631117	Pass	0.504020	Pass
Overlapping template	0.382867	Pass	0.574918	Pass

Table 2 Iterative comparison of chaotic systems

Chaos sequence generation time (s)				
Iteration times	Our proposed chaotic map	2D Logistic-Tent chaotic map	2D Henon chaotic map	2D Sine Logistic Modulation Map
300000	0.066657	0.016820	0.035081	0.060611
600000	0.148492	0.033743	0.068294	0.146796

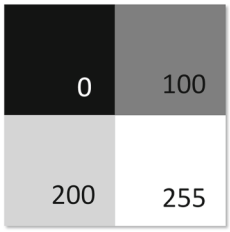

Fig. 7 A grayscale image represented by NEQR model

qubit with the 2nd qubit, the 5th qubit with the 1st qubit, and the 4th qubit with the 0th qubit, and then swap the 6th qubit with the 5th qubit, the 4th qubit with the 3rd qubit and the 2nd qubit with the 1st qubit. The resulting qubit-level can be expressed as:

$$\begin{aligned} |p_{yx}^{7'}\rangle &= |p_{yx}^{3}\rangle \quad |p_{yx}^{6'}\rangle = |p_{yx}^{1}\rangle \\ |p_{yx}^{5'}\rangle &= |p_{yx}^{2}\rangle \quad |p_{yx}^{4'}\rangle = |p_{yx}^{7}\rangle \\ |p_{yx}^{3'}\rangle &= |p_{yx}^{0}\rangle \quad |p_{yx}^{2'}\rangle = |p_{yx}^{5}\rangle \\ |p_{yx}^{1'}\rangle &= |p_{yx}^{6}\rangle \quad |p_{yx}^{0'}\rangle = |p_{yx}^{4}\rangle \end{aligned} \tag{11}$$

For the pixel value (Y, X), the qubit-level shift operation can be realized by the controlled swap gate U_{YX}, and the controlled swap gate U_{YX} is defined as:

$$\begin{aligned} U_{YX}(|P_{YX}\rangle) &= U_{YX}(|p_{yx}^{7} p_{yx}^{6} \cdots p_{yx}^{1} p_{yx}^{0}\rangle) \\ &= |p_{yx}^{3} p_{yx}^{1} p_{yx}^{2} p_{yx}^{7} p_{yx}^{0} p_{yx}^{5} p_{yx}^{6} p_{yx}^{4}\rangle \end{aligned} \tag{12}$$

The gray value is changed from $|p_{yx}^{7} p_{yx}^{6} \cdots p_{yx}^{1} p_{yx}^{0}\rangle$ to $|p_{yx}^{3} p_{yx}^{1} p_{yx}^{2} p_{yx}^{7} p_{yx}^{0} p_{yx}^{5} p_{yx}^{6} p_{yx}^{4}\rangle$ by the shift operation on the qubit-level. Although swap gates only change the position of the qubits, they change the pixel value to achieve diffusion.

4.2 Qubit-level cross-XOR-shift operation

In the proposed scheme, cross exclusive OR and shift operations are performed on the qubit level, as shown in Fig. 9.

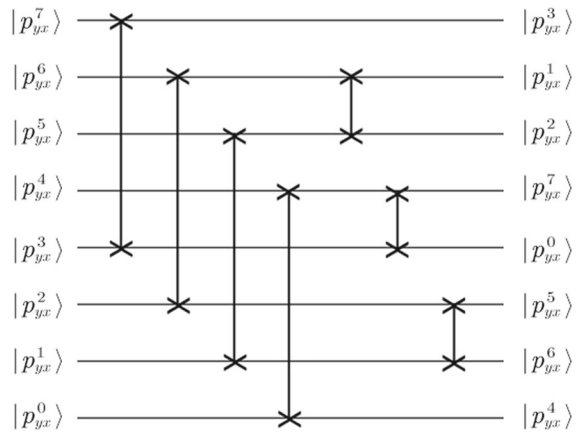

Fig. 8 Quantum circuit for qubit-level shift operations

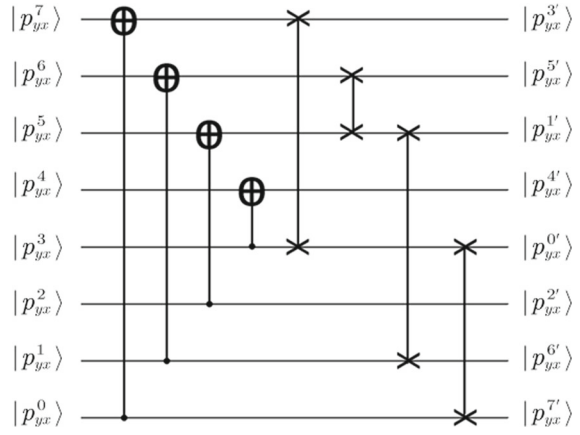

Fig. 9 Quantum circuit with cross-XOR-shift operation

First the XOR operation of the quantum bit is performed. In quantum circuits, CNOT gates are used to implement the XOR operation. The specific execution process is as follows: the 0th qubit is XOR with the 7th qubit to obtain the new 7th qubit state, the 1st qubit is XOR with the 6th qubit to obtain the new 6th qubit state, the 2nd qubit is XOR with the 5th qubit to get the new 5th qubit state, the 3rd qubit is XOR with the 4th qubit to get the new 4th qubit state. The resulting qubits are expressed as:

$$\begin{aligned}
&|p_{yx}^{7'}\rangle = |p_{yx}^{0} \oplus p_{yx}^{7}\rangle \quad |p_{yx}^{6'}\rangle = |p_{yx}^{1} \oplus p_{yx}^{6}\rangle \\
&|p_{yx}^{5'}\rangle = |p_{yx}^{2} \oplus p_{yx}^{5}\rangle \quad |p_{yx}^{4'}\rangle = |p_{yx}^{3} \oplus p_{yx}^{4}\rangle \\
&|p_{yx}^{3'}\rangle = |p_{yx}^{3}\rangle \quad |p_{yx}^{2'}\rangle = |p_{yx}^{2}\rangle \\
&|p_{yx}^{1'}\rangle = |p_{yx}^{1}\rangle \quad |p_{yx}^{0'}\rangle = |p_{yx}^{0}\rangle
\end{aligned} \tag{13}$$

The gray value changes from $|p_{yx}^{7} p_{yx}^{6} \cdots p_{yx}^{1} p_{yx}^{0}\rangle$ to $|p_{yx}^{7'} p_{yx}^{6'} \cdots p_{yx}^{1'} p_{yx}^{0'}\rangle$.

Second, the bit-level shift operation on the gray value $|p_{yx}^{7'} p_{yx}^{6'} \cdots p_{yx}^{1'} p_{yx}^{0'}\rangle$ can be implemented by the controlled swap gate U_{YX}. The gray value is changed from $|p_{yx}^{7'} p_{yx}^{6'} \cdots p_{yx}^{1'} p_{yx}^{0'}\rangle$ to $|p_{yx}^{3'} p_{yx}^{5'} p_{yx}^{1'} p_{yx}^{4'} p_{yx}^{0'} p_{yx}^{2'} p_{yx}^{6'} p_{yx}^{7'}\rangle$, and the obtained qubits can be expressed as:

$$\begin{aligned}
&|p_{yx}^{7'}\rangle = |p_{yx}^{3'}\rangle \quad |p_{yx}^{6'}\rangle = |p_{yx}^{5'}\rangle \\
&|p_{yx}^{5'}\rangle = |p_{yx}^{1'}\rangle \quad |p_{yx}^{4'}\rangle = |p_{yx}^{4'}\rangle \\
&|p_{yx}^{3'}\rangle = |p_{yx}^{0'}\rangle \quad |p_{yx}^{2'}\rangle = |p_{yx}^{2'}\rangle \\
&|p_{yx}^{1'}\rangle = |p_{yx}^{6'}\rangle \quad |p_{yx}^{0'}\rangle = |p_{yx}^{7'}\rangle
\end{aligned} \tag{14}$$

By the controlled swap gate U_{YX}, the pixel value (Y, X) of the quantum image can execute the qubit-level cross-XOR-shift operations; then, the controlled swap gate can be defined as:

$$\begin{aligned}
U_{YX}(|P_{YX}\rangle) &= U_{YX}(|p_{yx}^{7} p_{yx}^{6} \cdots p_{yx}^{1} p_{yx}^{0}\rangle) \\
&= |p_{yx}^{3'} p_{yx}^{5'} p_{yx}^{1'} p_{yx}^{4'} p_{yx}^{0'} p_{yx}^{2'} p_{yx}^{6'} p_{yx}^{7'}\rangle
\end{aligned} \tag{15}$$

4.3 Qubit-level cyclic shift operation

The cyclic left shift operation of the pixel value(Y, X) is realized through the quantum swap gate. As shown in Fig. 10, the pixel value (Y, X) of the quantum image is cyclically shifted t times to the left. The left side of Fig. 10 illustrates that the quantum bits are sequentially cyclically shifted 1 bit left, i.e.,$|p_{yx}^{7}\rangle$ to $|p_{yx}^{6}\rangle$ to $|p_{yx}^{5}\rangle$ to $|p_{yx}^{4}\rangle$ to $|p_{yx}^{3}\rangle$ to $|p_{yx}^{2}\rangle$ to $|p_{yx}^{1}\rangle$ to $|p_{yx}^{0}\rangle$ to $|p_{yx}^{7}\rangle$. The right side of Fig. 10 shows the result of a circular left shift of t bits.

The controlled swap gate U_{YX} performs a qubit-level cyclic shift operation on the pixel value (Y,X). The U_{YX} is defined as:

$$\begin{aligned}
U_{YX}(|P_{YX}\rangle) &= U_{YX}(|p_{yx}^{7} p_{yx}^{6} \cdots p_{yx}^{1} p_{yx}^{0}\rangle) \\
&= |p_{yx}^{7-t} \cdots p_{yx}^{0} \cdots p_{yx}^{7-t+1}\rangle
\end{aligned} \tag{16}$$

In addition, the entire quantum image can be completed through the cyclic shift control sequence $CS = \{t_1, t_2, \ldots, t_{2^{2n}}\}$. 2^{2n} is the total number of pixels in the image, and CS can be generated by the sender and receiver of the data through a chaotic system; see Sect. 6 for details.

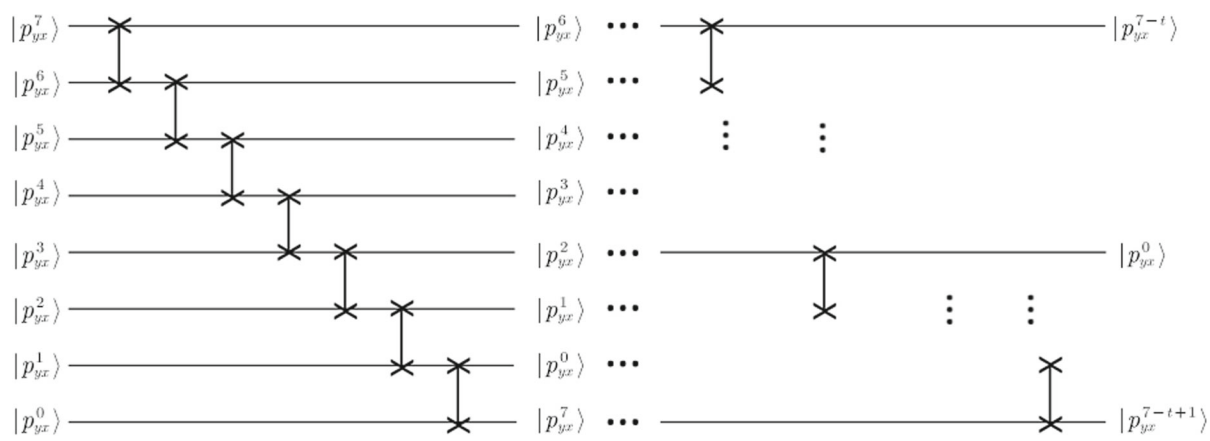

Fig. 10 Quantum circuit of qubit-level cyclic shift operation

5 Overlapping feedback diffusion of quantum images

In order to improve the avalanche effect of the encryption algorithm, an overlapping feedback diffusion method of quantum images is proposed, as shown in Fig. 11. Small changes in the original plaintext will also cause great differences in the ciphertext. The quantum overlapping feedback diffusion operation is shown in Eq. (17):

$$\begin{cases} |c_{yx}^{j}\rangle = |C_{y-1x}^{j}\rangle \oplus |Z_{yx}^{j}\rangle \\ |C_{yx}^{j}\rangle = |c_{yx}^{j}\rangle \oplus |X1_{yx}^{j}\rangle \end{cases} \tag{17}$$

where X1 denotes the sequence of encryption keys, and the quantum image is used to store the encryption key. Therefore, the quantum key image $|X1\rangle$ is generated using the NEQR model.

Z is the input of the diffusion operation. Depending on the actual encryption process, it can be either the original plaintext or the output result of the previous encryption operation. In our proposed algorithm, here Z is the result of the previous scrambling step. As a result, the NEQR model is used to construct the quantum image$|Z\rangle$.

$|c_{yx}^{j}\rangle$ is the j-th qubit of the y-th element of the x-th row in the diffusion intermediate result. $|C_{y-1x}^{j}\rangle$ is the j-th qubit of the $(y-1)$-th element of the x-th row in the diffusion output result. $|C_{yx}^{j'}\rangle$ is the j-th qubit of the y-th element of the x-th row in the diffusion output result.

where the first value of $|C_{yx}^{j}\rangle$ is the inverse of the first value of the $|Z_{yx}^{j}\rangle$ value. $j = 0,1,2,\ldots,7$.

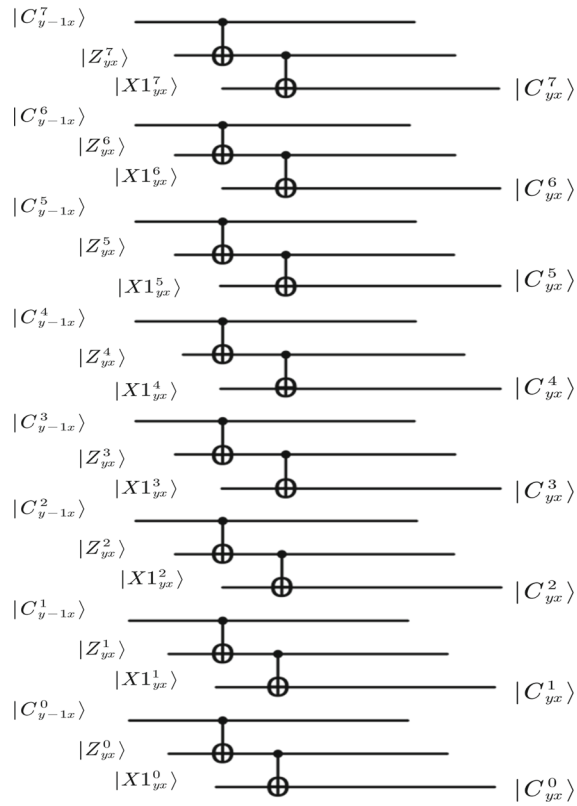

Fig. 11 Quantum circuit with overlapping feedback diffusion

The result of quantum image overlap feedback diffusion related is not only to the encryption key, but also to the result of the previous qubit diffusion, which can satisfy the avalanche effect and improve the security of the algorithm.

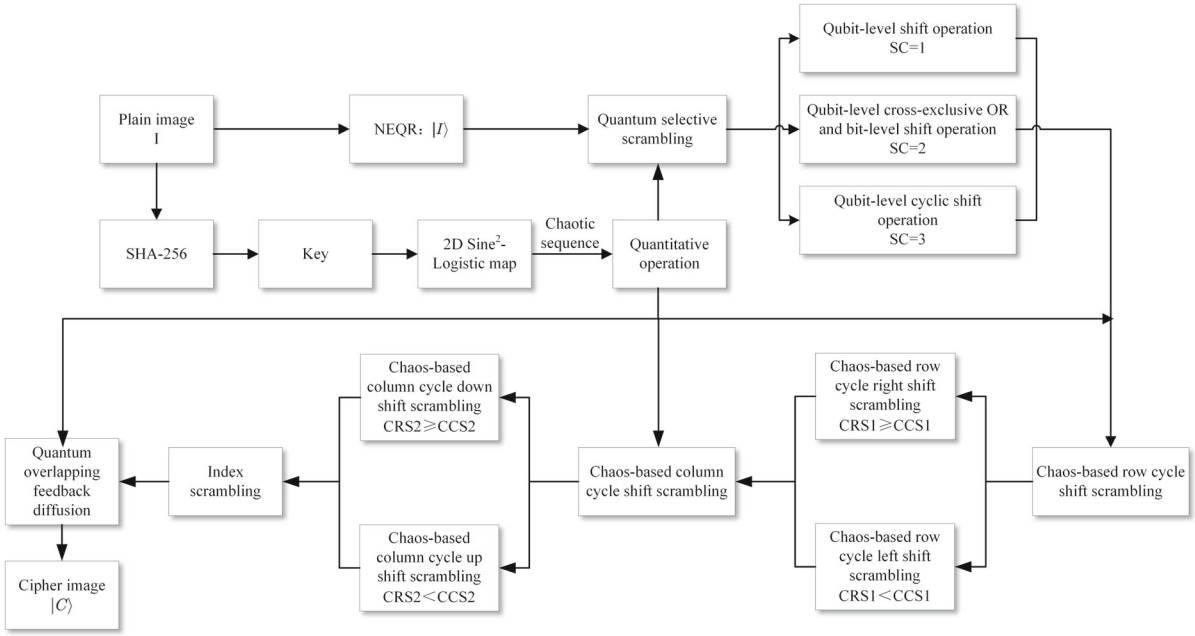

Fig. 12 Encryption flow chart

6 Quantum image encryption scheme

The designed quantum image encryption scheme consists of three stages. In the key generation stage, a 2D cross $Sine^2-Logistic$ chaotic map is used to generate random key sequences related to the plaintext image. In the qubit-level scrambling stage, the quantum selective scrambling operation is used to scramble the position of the qubit, and at the same time, it can disguise pixel values, achieving the effect of confusion and diffusion. In the qubit-level diffusion stage, the avalanche effect of the encryption scheme is further improved using the overlapping feedback diffusion method. The proposed scheme's specific implementation steps are described below, and the encryption flowchart is shown in Fig. 12.

Step 1. Use SHA-256 to calculate the hash value of the plaintext image I with the size of $M \times N$. The following formula may be used to obtain the 256-bit hash value represented by a hexadecimal array:

$$H(I) = Sha256(I) = [h_1, h_2, \ldots, h_{64}] \tag{18}$$

Step 2. The initial value of the 2D cross $Sine^2 - Logistic$ chaotic map is generated using array $H\ (I)$ in the following ways:

$$\begin{cases} x_0 = hex2dec(H(I)(\alpha : \alpha + 7)) \times 10^{-10} \\ y_0 = hex2dec(H(I)(\beta : \beta + 7)) \times 10^{-10} \end{cases} \tag{19}$$

where $hex2dec()$ represents the conversion function of the hexadecimal number to the decimal number. α, β are the keys set by the user.

Step 3. According to the NEQR model shown in Eq. (9), the classical image I is represented as a quantum image $|I\rangle$.

Step 4. Iterate the 2D cross $Sine^2-Logistic$ chaotic map with the initial values x_0, y_0 obtain two pseudo-random sequences X, Y with lengths of $M \times N$. The pseudo-random sequences X and Y are then mapped to between 0 and 255, representing $X1$ and $Y1$.

$$\begin{cases} X = \{x(1), x(2), x(3), \ldots, x(M \times N)\} \\ Y = \{y(1), y(2), y(3), \ldots, y(M \times N)\} \end{cases} \tag{20}$$

Step 5. The cyclic row/column shift control sequences $CRS1, CRS2, CCS1, CCS2$ are obtained by segmentation:

$$\begin{cases} CRS1 = X1(1 : M) \\ CRS2 = X1(M + 1 : 2 \times M) \\ CCS1 = Y1(1 : N) \\ CCS2 = Y1(N + 1 : 2 \times N) \end{cases} \tag{21}$$

Step 6. The chaotic random sequence Y is mapped between 1 and 3, and between 1 and 4 to obtain the selection control sequence SC and the cyclic shift con-

trol sequence CS, respectively.

$$\begin{cases} SC = uint8(mod(ceil(Y * 10^6), 3) + 1), \\ \qquad SC \in [1, 2, 3] \\ CS = uint8(mod(ceil(Y * 10^6), 4) + 1), \\ \qquad CS \in [1, 2, 3, 4] \end{cases} \tag{22}$$

Step 7. The proposed quantum selective scrambling method (in Sect. 4) changes the gray value of the quantum image $|I\rangle$. The controlled swap gate U_{YX} is defined as the sub-operation S_{YX}. The specific description is as follows:

$$\begin{aligned} S_{YX} &= \left(I \otimes \sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |yx\rangle\langle yx| \right) \\ &+ \begin{cases} U_{YX} \otimes |YX\rangle\langle YX|, SC = 1 \\ U_{YX} \otimes |YX\rangle\langle YX|, SC = 2 \\ U_{YX} \otimes |YX\rangle\langle YX|, SC = 3 \end{cases} \end{aligned} \tag{23}$$

The qubit-level selective shift operation of the pixel value, which can be realized by the quantum sub-operation S_{YX};

$$\begin{aligned} & S_{YX}|I\rangle \\ &= S_{YX}\left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |P_{yx}\rangle|yx\rangle \right) \\ &= \frac{1}{2^n} S_{YX}\left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |P_{yx}\rangle|yx\rangle + |P_{YX}\rangle|YX\rangle \right) \\ &= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |P_{yx}\rangle|yx\rangle \right. \\ &+ \left. \begin{cases} U_{YX}|P_{YX}\rangle|YX\rangle, SC = 1 \\ U_{YX}|P_{YX}\rangle|YX\rangle, SC = 2 \\ U_{YX}|P_{YX}\rangle|YX\rangle, SC = 3 \end{cases} \right) \\ &= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX}}^{2^n-1} |P_{yx}\rangle|yx\rangle + \right. \\ & \left. \begin{cases} |p_{YX}^3 p_{YX}^1 p_{YX}^2 p_{YX}^7 p_{YX}^0 p_{YX}^5 p_{YX}^6 p_{YX}^4\rangle|YX\rangle, SC = 1 \\ |p_{YX}^{3'} p_{YX}^{5'} p_{YX}^{1'} p_{YX}^{4'} p_{YX}^{0'} p_{YX}^{2'} p_{YX}^{6'} p_{YX}^{7'}\rangle|YX\rangle, SC = 2 \\ |p_{YX}^{7-t} \cdots p_{YX}^0 \cdots p_{YX}^{7-t+1}\rangle|YX\rangle, SC = 3 \end{cases} \right) \end{aligned} \tag{24}$$

$$\begin{aligned} & S_{Y_1X_1} S_{YX}|I\rangle \\ &= S_{Y_1X_1}(S_{YX}(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |P_{yx}\rangle|yx\rangle)) \\ &= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX, Y_1X_1}}^{2^n-1} |P_{yx}\rangle|yx\rangle \right. \\ &+ \begin{cases} U_{YX}|P_{YX}\rangle|YX\rangle, SC = 1 \\ U_{YX}|P_{YX}\rangle|YX\rangle, SC = 2 \\ U_{YX}|P_{YX}\rangle|YX\rangle, SC = 3 \end{cases} \\ &+ \left. \begin{cases} U_{YX}|P_{Y_1X_1}\rangle|Y_1X_1\rangle, SC = 1 \\ U_{YX}|P_{Y_1X_1}\rangle|Y_1X_1\rangle, SC = 2 \\ U_{YX}|P_{Y_1X_1}\rangle|Y_1X_1\rangle, SC = 3 \end{cases} \right) \\ &= \frac{1}{2^n}\left(\sum_{y=0}^{2^n-1} \sum_{\substack{x=0 \\ yx \neq YX, Y_1X_1}}^{2^n-1} |P_{yx}\rangle|yx\rangle \right. \\ &+ \begin{cases} |p_{YX}^3 p_{YX}^1 p_{YX}^2 p_{YX}^7 p_{YX}^0 p_{YX}^5 p_{YX}^6 p_{YX}^4\rangle|YX\rangle, \\ \quad SC = 1 \\ |p_{YX}^{3'} p_{YX}^{5'} p_{YX}^{1'} p_{YX}^{4'} p_{YX}^{0'} p_{YX}^{2'} p_{YX}^{6'} p_{YX}^{7'}\rangle|YX\rangle, \\ \quad SC = 2 \\ |p_{YX}^{7-t} \cdots p_{YX}^0 \cdots p_{YX}^{7-t+1}\rangle|YX\rangle, \\ \quad SC = 3 \end{cases} \\ &+ \left. \begin{cases} |p_{Y_1X_1}^3 p_{Y_1X_1}^1 p_{Y_1X_1}^2 p_{Y_1X_1}^7 p_{Y_1X_1}^0 p_{Y_1X_1}^5 p_{Y_1X_1}^6 p_{Y_1X_1}^4\rangle|Y_1X_1\rangle, \\ \quad SC = 1 \\ |p_{Y_1X_1}^{3'} p_{Y_1X_1}^{5'} p_{Y_1X_1}^{1'} p_{Y_1X_1}^{4'} p_{Y_1X_1}^{0'} p_{Y_1X_1}^{2'} p_{Y_1X_1}^{6'} p_{Y_1X_1}^{7'}\rangle|Y_1X_1\rangle \\ \quad SC = 2 \\ |p_{Y_1X_1}^{7-t} \cdots p_{Y_1X_1}^0 \cdots p_{Y_1X_1}^{7-t+1}\rangle|Y_1X_1\rangle, SC = 3 \end{cases} \right) \end{aligned} \tag{25}$$

We change all the pixel values of the quantum plaintext image $|I\rangle$ to obtain the quantum selective scrambled image $|I_1\rangle$ as follows:

$$\begin{aligned} S|I\rangle &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} S_{YX}|I\rangle \\ &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^n-1} S_{YX}\left(\frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |P_{YX}\rangle|YX\rangle \right) \\ &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} S_{YX}(|P_{YX}\rangle|YX\rangle) \\ &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \begin{cases} |p_{YX}^3 p_{YX}^1 p_{YX}^2 p_{YX}^7 p_{YX}^0 p_{YX}^5 \\ \quad p_{YX}^6 p_{YX}^4\rangle|YX\rangle, SC = 1 \\ |p_{YX}^{3'} p_{YX}^{5'} p_{YX}^{1'} p_{YX}^{4'} p_{YX}^{0'} p_{YX}^{2'} \\ \quad p_{YX}^{6'} p_{YX}^{7'}\rangle|YX\rangle, SC = 2 \\ |p_{YX}^{7-t} \cdots p_{YX}^0 \cdots p_{YX}^{7-t+1}\rangle|YX\rangle, \\ \quad SC = 3 \end{cases} \end{aligned}$$

$$= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |P'_{YX}\rangle |YX\rangle$$
$$= |I'\rangle \tag{26}$$

Step 8. The chaos-based row/column cyclic shift method is used to change the position of image pixels and reduce the correlation between adjacent pixels. Classic grayscale information is accurately extracted from quantum image models by quantum measurement, as shown in Algorithm 1.

Algorithm 1: The chaos-based row/column cyclic shift method

Input: Read the classic image I_1 of size M×N, Sequence CRS1,CRS2,CCS1,CCS2
Output: Scrambling image Z

```
for i ← to M do
    if CRS1>=CCS1 then
        z(i,:)= circshift(I1(i,:),double(CRS1(i))-
        double(CCS1(i)));
    else
        z(i,:)= circshift(I1(i,:),-(double(CCS1(i))-
        double(CRS1(i))));
    end
end
for j ← to N do
    if CRS2>=CCS2 then
        zz(:,j)=
        circshift(z(:,j),double(CRS2(j))-double(CCS2(j)));
    else
        zz(:,j)= circshift(z(:,j),-(double(CCS2(j))-
        double(CRS2(j))));
    end
end
```

In the case of the 4×4 image shown in Fig. 13, it is clear that the pixel values at each location have changed to achieve confusion. Then, an index scrambling operation is performed on the scrambled image, and finally, a scrambled image Z with a size of $M \times N$ is obtained.

Step 9. The scrambled image Z can be expressed as a quantum state through Eq. (9) of NEQR.

Step 10. The final ciphertext image $|C\rangle$ is obtained using overlapping feedback diffusion. The diagram in Fig. 14 briefly describes the chaotic overlapping feedback diffusion process, which achieves the avalanche effect and greatly improves the algorithm's security.

Since this algorithm is symmetric, the decryption process is the inverse of the encryption process.

7 Experimental simulation and performance analysis

To verify the security and effectiveness of the algorithm, three grayscale images of 512×512 "Boat," "Pepper" and "Baboon," a color image "Lung" and two gray images "House" and "Butterfly" of 256×256 are used as test images.

The experiment was carried out in the following environment: Windows 10 operating system, numerical simulation in MATLAB R2015b. The simulation results of encryption and decryption are shown in Fig. 15. No meaningful information can be observed at all anymore from the encrypted images Fig. 15b, e, h. The decrypted images Fig. 15c, f, i completely reconstruct the original content of the plaintext images.

7.1 Key space analysis

It is noted that an encryption algorithm's key space is sufficiently large (greater than 2^{100}), it may successfully resist brute force attacks [44]. The encryption algorithm proposed in this paper has three keys x_0, y_0, μ, and the accuracy of the initial key is set to 10^{-16}, so the key space is $(10^{16})^3 = 10^{48} > 2^{100} \approx 1.27 \times 10^{30}$. Therefore, this encryption scheme has a large key space, which enables it to resist brute force attacks.

7.2 Key sensitivity analysis

Key sensitivity refers to the small changes in the key during the image encryption process, which will have a great impact on the decrypted image [45]. Given initial key $key = x_0, y_0$. We change the initial keys x_0 and y_0 by 10^{-15} to obtain the changed keys $Ekey1$, $Ekey2$:

$$\begin{cases} Ekey1 = \{x_0 + 10^{-15}, y_0\} \\ Ekey2 = \{x_0, y_0 + 10^{-15}\} \end{cases} \tag{27}$$

$$\begin{cases} C = encrypt(key, P) \\ C1 = encrypt(Ekey1, P) \\ C2 = encrypt(Ekey2, P) \end{cases} \tag{28}$$

$$\begin{cases} D = decrypt(key, C) \\ W1 = decrypt(Ekey1, C) \\ W2 = decrypt(Ekey2, C) \end{cases} \tag{29}$$

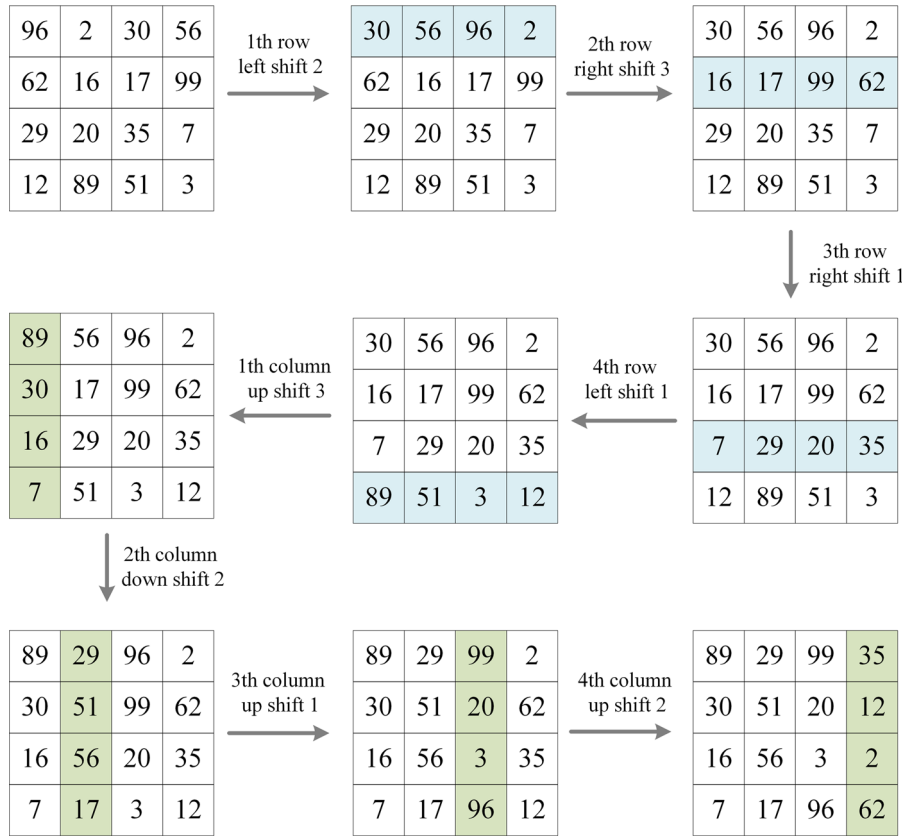

Fig. 13 Chaos-based row/column cyclic shift operation

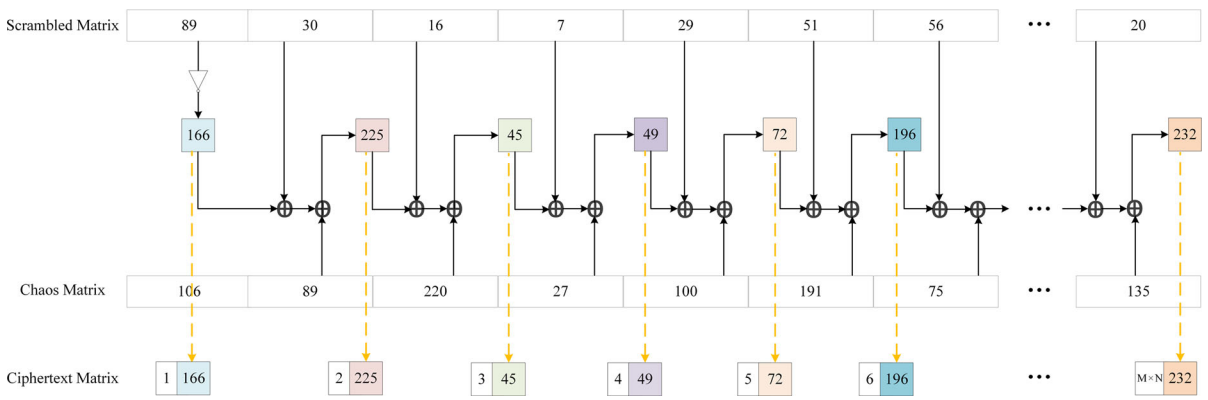

Fig. 14 Chaotic overlapping feedback diffusion process

where encrypt() and decrypt() are the algorithm functions for encryption and decryption, respectively. P is a plaintext image, and C, C1 and C2 are images encrypted with keys key, $Ekey1 and Ekey2$, respectively. D is the correctly decrypted image decrypted with the correct key. W1 and W2 are the wrong decrypted images obtained by performing decryption operations with wrong keys $Ekey1$, $Ekey2$.

Figure 16 shows the correctly decrypted image D of "Boat" and its corresponding incorrectly decrypted images W1 and W2. Figure 17 shows the "Boat" plaintext image and its corresponding encrypted images C, C1 and C2.

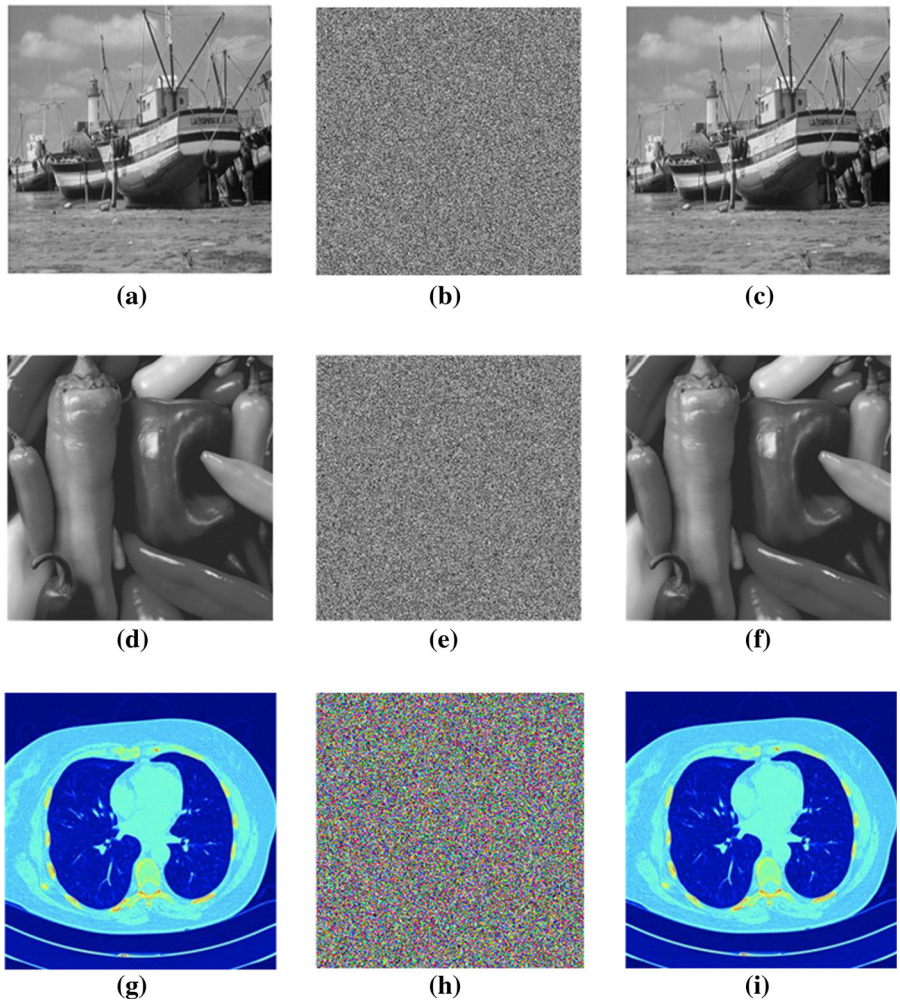

Fig. 15 The results of encryption and decryption: **a** boat; **b** encrypted (**a**); **c** decrypted (**b**); **d** peppers; **e** encrypted (**d**); **f** decrypted (**e**); **g** lung; **h** encrypted (**g**); **i** decrypted (**h**)

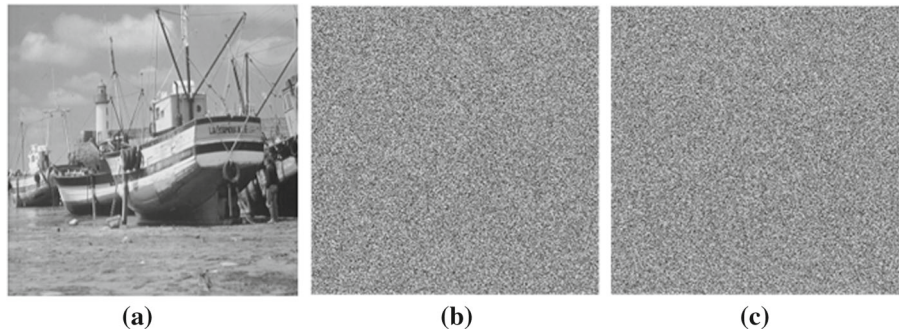

Fig. 16 **a** Correctly decrypted image D; **b** incorrectly decrypted image W1; **c** incorrectly decrypted image W2

In this paper, key sensitivity analysis is carried out for the three images of "Boat," "Peppers," "Baboon" and "House," respectively. To illustrate the algorithm's key sensitivity during the decryption process, Table 3 compares the NPCR and UACI [46] values obtained after decrypting images using the correct and wrong decryption keys. The introduction of NPCI and UACI is detailed in Sect. 7.6. Moreover, the NPCR, UACI values are calculated between different encrypted images obtained using the same plaintext image but also with different encryption keys. The calculation results are

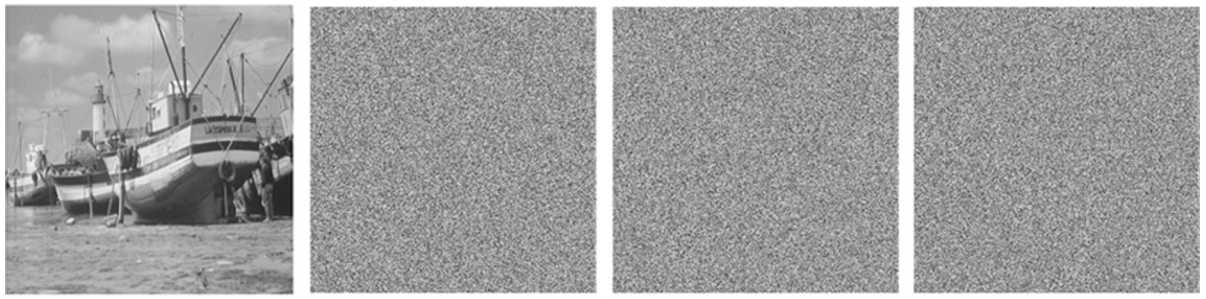

Fig. 17 **a** Plaintext image; **b** encrypted image C; **c** encrypted image C1; **d** encrypted image C2

Table 3 Key sensitivity analysis result of the difference between decryption keys 10^{-15}(NPCR/UACI) (unit:%)

Image size	Image	NPCR(D, W1)	UACI(D, W1)	NPCR(D, W2)	UACI(D, W2)
512×512	Boat	99.5117	27.1434	99.5079	27.1695
512×512	Peppers	99.5018	28.2322	99.4732	28.1669
512×512	Baboon	99.5785	26.8459	99.5533	26.8630
256×256	House	99.3668	27.5692	99.3835	27.5201

Table 4 Key sensitivity analysis results of the difference between encryption keys 10^{-15}(NPCR/UACI) (unit:%)

Image size	Image	NPCR(C, C1)	UACI(C, C1)	NPCR(C, C2)	UACI(C, C2)
512×512	Boat	99.6154	33.5592	99.6028	33.3755
512×512	Peppers	99.6048	33.5099	99.5949	33.5059
512×512	Baboon	99.6098	33.5075	99.6113	33.5270
256×256	House	99.5743	33.5851	99.5972	33.4524

listed in Table 4. The results show that the encryption scheme proposed in this paper is very sensitive to keys.

7.3 Histogram analysis

Histogram is a common tool that can be used to evaluate the uniformity of ciphertext images. Figure 18 shows the histograms for the plaintext and encrypted images of the three images tested in this paper. We can find that the histogram of the plaintext image is quite different from that of the encrypted image, which is rather uniform.

The Chi-square test is an important method to quantitatively analyze the uniform distribution of pixels in the encrypted image [47]. The calculation formula of the x^2 test is shown in Eq. (30):

$$x^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0}, v_0 = \frac{M \times N}{256} \tag{30}$$

Table 5 shows the results of the x^2 test. The test result of the encrypted image is lower than 293.24783, and the test is all passed. Through histogram analysis and the x^2 test, it is proven that the algorithm can resist statistical attacks.

7.4 Correlation of adjacent pixels

In general, images present information with specific and specific meanings, and the pixel contents are continuous, so the correlation between two neighboring pixels is very high. Attackers can crack encryption algorithms by analyzing the correlation between pixels in encrypted images. A good encryption algorithm should attempt to minimize the correlation between adjacent pixels in the encrypted image.

We randomly select 5000 pairs of adjacent pixels in horizontal, vertical and diagonal directions from the plaintext and encrypted images of the "Boat," respec-

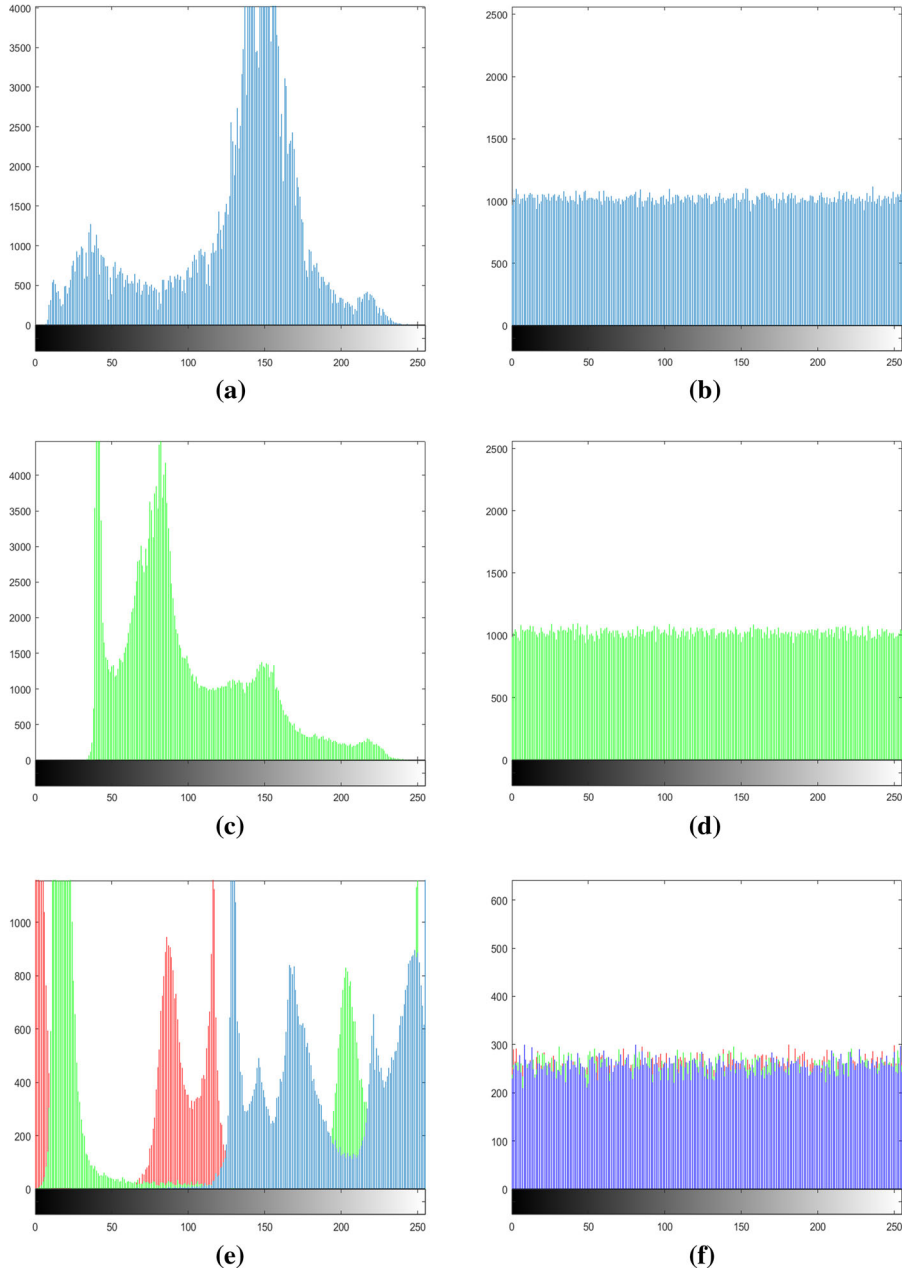

Fig. 18 **a**, **c**, **e** Histograms of plaintext images "Boat," "Peppers," "Lung"; **b**, **d**, **f** histograms of encrypted images "Boat," "Peppers," "Lung"

Table 5 x^2 test

Image size	Image	x^2 value	Pass or fail
512×512	Boat	274.4766	Pass
512×512	Peppers	249.8965	Pass
512×512	Baboon	247.1309	Pass
256×256	Lung	274.6510	Pass
256×256	House	233.7188	Pass
256×256	Butterfly	245.3906	Pass

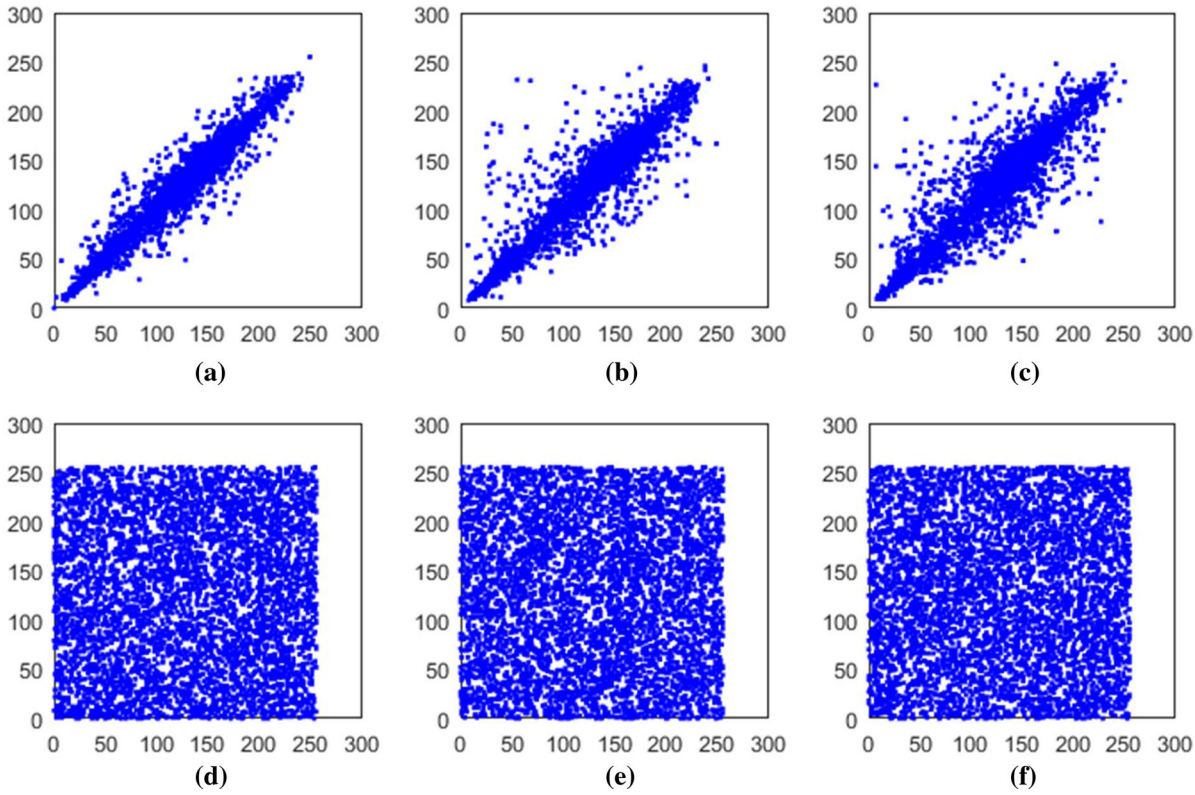

Fig. 19 **a–c** are the correlations between adjacent pixels in the horizontal, vertical and diagonal directions of the plaintext image "Boat," respectively; **d–f** are the correlations of adjacent pixels in the horizontal, vertical and diagonal directions of the encrypted image "Boat," respectively

tively, to calculate and compare the correlation and correlation coefficients of the plaintext/ciphertext, as shown in Fig. 19. The correlation coefficient is calculated as follows [48]:

$$\begin{cases} r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \\ \operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \end{cases} \tag{31}$$

where x and y represent adjacent pixels in two grayscale images and N is the total number of pixels in the image.

As seen in Fig. 19, the correlations in all directions of the encrypted images are very small and uniformly distributed in the figure. Table 6 lists the calculation results of the correlation coefficients of this algorithm. As shown, the correlation coefficients between adjacent pixels in the encrypted image are extremely close to 0, indicating that the encryption method is sufficiently secure.

7.5 Information entropy

The information entropy of an image may be used to determine the average amount of information contained within it, is another important factor in evaluating the resistance of a cryptographic system. Information entropy is defined as [50]:

Table 6 Correlation analysis

Image size	Image	Horizontal	Vertical	Diagonal
512×512	Boat	0.9721	0.9425	0.9248
	Encrypted boat	0.0008	−0.0074	−0.0060
512×512	Peppers	0.9813	0.9759	0.9623
	Encrypted peppers	0.0002	−0.0021	−0.0083
512×512	Baboon	0.7687	0.8642	0.8642
	Encrypted baboon	−0.0026	−0.0002	−0.0021
256×256	Lung_R	0.9386	0.9639	0.9049
	Lung_G	0.9677	0.9820	0.9589
	Lung_B	0.9315	0.9575	0.9072
	Encrypted lung_R	0.0021	−0.0004	0.0073
	Encrypted lung_G	−0.0005	−0.0060	0.0097
	Encrypted lung_B	−0.0030	−0.0001	−0.0011
256×256	House	0.9116	0.8602	0.7933
	Encrypted house	0.0002	−0.0079	−0.0086
256×256	Butterfly	0.9277	0.9372	0.9162
	Encrypted butterfly	−0.0021	0.0039	−0.0009
256×256	[33]	0.0153	0.0191	0.0055
512×512	[36]	0.0295	0.0187	0.0393
512×512	[49]	−0.0072	0.0258	−0.0098

$$H(s) = -\sum_{i=0}^{2^L-1} p(s_i)\log_2 p(s_i) \tag{32}$$

where L is the total number of pixels in the encrypted image, and $p(s_i)$ represents the probability of s_i.

According to Eq. (32), the higher the randomness of the pixel is, the larger the image's information entropy. The greater the entropy is, the higher the security. The ideal value of the information entropy of an 8-bit image is 8. Table 7 shows the information entropy of the encrypted images. Compared to other algorithms, our encryption algorithm's entropy is quite near the ideal value and can effectively resist an entropy attack.

Table 7 Information entropy

Image size	Image	Entropy value
512×512	Boat	7.9992
512×512	Peppers	7.9993
512×512	Baboon	7.9993
256×256	Lung_R	7.9968
	Lung_G	7.9967
	Lung_B	7.9971
256×256	House	7.9974
256×256	Butterfly	7.9973
256×256	[51]	7.9115
512×512	[52]	7.9289
512×512	[53]	7.9985

7.6 Differential attack

A good algorithm for image encryption should be sensitive to plaintext images; even if the pixels in the plaintext image are slightly changed, two completely different encrypted images can be obtained. Two important indicators to evaluate the effect of differential attack analysis are the number of pixel change rates (NPCR) and the unified average change intensity (UACI). NPCR and UACI are defined as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{33}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{34}$$

Table 8 NPCR and UACI results

Image size	Image	NPCR(%)	UACI(%)
512×512	Boat	99.6067	33.4875
512×512	Peppers	99.6056	33.4593
512×512	Baboon	99.6040	33.4720
256×256	Lung_R	99.5972	33.4784
	Lung_G	99.6109	33.4082
	Lung_B	99.6033	33.4672
256×256	House	99.6155	33.4689
256×256	Butterfly	99.6078	33.4650
256×256	[54]	99.58	27.31
512×512	[55]	99.68	33.93
512×512	[56]	99.6273	32.4228

where $C_1(i, j)$ and $C_2(i, j)$ are, respectively, the encrypted images before and after changing one pixel of the plaintext image, and $D(i, j)$ is defined as Eq. (35).

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{35}$$

We randomly change a pixel value for the grayscale images "Boat," "Peppers," "Baboon," "House," "Butterfly" and color image "Lung" and perform NPCR and UACI tests. It can be seen in Table 8 that compared with the literature algorithm, the proposed algorithm's NPCR and UACI values are quite near the theoretical values, and the scheme performs well against differential attacks.

7.7 Cutting attack

During image transmission and storage, it is necessary to consider the possibility that a portion of the data may be corrupted or intercepted. To evaluate the ability of the encryption scheme to recover the plaintext image after losing part of the ciphertext data, that is, the algorithm's resistance to cutting attacks, the areas of size 128×128, 256×256 and 512×256 are deleted from the encrypted image "Boat," as shown in Fig. 20a–d.

In Fig. 20e–h, it can be seen that, even after the loss of 1/2 of the data, decrypted images recover information about plaintext images well. Experiments show that this algorithm can effectively resist cutting attacks.

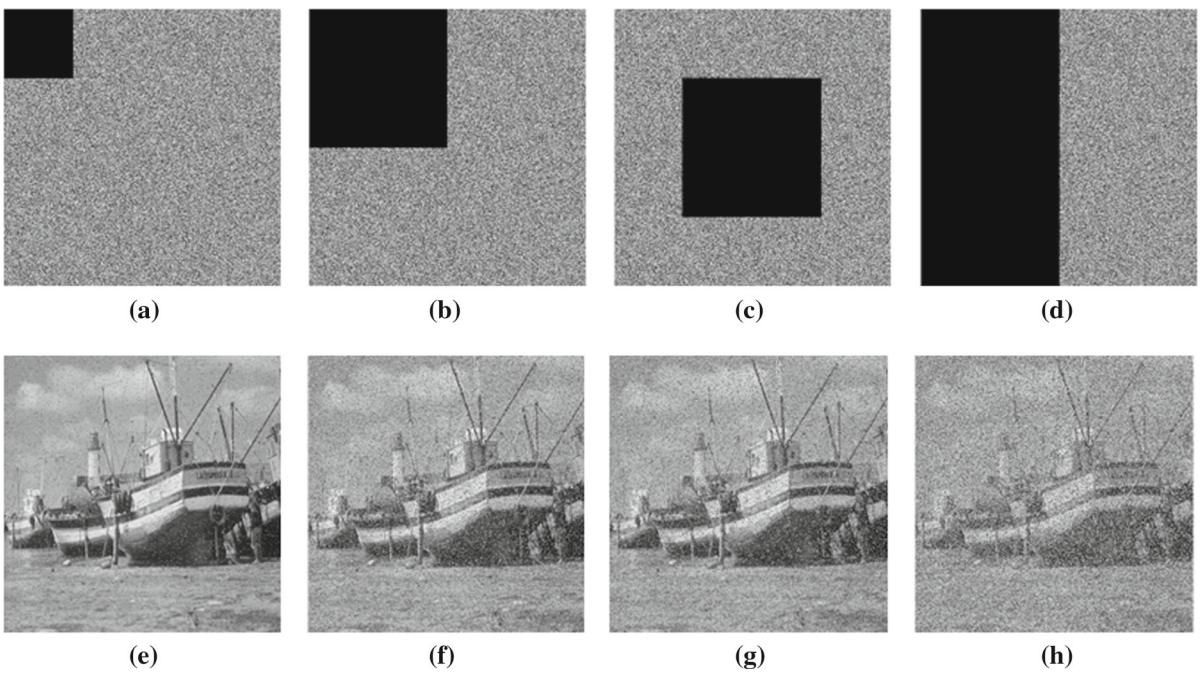

Fig. 20 "Boat" cutting attack: **a** Cut loss 128×128; **b**, **c** cut loss 256×256 in different positions; **d** cut loss 512×256; **e**–**h** correspond to the decrypted images of (**a**)–(**d**), respectively

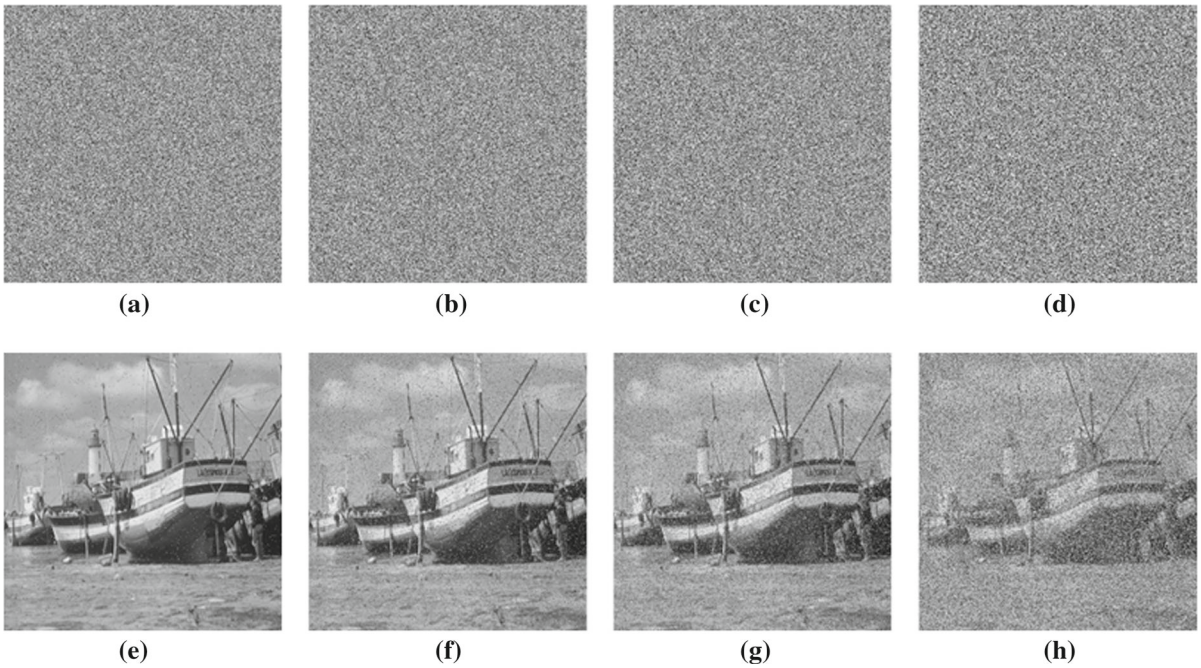

Fig. 21 "Boat" noise attack: **a**–**d** cipher images with 0.01, 0.05, 0.1 and 0.3 salt and pepper noise; **e**–**h** correspond to the decrypted images of (**a**)–(**d**), respectively

7.8 Noise attack

Interference noise from the transmission or storage process can have an impact on the decryption process of the algorithm. As a result, a secure encryption scheme should be resistant to noise attacks.

We use 0.01, 0.05, 0.1 and 0.3 salt and pepper noise to attack the encrypted image "Boat," as shown in Fig. 21a–d. The corresponding decryption results after these noise attacks are shown in Fig. 21e–h. Experiments show that the algorithm can resist noise attacks well and has good robustness.

8 Conclusion

This paper proposes a qubit-level selective scrambling and overlapping feedback diffusion method based on a new 2D cross $Sine^2 - Logistic$ chaotic map. A new type of 2D cross $Sine^2 - Logistic$ hyperchaotic system is proposed, which greatly improves the key space and has higher chaotic behavior. Therefore, the chaotic map proposed in this paper is more suitable for the image encryption field. In the quantum encryption algorithm, the SHA-256 function is used to calculate the hash value of the plaintext image to obtain the key, which can effectively resist the chosen plaintext attack. A quantum selective scrambling method based on the NEQR model is proposed. Changing the position of the bit level can effectively change the pixel value and achieve the effect of confusion diffusion. In order to improve the security of the algorithm, a quantum overlapping feedback diffusion method is proposed to improve the avalanche effect of the encryption scheme. A chaos-based row/column cyclic shift method is designed to reduce the correlation between adjacent pixels. The simulation and performance analysis results indicate that the quantum image encryption scheme is both safe and reliable. In future work, we will conduct more in-depth research on asymmetric cryptography to improve and refine our algorithm. The key transmission problem in symmetric cryptography is better solved to achieve a more secure encryption algorithm. Additionally, we will conduct more in-depth research on new chaotic systems, quantum chaotic systems and more complex chaotic systems, expecting better results.

Funding This research is supported by the National Key Research and Development Program (2018YFB1800303), the Natural Science Foundation Project of the Science and Technol-

ogy Department, Jilin Province (20190201188JC), the Changchun University of Science and Technology Youth Fund (XJJLG-2019-01) and the Jilin Province Science and Technology Development Plan Project, International Science and Technology Cooperation (20220402013GH).

Data availability The author declares that the data supporting the results of this study are available in the article.

Declarations

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

References

1. Li, R.: Fingerprint-related chaotic image encryption scheme based on blockchain framework. Multimed. Tools Appl. **80**(20), 30583–30603 (2021)
2. Ali, T.S., Ali, R.: A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimed. Tools Appl. **79**(27), 19853–19873 (2020)
3. Matthews, R.: On the derivation of a"chaotic"encryption algorithm. Cryptologia **13**(1), 29–42 (1989)
4. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurc. Chaos **8**(06), 1259–1284 (1998)
5. Nezhad, S.Y.D., Safdarian, N., Zadeh, S.A.H.: New method for fingerprint images encryption using dna sequence and chaotic tent map. Optik **224**, 165661 (2020)
6. Moumen, A., Sissaoui, H.: Images encryption method using steganographic lsb method, aes and rsa algorithm. Nonlinear Eng. **6**(1), 53–59 (2017)
7. Ye, G., Jiao, K., Huang, X.: Quantum logistic image encryption algorithm based on SHA-3 and rsa. Nonlinear Dyn. **104**(3), 2807–2827 (2021)
8. Su, Y., Xu, W., Li, T., Zhao, J., Liu, S.: Optical color image encryption based on fingerprint key and phase-shifting digital holography. Opt. Lasers Eng. **140**, 106550 (2021)
9. Li, C., Qian, K., He, S., Li, H., Feng, W.: Dynamics and optimization control of a robust chaotic map. IEEE Access **7**, 160072–160081 (2019)
10. Yu, J., Li, C., Song, X., Guo, S., Wang, E.: Parallel mixed image encryption and extraction algorithm based on compressed sensing. Entropy **23**(3), 278 (2021)
11. Moumen, A., Bouye, M., Sissaoui, H.: New secure partial encryption method for medical images using graph coloring problem. Nonlinear Dyn. **82**(3), 1475–1482 (2015)
12. Huang, Z.J., Cheng, S., Gong, L.H., Zhou, N.R.: Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. Opt. Lasers Eng. **124**, 105821 (2020)
13. Zhou, Y., Li, C., Li, W., Li, H., Feng, W., Qian, K.: Image encryption algorithm with circle index table scrambling and partition diffusion. Nonlinear Dyn. **103**(2), 2043–2061 (2021)
14. Liu, Y., Tang, S., Liu, R., Zhang, L., Ma, Z.: Secure and robust digital image watermarking scheme using logistic and rsa encryption. Expert Syst. Appl. **97**, 95–105 (2018)
15. Li, Z., Peng, C., Tan, W., Li, L.: A novel chaos-based color image encryption scheme using bit-level permutation. Symmetry **12**(9), 1497 (2020)
16. Hosny, K.M., Kamal, S.T., Darwish, M.M., Papakostas, G.A.: New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. Electronics **10**(9), 1066 (2021)
17. Liu, J., Zhang, M., Tong, X., Wang, Z.: Image compression and encryption algorithm based on compressive sensing and nonlinear diffusion. Multimed. Tools Appl. **80**, 25433–25452 (2021)
18. Talhaoui, M.Z., Wang, X.: A new fractional one dimensional chaotic map and its application in high-speed image encryption. Inf. Sci. **550**, 13–26 (2021)
19. Teng, L., Wang, X., Yang, F., Xian, Y.: Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. Nonlinear Dyn. **105**(2), 1859–1876 (2021)
20. Hua, Z., Zhou, Y.: Image encryption using 2D logistic-adjusted-sine map. Inf. Sci. **339**, 237–253 (2016)
21. Li, C., Chen, Z., Yang, X., He, S., Yang, Y., Du, J.: Self-reproducing dynamics in a two-dimensional discrete map. Eur. Phys. J. Spec. Topics **230**(7), 1959–1970 (2021)
22. 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)
23. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**(1), 63–84 (2011)
24. Zhang, Y., Lu, K., Gao, Y., Wang, M.: Neqr: a novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**(8), 2833–2860 (2013)
25. Yang, Y.G., Jia, X., Sun, S.J., Pan, Q.X.: Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding. Inf. Sci. **277**, 445–457 (2014)
26. Caraiman, S., Manta, V.: Image processing using quantum computing. In: 2012 16th International Conference on System Theory, Control and Computing (ICSTCC), pp. 1–6. IEEE (2012)
27. Sang, J., Wang, S., Li, Q.: A novel quantum representation of color digital images. Quantum Inf. Process. **16**(2), 1–14 (2017)
28. Sun, B., Iliyasu, A., Yan, F., Dong, F., Hirota, K.: An rgb multi-channel representation for images on quantum computers. J. Adv. Comput. Intell. Intell. Inform **17**(3) (2013)
29. Li, H.S., Zhu, Q., Zhou, R.G., Song, L., Yang, X.: Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. Quantum Inf. Process. **13**(4), 991–1011 (2014)
30. Yuan, S., Mao, X., Xue, Y., Chen, L., Xiong, Q., Compare, A.: Sqr: a simple quantum representation of infrared images. Quantum Inf. Process. **13**(6), 1353–1379 (2014)
31. Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log-polar images. Quantum Inf. Process. **12**(9), 3103–3126 (2013)

32. Sang, J., Wang, S., Song, X., Yan, X., Niu, X.: A novel representation for multi-channel log-polar quantum images. J. Inf. Hiding Multimed. Signal Process. **6**(2), 340–350 (2015)
33. Liu, X., Xiao, D., Liu, C.: Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. Quantum Inf. Process. **19**(8), 1–23 (2020)
34. Zhou, R.G., Li, Y.B.: Quantum image encryption based on Lorenz hyper-chaotic system. Int. J. Quantum Inf. **18**(05), 2050022 (2020)
35. Hu, W.W., Zhou, R.G., Jiang, S., Liu, X., Luo, J.: Quantum image encryption algorithm based on generalized Arnold transform and logistic map. CCF Trans. High Perform. Comput. **2**(3), 228–253 (2020)
36. Liu, X., Xiao, D., Liu, C.: Three-level quantum image encryption based on Arnold transform and logistic map. Quantum Inf. Process. **20**(1), 1–22 (2021)
37. Dai, J.Y., Ma, Y., Zhou, N.R.: Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4d hyper-chaotic henon map. Quantum Inf. Process. **20**(7), 1–24 (2021)
38. Luo, Y., Tang, S., Liu, J., Cao, L., Qiu, S.: Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt. Lasers Eng. **124**, 105836 (2020)
39. Wu, Y., Noonan, J.P., Yang, G., Jin, H.: Image encryption using the two-dimensional logistic chaotic map. J. Electron. Imag. **21**(1), 013014 (2012)
40. Hua, Z., Zhou, Y., Pun, C.M., Chen, C.P.: 2D sine logistic modulation map for image encryption. Inf. Sci. **297**, 80–94 (2015)
41. Gottwald, G.A., Melbourne, I.: The 0–1 test for chaos: a review. Chaos Detect. Predict. pp. 221–247 (2016)
42. Mansouri, A., Wang, X.: A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme. Inf. Sci. **563**, 91–110 (2021)
43. Zheng, J., Liu, L.: Novel image encryption by combining dynamic dna sequence encryption and the improved 2D logistic sine map. IET Image Proc. **14**(11), 2310–2320 (2020)
44. Khalil, N., Sarhan, A., Alshewimy, M.A.: An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. Opt. Laser Technol. **143**, 107326 (2021)
45. Man, Z., Li, J., Di, X., Sheng, Y., Liu, Z.: Double image encryption algorithm based on neural network and chaos. Chaos Solitons Fractals **152**, 111318 (2021)
46. Man, Z., Li, J., Di, X., Bai, O.: An image segmentation encryption algorithm based on hybrid chaotic system. IEEE Access **7**, 103047–103058 (2019)
47. Li, C.L., Zhou, Y., Li, H.M., Feng, W., Du, J.R.: Image encryption scheme with bit-level scrambling and multiplication diffusion. Multimed. Tools Appl. **80**(12), 18479–18501 (2021)
48. Es-Sabry, M., El Akkad, N., Merras, M., Saaidi, A., Satori, K.: A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators. Soft. Comput. **24**(5), 3829–3848 (2020)
49. Jiang, N., Dong, X., Hu, H., Ji, Z., Zhang, W.: Quantum image encryption based on henon mapping. Int. J. Theor. Phys. **58**(3), 979–991 (2019)
50. Moumen, A.: Medical and biological image analysis. In: Medical and Biological Image Analysis. IntechOpen (2018)
51. Wang, H., Wang, J., Geng, Y.C., Song, Y., Liu, J.Q.: Quantum image encryption based on iterative framework of frequency-spatial domain transforms. Int. J. Theor. Phys. **56**(10), 3029–3049 (2017)
52. Zhou, N., Hu, Y., Gong, L., Li, G.: Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. Quantum Inf. Process. **16**(6), 164 (2017)
53. Li, X.Z., Chen, W.W., Wang, Y.Q.: Quantum image compression-encryption scheme based on quantum discrete cosine transform. Int. J. Theor. Phys. **57**(9), 2904–2919 (2018)
54. Abd-El-Atty, B., El-Latif, A., Ahmed, A., Venegas-Andraca, S.E.: An encryption protocol for neqr images based on one-particle quantum walks on a circle. Quantum Inf. Process. **18**(9), 1–26 (2019)
55. Khan, M., Waseem, H.M.: A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS ONE **13**(11), e0206460 (2018)
56. Rajakumaran, C., Kavitha, R., et al.: Chaos based encryption of quantum images. Multimed. Tools Appl. **79**(33), 23849–23860 (2020)