



RESEARCH

# An image encryption approach based on a novel two-dimensional chaotic system

Mingjie Zhao · Lixiang Li · Zheng Yuan

Received: 3 March 2024 / Accepted: 20 July 2024 / Published online: 16 August 2024  
© The Author(s), under exclusive licence to Springer Nature B.V. 2024

**Abstract** Chaotic systems are applicable to image cryptography with their inherent properties. Unfortunately, in numerous existing chaos-based image cryptography, chaotic systems face the problems of uneven chaotic trajectories and narrow chaotic regions, which leads to hidden risks in the encryption approach. To solve these problems, a novel two-dimensional Sine-Arcsin-Cos-Arcsin (2D-SACA) chaotic model is constructed, which can design chaotic systems according to users' own needs, and then we propose an image encryption approach applying the designed chaotic systems. Compared with the existing chaotic systems in image cryptography, the designed chaotic systems have better randomness, sensitivity, wide chaotic regions and more uniform trajectory distribution. The major contribution of this scheme is to design a 2D-SACA chaotic model, which can generate different superior chaotic systems, and propose an image encryption approach that enables images of different dimensions and categories to be encrypted. Simulation analysis illustrates that this approach has superior performance, high efficiency, strong key sensitivity, and wide key space,

thanks to the sensitivity of designed chaotic systems and the extensive chaotic region, which can prevent various attacks. And even with noise interference and data loss, the original image can be successfully restored.

**Keywords** Image encryption · Image security · 2D chaotic model · 2D chaotic map

## 1 Introduction

With the popularization and evolution of the Internet of Things, digital images have developed into the preferred information carrier in network communication with their intuitive and vivid characteristics [1]. However, while enjoying the convenience brought by the development of science and technology, people also began to attach importance to the security of images. The disclosure of image information may lead to leakage of personal privacy information, and may also affect business secrets or national security [2]. Accordingly, image encryption has become an important technology to protect image information [3,4]. Image cryptography is dissimilar to text cryptography in that there is great redundancy and high pixel correlation [5–7]. In image cryptography with enormous data, Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are inefficient and have been gradually replaced by novel technologies [8,9], such as DNA coding [10–13], cellular automata [14,15], S-box [16,17],

---

M. Zhao · L. Li  
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China  
e-mail: zhaomingjie@bupt.edu.cn

Z. Yuan (✉)  
Beijing Electronic Science and Technology Institute, Beijing 100070, China  
e-mail: zyuan@tsinghua.edu.cn

compressed sensing [18–20], and chaotic systems [21–25] have emerged continuously.

Chaotic systems can greatly improve the performance of encryption algorithms because of their initial value sensitivity, aperiodicity and internal randomness, so they have a good application prospect in many fields, such as image cryptography, neural networks, secure communication, economics, mathematics, physics, and so on [26–28]. Chaotic systems can be categorized into one-dimensional (1D) and high-dimensional (HD) chaotic systems [29]. The 1D chaotic systems are straightforward frameworks and easy to implement, but they are easily cracked due to the limited chaotic region and simple trajectory. The HD chaotic systems exhibit superior structural complexity and chaotic performance, while the implementation cost is high [30].

The 2D chaotic systems not only have the easy realization of 1D systems but also have the complex chaotic behavior of HD systems, so they can give consideration to efficiency and performance. Recently, various 2D chaotic systems have been derived and implemented in image cryptography. Teng et al. [31] generated a 2D-Coupled system with good chaotic performance using the nonlinear function and two 1D maps and presented an image encryption technique grounded on the 2D-Coupled map. Hua et al. [32] first constructed a 2D-LSM chaotic system to overcome the weakness of the traditional chaotic system. Then, they designed a color image encryption approach with Latin squares and 2D-LSM. Teng et al. [33] developed a 2D-CLSS chaotic system with excellent chaotic properties and applied the 2D-CLSS system to image cryptography. Qiu et al. [34] produced a color image encryption method on the developed 2D-CSCM system, where emulation experiments proved that 2D-CSCM has beneficial chaotic behavior and this scheme has high security.

The 2D chaotic systems designed above have superior chaotic performance, but these systems are fixed and can increase the risk when utilizing identical chaotic systems in multiple algorithms. Thus, designing a universal chaotic model with superior chaotic performance has good application value and prospects. Zhou et al. [35] developed a 2D cross-coupled modular chaotic model (2D-CMCM) with good chaotic performance by using nonlinear function and mod operation, which can generate different chaotic systems. Then the chaotic system was introduced to implement permutation and diffusion simultaneously in the encryption stage. Security evaluation indicated that this scheme

enables several images of various dimensions and types to be encrypted, and has good anti-attack and encryption efficiency. Wang et al. [36] designed a 2D cross-coupled chaotic model (2D-CCCM), for producing various chaotic systems with complicated chaotic behaviors and extensive chaotic distribution range. Furthermore, a novel visual color image encryption approach was suggested, which adopts cyclic shift and scrambling technology to acquire a cryptographic image. The cryptographic image is hidden in the host image with the 2D discrete cosine transform, further improving the reliability of this method.

The chaotic system applied in the above-mentioned schemes has a narrow chaotic region, which leads to limited key space, weak security, and vulnerability to various attacks. To enlarge the chaotic region and strengthen the confidentiality of the encryption approach, an image encryption approach that can encrypt different sizes and types is proposed based on a novel chaotic model in this paper. Overall, the principal contributions of this paper are summarized below.

- (1) 2D-SACA chaotic model. To solve the problems of uneven chaotic trajectory and limited scope in existing chaotic systems, a novel 2D-SACA chaotic model is designed, which can design chaotic systems according to their requirements. The Logistic-Sine map and Cubic-Fraction map are combined as seed maps of 2D-SACA to generate the Sine-Arcsin-Cos-Arcsin-Logistic-Sine (2D-SACALS) map and Sine-Arcsin-Cos-Arcsin-Cubic-Fraction (2D-SACACF) map respectively.
- (2) Chaotic performance analysis. The performance of the 2D-SACALS map and 2D-SACACF map is evaluated by bifurcation diagram, trajectory diagram, Lyapunov exponent (LE), Shannon entropy (SE), sensitivity analysis, randomness tests, degree of non-periodicity and statistical complexity measure, demonstrating they have a widely hyperchaotic region, high non-periodic, excellent randomness and sensitivity, and their chaotic performance is superior.
- (3) Image encryption approach. To strengthen the capability of image protection, an image encryption approach is proposed. The image encryption scheme can encrypt images of different sizes and categories. SHA-512 generates the keys of the chaotic systems from the original image so that

each original image has a unique key. The proposed image encryption algorithm adopts the proposed 2D-SACALS map in both interference and diffusion stages, and does not use other interference and diffusion techniques.

- (4) Simulation and security evaluation. Extensive simulation analysis verifies that this approach has excellent performance and high efficiency, and can prevent statistical attacks and differential cryptanalysis. The key space is  $> 2^{912}$ , which can withstand brute force attacks. At the same time, it is extremely sensitive to the key although the key difference is  $10^{-16}$ , it cannot be decrypted successfully. When the cryptographic image is affected by noise pollution and data loss, most of the data can still be successfully decrypted.

The rest of the organizations in this article are given as follows. Section 2 constructs a novel 2D chaotic model. The performance of the designed chaotic systems is evaluated in Sect. 3. Section 4 details the image cryptosystem with the proposed chaotic systems. Section 5 gives the simulation and evaluation of the image encryption approach. Section 6 draws a conclusion.

## 2 Sine-Arcsin-Cos-Arcsin (2D-SACA) chaotic model

For users who can design chaotic systems with superior performance according to their requirements, this paper

designs a 2D-SACA chaotic model. In this chaotic model, 1D maps are utilized to derive 2D chaotic maps. The 1D seed maps adopted in this paper are specified as

$$\text{Logistic: } x_{n+1} = 4ax_n(1 - x_n), a \in [0, 1], x_n \in (0, 1) \tag{1}$$

$$\text{Sine: } x_{n+1} = a \sin(\pi x_n), a \in [0, 1], x_n \in [0, 1] \tag{2}$$

$$\text{Cubic: } x_{n+1} = ax_n(1 - x_n^2), a \in [0, 3], x_n \in (0, 1) \tag{3}$$

$$\text{Fraction: } x_{n+1} = 1/(x_n^2 + 0.1) - ax_n, a \in [0, 1], x_n \in (0, 1) \tag{4}$$

Table 1 surveys six existing 2D chaotic systems. Aiming at the shortcoming that some existing chaotic systems have narrow chaotic intervals, a novel 2D-SACA chaotic model with superior chaotic behavior and wide chaotic region is designed based on absolute value and trigonometric function. The basic framework of the 2D-SACA chaotic model is shown in Fig. 1.

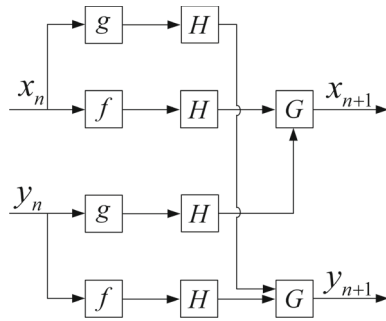
Here  $(x_n, y_n)$  denotes the input and  $(x_{n+1}, y_{n+1})$  represents the output.  $f$  and  $g$  express two existing 1D chaotic systems.  $H$  and  $G$  are the trigonometric and absolute value functions, and their mathematical expressions can be described as follows

$$H(x) = \left| \frac{100x}{\arcsin(x/2)} \right| \tag{5}$$

$$G(x, y) = |\sin x - \cos y|$$

**Table 1** Existing 2D chaotic maps

Schemes	Year	2D chaotic system name	Formula	Control parameter
Ref. [31]	2021	2D-Coupled	$\begin{cases} x_{n+1} = \sin(\alpha / \sin y_n) \\ y_{n+1} = \beta \sin(\pi(x_n + y_n)) \end{cases}$	$\alpha \neq 0, \beta \in (0, 1]$
Ref. [32]	2021	2D-LSM	$\begin{cases} x_{n+1} = \cos(4ax_n(1 - x_n) + b \sin(\pi y_n) + 1) \\ y_{n+1} = \cos(4ay_n(1 - y_n) + b \sin(\pi x_n) + 1) \end{cases}$	$a, b \in [1, 100]$
Ref. [33]	2022	2D-CLSS	$\begin{cases} x_{n+1} = \sin(\pi(py_n(1 - y_n))) \\ y_{n+1} = \sin(\pi(x_n + y_n)) \end{cases}$	$p \in [0, 4]$
Ref. [34]	2022	2D-CSCM	$\begin{cases} x_{n+1} = \cos(\alpha \cos^{-1}(\sin(x_n - y_n))) \\ y_{n+1} = \beta \sin(\pi(x_n + y_n)) \end{cases}$	$\alpha, \beta \in [2, +\infty)$
Ref. [35]	2023	2D-SICMM	$\begin{cases} x_{n+1} = \text{mod}(a \sin(\pi x_n) + b \sin(x_n) \cos(y_n), 3) \\ y_{n+1} = \text{mod}(b \sin(9/x_n) + ax_n y_n^2, 3) \end{cases}$	$a, b \in [1, 100]$
Ref. [36]	2023	2D-SICM	$\begin{cases} x_{n+1} = \alpha \sin(\pi(\sin y_n + \cos x_n)) \\ y_{n+1} = \sin(\beta / (\sin x_n + \cos y_n)) \end{cases}$	$\alpha, \beta \in [1, +\infty)$



**Fig. 1** 2D-SACA chaotic model framework

The 2D-SACA chaotic model is expressed by

$$\begin{cases} x_{n+1} = G(H(f(a, x_n)), H(g(b, y_n))) \\ y_{n+1} = G(H(f(a, y_n)), H(g(b, x_n))) \end{cases} \quad (6)$$

where  $a$  and  $b$  are chaotic parameters.

(1) Sine-Arcsin-Cos-Arcsin-Logistic-Sine (2D-SACA LS) chaotic map

To confirm the correctness of the 2D-SACA model, set the  $f$  and  $g$  of the 2D-SACA model as the Logistic and Sine maps individually. 2D-SACALS map is derived by

$$\begin{cases} x_{n+1} = \left| \sin \left| \frac{100 \times 4ax_n(1 - x_n)}{\arcsin(x_n/2)} \right| \right. \\ \quad \left. - \cos \left| \frac{100b \sin(\pi y_n)}{\arcsin(y_n/2)} \right| \right| \\ y_{n+1} = \left| \sin \left| \frac{100 \times 4ay_n(1 - y_n)}{\arcsin(y_n/2)} \right| \right. \\ \quad \left. - \cos \left| \frac{100b \sin(\pi x_n)}{\arcsin(x_n/2)} \right| \right| \end{cases} \quad (7)$$

When  $a \neq 0, b \in (-\infty, +\infty)$ , the 2D-SACA LS map is a fully chaotic state in  $x, y \in [0, 2]$ . When  $a = 0, b \in (-\infty, +\infty)$ , the 2D-SACALS map has partial chaotic in  $x, y \in [0, 1]$ . The details are illustrated in Fig. 3a.

(2) Sine-Arcsin-Cos-Arcsin-Cubic-Fraction (2D-SACACF) chaotic map

Similarly, the Cubic map and Fraction map are selected as  $f$  and  $g$  of the 2D-SACA model to generate a 2D-SACACF map. The mathematical definition of the 2D-SACACF model is

$$\begin{cases} x_{n+1} = \left| \sin \left| \frac{100ax_n(1 - x_n^2)}{\arcsin(x_n/2)} \right| \right. \\ \quad \left. - \cos \left| \frac{100(1/(y_n^2 + 0.1) - by_n)}{\arcsin(y_n/2)} \right| \right| \\ y_{n+1} = \left| \sin \left| \frac{100ay_n(1 - y_n^2)}{\arcsin(y_n/2)} \right| \right. \\ \quad \left. - \cos \left| \frac{100(1/(x_n^2 + 0.1) - bx_n)}{\arcsin(x_n/2)} \right| \right| \end{cases} \quad (8)$$

In the case of  $a \neq 0, b \in (-\infty, +\infty)$ , the 2D-SACACF map is in a fully chaotic state in  $x, y \in [0, 2]$ . When  $a = 0, b \in (-\infty, +\infty)$ , the 2D-SACACF map is a fully chaotic state in  $x, y \in [0, 1]$ , as depicted in Fig. 3g.

### 3 Chaotic performance analysis

This section aims to test the performance of the designed chaotic maps. MATLAB R2020a is used to simulate the 2D-SACALS map and the 2D-SACACF map from six aspects: bifurcation diagram, trajectory diagram, LE, SE, sensitivity, randomness tests, degree of non-periodicity and statistical complexity measure.

#### 3.1 Bifurcation diagram

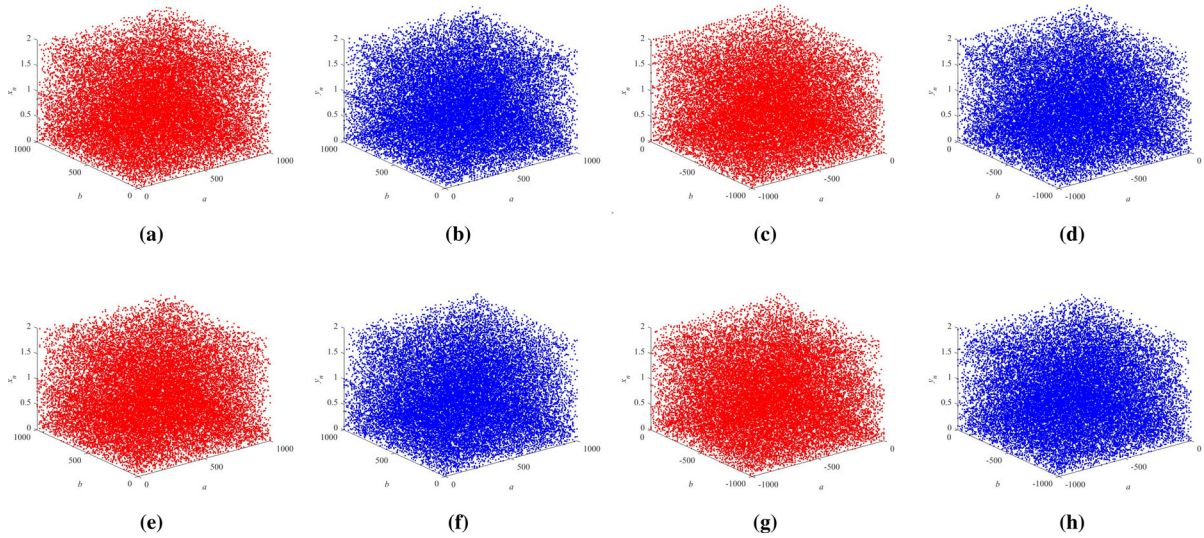
The bifurcation diagram refers to the small and continuous transformation of system parameters in a dynamic system, but it causes a qualitative alteration of the system. It can intuitively evaluate the dynamic properties of the system. A superior dynamical system requires a pseudo-random distribution of its chaotic series [37].

Figure 2 depicts the bifurcation diagrams of the 2D-SACALS map and the 2D-SACACF map with  $a, b \in [0, 1000]$  and  $a, b \in [-1000, 0]$ . In Fig. 2, within the range of chaotic parameters, no matter how the chaotic parameters transform, the 2D-SACALS map and the 2D-SACACF map are always in a fully chaotic state, proving that the 2D-SACA chaotic model has a widely chaotic region and strong randomness.

#### 3.2 Trajectory diagram

Given the initial conditions, the trajectory diagram of a 2D chaotic system intuitively reflects the motion state





**Fig. 2** Bifurcation diagrams, where red is the variable  $x$  and blue is the variable  $y$ . 2D-SACALS with **a–b**  $a, b \in [0, 1000]$  and **c–d**  $a, b \in [-1000, 0]$ . 2D-SACACF with **e–f**  $a, b \in [0, 1000]$  and **g–h**  $a, b \in [-1000, 0]$

of the system with time evolution [38]. Chaotic systems generally occupy partial phase space to indicate the uncertainty of the system output. Consequently, chaotic systems with satisfactory chaotic behavior normally occupy the trajectory of a wide phase space.

Figure 3 depicts the trajectory diagrams of the chaotic maps. It can be seen that when  $a = 0$ , the 2D-SACALS map is partially chaotic in  $[0, 1]$ , as given in Fig. 3a. However, the 2D-SACACF map is completely chaotic in  $[0, 1]$  when  $a = 0$ , as shown in Fig. 3g. When  $a \neq 0, b \in (-\infty, +\infty)$ , the trajectories generated by different initial values and parameters are all uniformly distributed in the  $[0, 2]$ , as shown in Fig. 3b–f and h–l. Trajectory diagram results demonstrate that the 2D-SACALS map and the 2D-SACACF map are completely chaotic in the chaotic range  $a \neq 0, b \in (-\infty, +\infty)$ .

### 3.3 Lyapunov exponent (LE)

The LE is responsible for deciding whether the system is chaotic. It points out that when  $LE > 0$ , the chaotic system is chaotic. Greater LE signifies more complicated chaotic behavior [39].

The LEs of the 2D chaotic system are calculated as follows

$$f(x, y) = \begin{cases} x_{i+1} = f_1(x_i, y_i) \\ y_{i+1} = f_2(x_i, y_i) \end{cases} \quad (9)$$

where  $f(x, y)$  represents a 2D chaotic system.  $J(x_i, y_i)$  is the Jacobian matrix of the  $f(x, y)$  and is calculated as follows

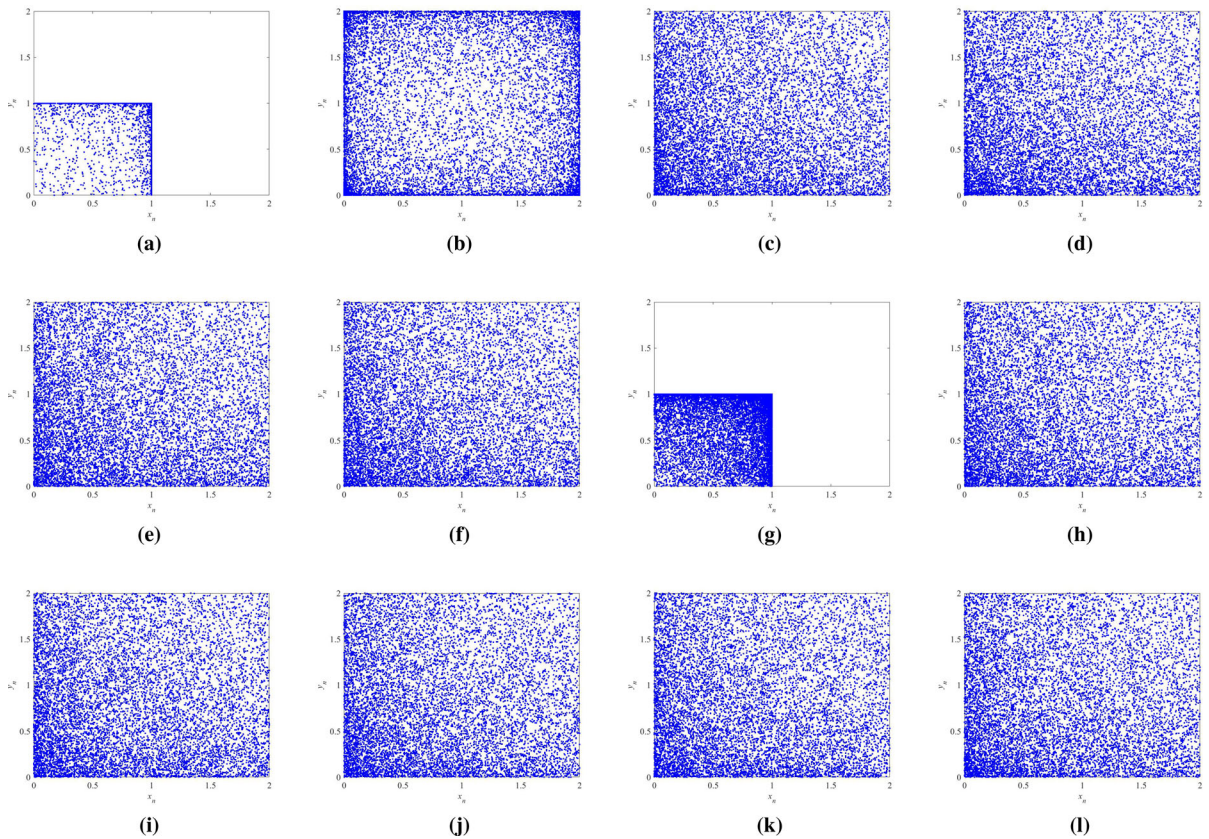
$$J(x_i, y_i) = \begin{pmatrix} \frac{\partial f_1(x,y)}{\partial x} & \frac{\partial f_1(x,y)}{\partial y} \\ \frac{\partial f_2(x,y)}{\partial x} & \frac{\partial f_2(x,y)}{\partial y} \end{pmatrix} \quad (10)$$

Suppose the eigenvalues are  $\lambda_1(J)$  and  $\lambda_2(J)$  for the 2D matrix  $J$ .

$$LE_i = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln |\lambda_i(J)| \quad (11)$$

where the maximum number of iterations is  $n$ .

The 2D-SACALS and 2D-SACACF maps have two LEs. With the initial parameters set to  $(x, y) = (0.7, 0.8)$  and control parameters to  $a, b \in [0.1, 1000]$  the calculated LEs are depicted in Fig. 4. The LEs of the 2D-SACALS map concerning parameters  $a, b \in [0.1, 1000]$  are presented in Fig. 4a and b. Similarly, LEs analyses of the 2D-SACACF map are graphed in Fig. 4d and e, separately. The outcomes indicate that the 2D-SACALS map and the 2D-SACACF map are



**Fig. 3** Trajectory diagrams. 2D-SACALS with **a** ( $x_0 = 0.2, y_0 = 0.3, a = 0, b = 8$ ), **b** ( $x_0 = 0.4, y_0 = 0.5, a = 7, b = 0$ ), **c** ( $x_0 = 0.5, y_0 = 0.6, a = -55, b = 67$ ), **d** ( $x_0 = 0.7, y_0 = 0.8, a = 76, b = 85$ ), **e** ( $x_0 = 0.43, y_0 = 0.72, a = -998, b = -785$ ) and **f** ( $x_0 = 0.89, y_0 = 0.92, a = 1735, b = 8470$ ).

2D-SACACF with **g** ( $x_0 = 0.49, y_0 = 0.52, a = 0, b = 158$ ), **h** ( $x_0 = 0.7, y_0 = 0.8, a = -281, b = 0$ ), **i** ( $x_0 = 0.45, y_0 = 0.83, a = -735, b = 467$ ), **j** ( $x_0 = 0.73, y_0 = 0.92, a = 352, b = -568$ ), **k** ( $x_0 = 0.75, y_0 = 0.23, a = -7378, b = -5786$ ) and **l** ( $x_0 = 0.32, y_0 = 0.21, a = 1789, b = 3852$ ).

positive numbers within the parameter range and have complex chaotic features.

Since the 2D-CLSS map has only one chaotic parameter, all other 2D chaotic maps except the 2D-CLSS map have two chaotic parameters. For providing a more intuitive and fair comparison, one parameter is set as a fixed value in all 2D chaotic maps except the 2D-CLSS map, and the LEs comparative analyses of all 2D chaotic maps under the other chaotic parameter are revealed in Fig. 4c and f. The LEs of the 2D-SACALS and 2D-SACACF maps are the maximum, indicating that their chaotic complexity is superior to other 2D chaotic maps.

### 3.4 Shannon entropy (SE)

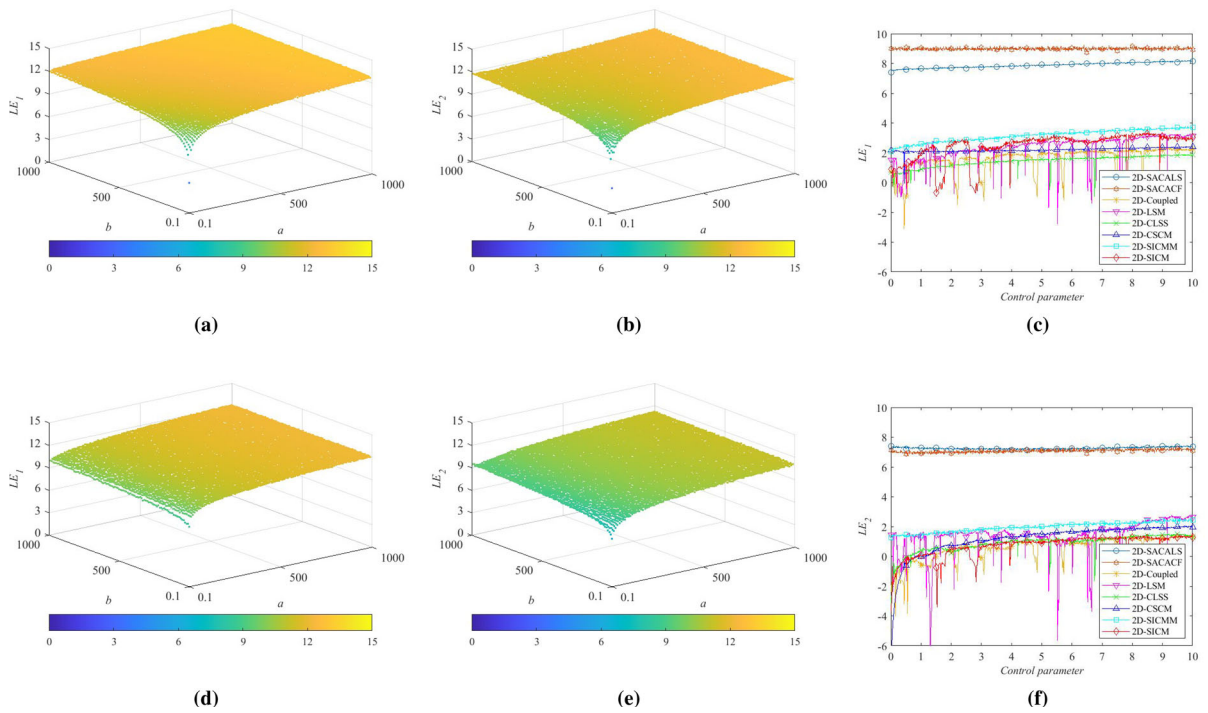
The SE reveals the complexity of time sequences [40]. As SE increases, the chaotic behavior is more complex,

and the chaotic sequence is more random. It can be calculated by

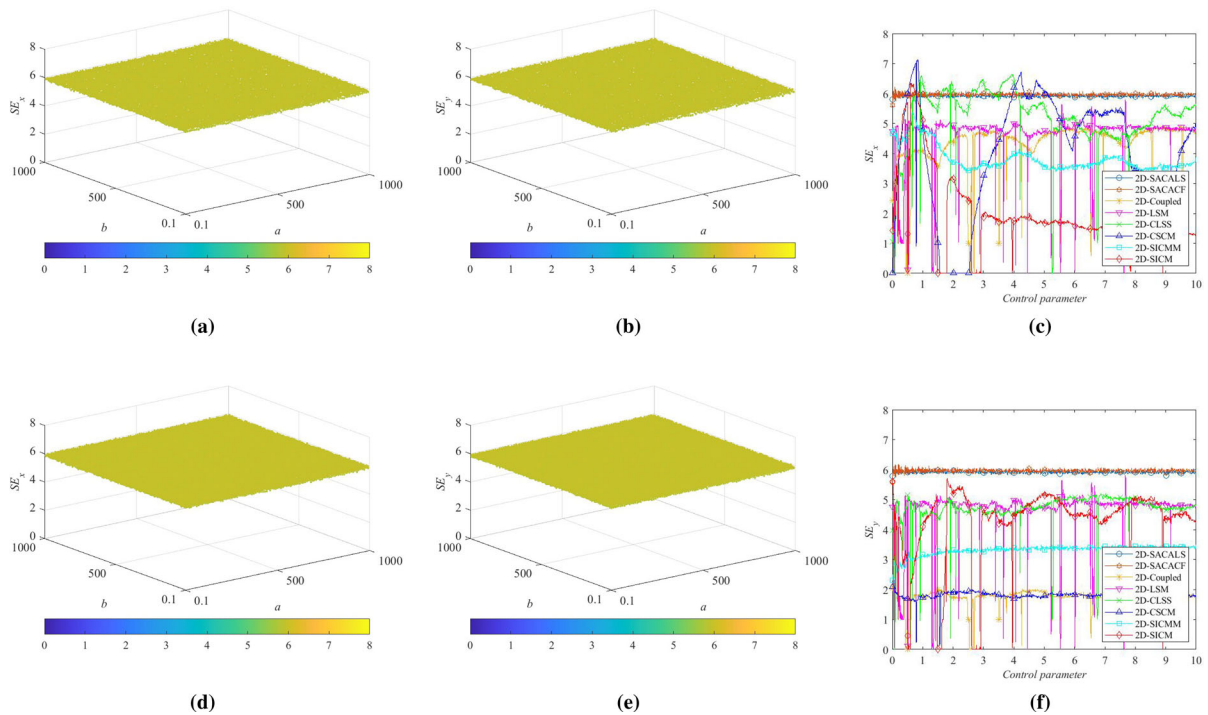
$$H(s) = \sum_{i=0}^{2^m-1} p(s_i) \log_2 \frac{1}{p(s_i)} \tag{12}$$

where  $H(s)$  is the value of SE,  $s$  is the information source and  $p(s_i)$  is the probability of the occurrence of the information  $s_i$ . For the random source with  $m$  symbols, the theoretical value of SE is equal to  $\log_2(m)$ .

Figure 5 illustrates the SE of the 2D-SACALS map and 2D-SACACF map with respect to parameters  $a$  and  $b$ , which reveals that the proposed chaotic maps have a high SE, indicating that they have a high degree of chaos and strong randomness. The comparative SEs of 2D-SACALS, 2D-SACACF, 2D-Coupled, 2D-LSM, 2D-CLSS, 2D-CSCM, 2D-SICMM and 2D-SICM are

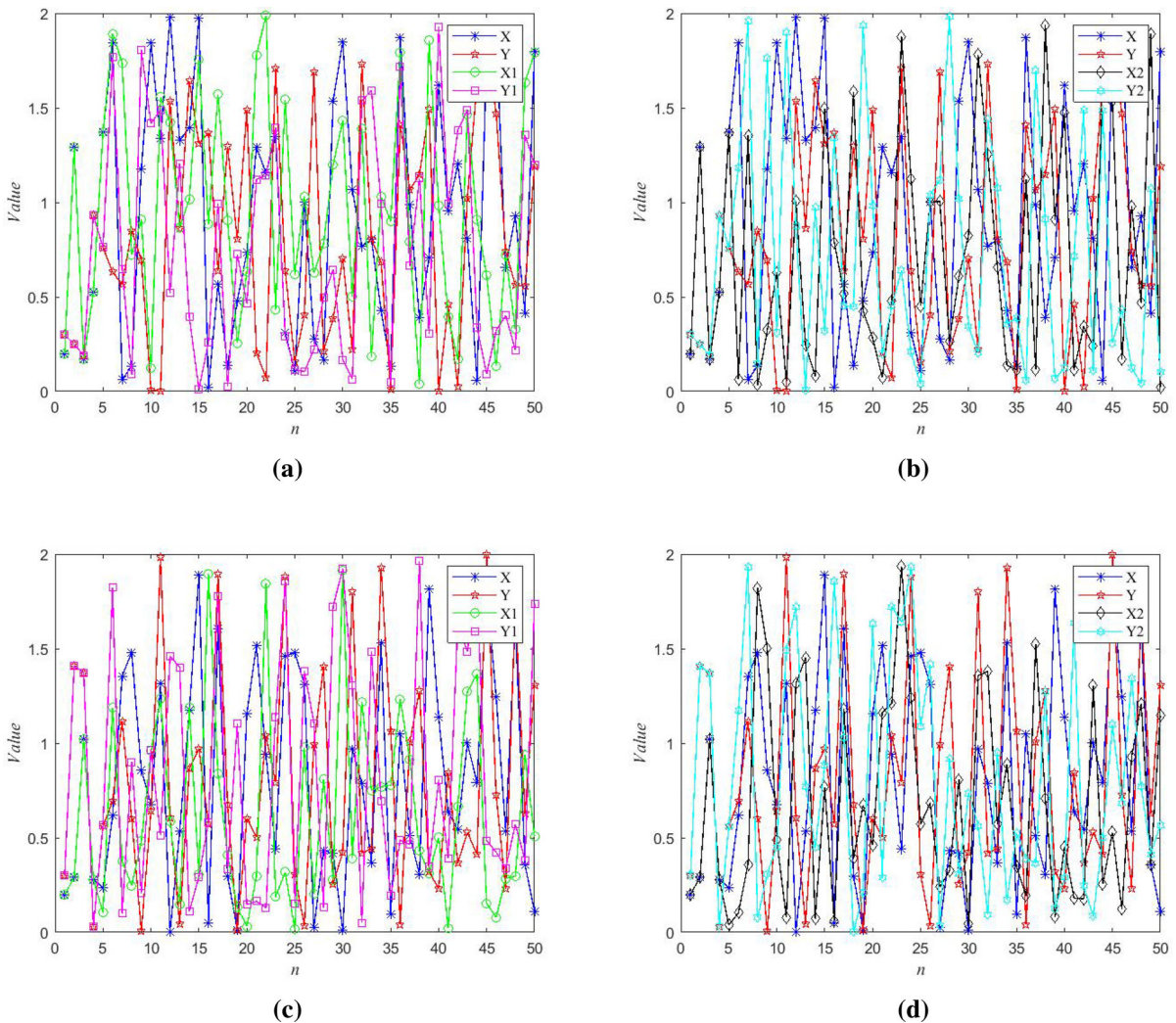


**Fig. 4** LE analysis. LE spectrum of 2D-SACALS with **a**  $LE_1$  and **b**  $LE_2$ . LE spectrum of 2D-SACACF with **d**  $LE_1$  and **e**  $LE_2$ . Comparative LEs for **c**  $LE_1$ , **f**  $LE_2$



**Fig. 5** SE analysis. SE spectrum of 2D-SACALS with **a**  $SE_x$  and **b**  $SE_y$ . SE spectrum of 2D-SACACF with **d**  $SE_x$  and **e**  $SE_y$ . Comparative SEs for **c**  $SE_x$ , **f**  $SE_y$





**Fig. 6** Sensitivity analysis. Differences with initial conditions  $(x_0, y_0, a, b)$  and  $(x_0^*, y_0^*, a, b)$  in sequences **a** 2D-SACALS, **c** 2D-SACACF. Differences with initial conditions  $(x_0, y_0, a, b)$  and  $(x_0, y_0, a^*, b^*)$  in sequences **b** 2D-SACALS, **d** 2D-SACACF

depicted in Fig. 5c and f. According to observation, the SEs of the 2D-SACALS and 2D-SACACF maps are the largest, which indicates that the proposed chaotic maps have complicated behavior and strong randomness.

### 3.5 Sensitivity analysis

An excellent chaotic system should produce different chaotic sequences when the initial values or chaotic parameters have extremely minimal variation. Using  $(x_0 = 0.2, y_0 = 0.3, a = 3, b = 5)$  to generate chaotic sequences  $(X, Y)$ ,  $(x_0^* = 0.2 + 10^{-16}, y_0^* = 0.3 + 10^{-16}, a = 3, b = 5)$  constructs sequences  $(X1, Y1)$ ,

and  $(x_0 = 0.2, y_0 = 0.3, a^* = 3 + 10^{-15}, b^* = 5 + 10^{-15})$  produces sequences  $(X2, Y2)$  to test the sensitivity of the 2D-SACALS map and the 2D-SACACF map.

Figure 6 measures the sensitive analysis of the 2D-SACALS and 2D-SACACF maps. From Fig. 6a and c, although the initial values  $(x_0, y_0)$  and  $(x_0^*, y_0^*)$  of the 2D-SACALS and 2D-SACACF maps are only different from  $10^{-16}$ , the chaotic curves generated by the two initial values are totally different. In Fig. 6b and d, when chaotic parameter values  $(a, b)$  and  $(a^*, b^*)$  of the 2D-SACALS and 2D-SACACF maps are only different from  $10^{-15}$ , the resulting chaotic sequences  $(X, Y)$  and

**Table 2** NIST test results

Sub-tests	2D-SACALS		2D-SACACF		Result: Pass (✓) / Fail (×)
	<i>P</i> -value ( <i>x</i> )	<i>P</i> -value ( <i>y</i> )	<i>P</i> -value ( <i>x</i> )	<i>P</i> -value ( <i>y</i> )	
Frequency	0.911413	0.911413	0.911413	0.964295	✓
Block frequency	0.911413	0.911413	0.834308	0.964295	✓
Cumulative sums	0.834308	0.534146	0.437274	0.637119	✓
Runs	0.534146	0.437274	0.122325	0.350485	✓
Longest run	0.991468	0.437274	0.350485	0.534146	✓
Rank	0.739918	0.739918	0.437274	0.275709	✓
FFT	0.534146	0.739918	0.437274	0.350485	✓
Non-overlapping template	0.991468	0.999438	0.991468	0.991468	✓
Overlapping template	0.213309	0.637119	0.739918	0.437274	✓
Universal	0.637119	0.350485	0.637119	0.437274	✓
Approximate entropy	0.991468	0.350485	0.637119	0.534146	✓
Random excursions	0.834308	0.739918	0.911413	0.834308	✓
Random excursions variant	0.964295	0.911413	0.991468	0.999438	✓
Serial	0.534146	0.534146	0.739918	0.350485	✓
Linear complexity	0.964295	0.534146	0.964295	0.834308	✓

( $X_2$ ,  $Y_2$ ) are completely different. Figure 6 proves that minimal modification in the initial conditions of the chaotic systems will produce novel sequences. Accordingly, the 2D-SACALS and 2D-SACACF maps are extremely sensitive to the initial conditions. When they are used in encryption algorithms, the sensitivity of algorithms to keys can be enhanced.

### 3.6 Randomness tests

To further evaluate the uncertainty of the 2D-SACALS and 2D-SACACF chaotic sequences, the National Institute of Standards and Technology (NIST) test [41] and TestU01 [42] are utilized for measuring.

The NIST test involves 15 subtests, and individual subtests will produce a probability value (*P*-value) representing the consistency of chaotic sequences. Evidence that the evaluation passes when the *P*-value is within [0.001,1] and the sequences are random [41]. This paper uses a random number as the initial value of the 2D-SACALS and 2D-SACACF maps. Then, the chaotic sequences are divided according to 1000,000 in the length of an individual group. The NIST test conclusions are enumerated in Table 2, highlighting that the 2D-SACALS and 2D-SACACF maps have strong randomness, which helps to strengthen the reliability of image cryptography.

TestU01 is a test suite for evaluating pseudo-random number generators (PRNG) and random number sequences, which includes a series of statistical tests and randomness measurements to evaluate the quality and performance of random number generators. TestU01 contains three different kinds of crush batteries, namely SmallCrush, Crush and BigCrush. For each test, if the *P*-value is within the range [ $10^{-4}$ ,  $1 - 10^{-4}$ ], the associated test is a success [42]. These test results can help to judge whether the generated random number sequence has the required randomness characteristics. The test results of TestU01 are given in Table 3. It can be seen that the *x* sequences and *y* sequences of 2D-SACALS and 2D-SACACF maps have passed the test, which proves that the generated chaotic sequences have good randomness.

### 3.7 Degree of non-periodicity

To detect and study the non-periodicity of the 2D-SACALS and 2DSACACF chaotic sequences, the scale index analysis is carried out. Since the scale index indicates a measure of the non-periodicity of the signal, it can specify which chaotic parameter values are most suitable for generating pseudo-random number sequences [43].

**Table 3** TestU01 test results

Battery	Parameters	Number of statistics	Result: Pass (✓) / Fail (×)			
			2D-SACALS		2D-SACACF	
			<i>x</i>	<i>y</i>	<i>x</i>	<i>y</i>
SmallCrush	Standard	15	✓	✓	✓	✓
Crush	Standard	144	✓	✓	✓	✓
BigCrush	Standard	160	✓	✓	✓	✓

The scale index of a time series *f* in the scale interval [*s*<sub>0</sub>, *s*<sub>1</sub>] is calculated by quotient as follows

$$i_{scale} := \frac{S(s_{min})}{S(s_{max})} \tag{13}$$

where *s*<sub>max</sub> ∈ [*s*<sub>0</sub>, *s*<sub>1</sub>] is the maximum scale of *s* ∈ [*s*<sub>0</sub>, *s*<sub>1</sub>] so that *S*(*s*) ≤ *S*(*s*<sub>max</sub>), and *s*<sub>min</sub> ∈ [*s*<sub>max</sub>, 2*s*<sub>1</sub>] is the smallest scale of *s* ∈ [*s*<sub>max</sub>, 2*s*<sub>1</sub>] such that *S*(*s*<sub>min</sub>) ≤ *S*(*s*). By its definition, the scale index *i*<sub>scale</sub> ∈ [0, 1] is close to 0 for periodic series and close to 1 for highly non-periodic series.

In Fig. 7a–d, when *b* = 5, the scale index analysis of the 2D-SACALS and 2D-SACACF maps for parameter *a* ∈ (0, 1000] are presented. By definition, for highly non-periodic signals the scale index will be close to 1. Therefore, from Fig. 7a–d, it can be concluded that the first best values (*i*<sub>scale</sub> = 1) of chaotic parameters are *a* = 20 and *b* = 5 for the *x* sequence of 2D-SACALS map, while the first extreme point (*i*<sub>scale</sub> = 1) of the *y* sequence of 2D-SACALS map is *a* = 74.1 and *b* = 5. For the 2D-SACACF map, the first optimal chaotic parameters (*i*<sub>scale</sub> = 1) of *x* and *y* sequences are *a* = 548.1, *b* = 5 and *a* = 2.1, *b* = 5, respectively. Similarly, Fig. 7e–f shows the scale index analysis of the 2D-SACALS map for parameter *b* ∈ [0, 1000] are presented when *a* = 5, and the first optimal values of chaotic parameters of the *x* sequence and *y* sequence are *a* = 5, *b* = 21.1 and *a* = 5, *b* = 91.1 respectively. While Fig. 7g–h represents the scale index analysis of the *x* and *y* sequences of the 2D-SACACF map, and the first optimal values of their chaotic parameters are *a* = 5, *b* = 149.1 and *a* = 5, *b* = 163.1 respectively. It is worth noting that in Fig. 7, the average points of scale index are all around 0.7, which proves that the 2D-SACALS and 2DSACACF maps are highly non-periodic.

### 3.8 Statistical complexity measure

Statistical complexity measures (SCM) is a method to quantify the degree of physical structure of signals. Statistical complexity can be utilized to research complex structures hidden in dynamics [44].

For the probability distribution *P* = {*p*<sub>*i*</sub>, *i* = 1, 2, . . . , *M*} of any time series, SCM can be defined as

$$C [P] = H_S [P] \cdot Q_J [P, P_e] \tag{14}$$

where *H*<sub>*S*</sub> [*P*] = *S*[*P*]/*S*<sub>max</sub>, (0 ≤ *H*<sub>*S*</sub> ≤ 1) represents the normalized shannon entropy (NSE), with *S*<sub>max</sub> = *S*[*P*<sub>*e*</sub>] = ln *M* and *S*[*P*] = -∑<sub>*i*=1</sub><sup>*M*</sup> *p*<sub>*i*</sub> ln (*p*<sub>*i*</sub>). *P*<sub>*e*</sub> = {1/*M*, . . . , 1/*M*} is the equilibrium distribution. The disequilibrium *Q*<sub>*J*</sub> is defined in terms of the Jensen-Shannon divergence and is given by

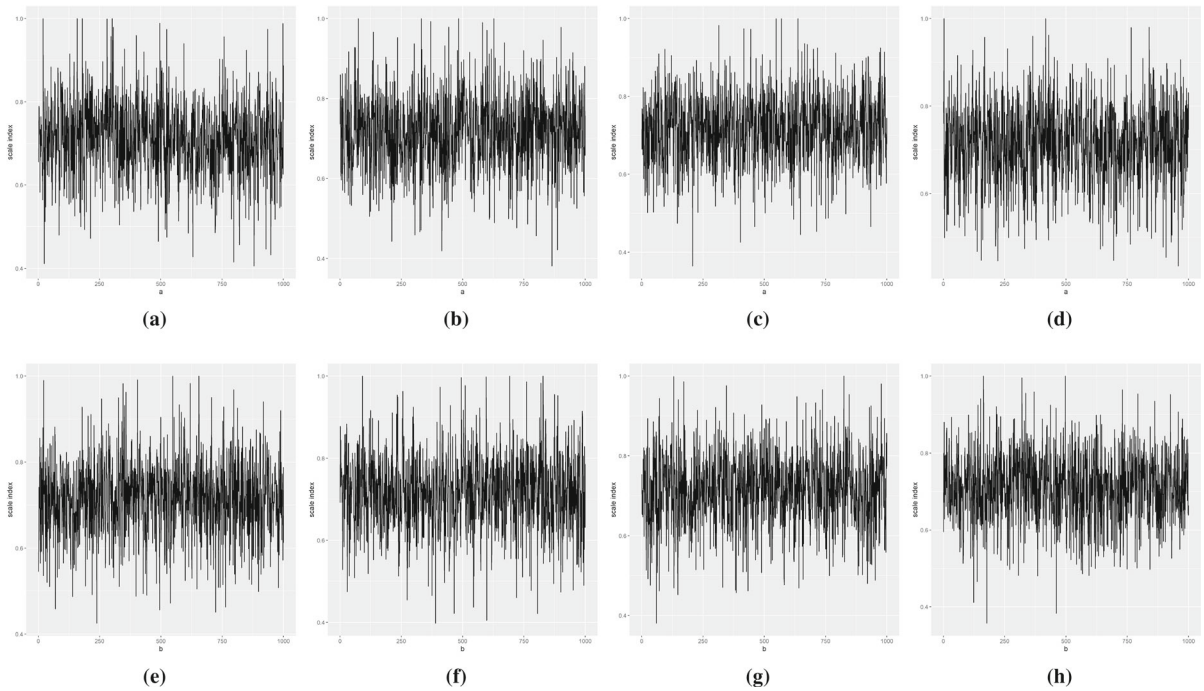
$$Q_J [P, P_e] = Q_0 \{S[(P + P_e)/2] - S[P]/2 - S[P_e]/2\} \tag{15}$$

$$Q_0 = -2\{(M + 1/M) \ln (M + 1) - 2 \ln (2M) + \ln M\}^{-1} \tag{16}$$

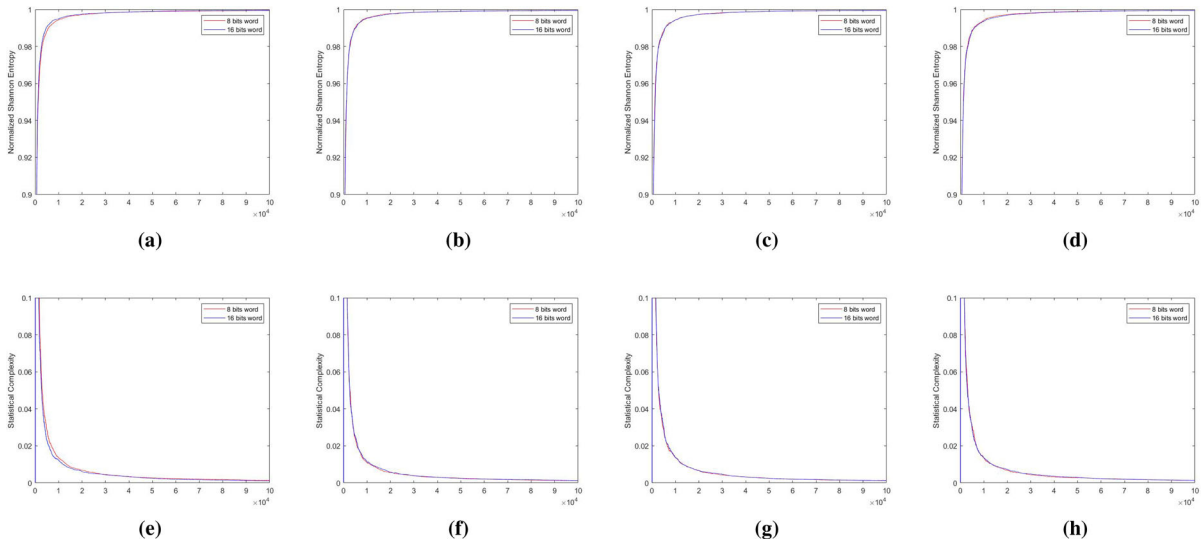
where *Q*<sub>0</sub> is a normalization constant.

Based on the above calculation, NSE and intensive statistical complexity as functions of the number of 8-bit and 16-bit words are given in Fig. 8. Figure 8a–b represent the NSE of *x* sequence and *y* sequence by 2D-SACALS map respectively, and Fig. 8c–d indicate the NSE of *x* and *y* sequences by 2D-SACACF map respectively. Similarly, Fig. 8e–h depicts the intensive complexity statistics of *x* and *y* sequences of 2D-SACALS and 2D-SACACF maps. From Fig. 8, the statistical complexity and NSE of 2D-SACALS and 2D-SACACF maps tend to be 0 and 1 respectively, regardless of the number of 8-bit words or 16-bit words, which





**Fig. 7** The scale index of 2D-SACALS map and 2D-SACACF map. **a–d**  $b = 5, a \in (0, 1000]$ , **e–h**  $a = 5, b \in [0, 1000]$



**Fig. 8** The normalized shannon entropy (NSE) and intensive statistical complexity measure of 2D-SACALS map and 2D-SACACF map. **a–d** NSE, **e–h** intensive statistical complexity measure

concluded that the statistical complexity and NSE successfully verify the randomness of the proposed chaotic maps.

#### 4 Image encryption approach

This section focuses on the preparedness and the proposed encryption scheme. Firstly, this section presents

the key generation method, then describes the encryption steps in detail, and finally the decryption stage is given. The 2D-SACALS map is applied to the image encryption scheme.

### 4.1 Generating keys

The 512-bit hash values *Hash* are calculated by SHA-512 function, and then the hash values are divided by 8 bits to obtain 64 hash value groups  $h_1, h_2, \dots, h_{63}, h_{64}$ . The SHA-512 function can be used to calculate the keys from the original image, so that different original images will generate different sub-keys. The specific operation of the SHA-512 function can be represented as

$$Hash = h_1, h_2, \dots, h_{63}, h_{64} \tag{17}$$

Then  $h_1, h_2, \dots, h_{63}, h_{64}$  are combined to get 16 hash combinations H1, H2, ..., H16, which are described as

$$\left\{ \begin{array}{l} H1 = \min(h_1, h_2, \dots, h_{15}, h_{16}) \\ H2 = \max(h_1, h_2, \dots, h_{15}, h_{16}) \\ H3 = h_1 + h_2 + \dots + h_{15} + h_{16} \\ H4 = h_1 \oplus h_2 \oplus \dots \oplus h_{15} \oplus h_{16} \\ H5 = \min(h_{17}, h_{18}, \dots, h_{31}, h_{32}) \\ H6 = \max(h_{17}, h_{18}, \dots, h_{31}, h_{32}) \\ H7 = h_{17} + h_{18} + \dots + h_{31} + h_{32} \\ H8 = h_{17} \oplus h_{18} \oplus \dots \oplus h_{31} \oplus h_{32} \\ H9 = \min(h_{33}, h_{34}, \dots, h_{47}, h_{48}) \\ H10 = \max(h_{33}, h_{34}, \dots, h_{47}, h_{48}) \\ H11 = h_{33} + h_{34} + \dots + h_{47} + h_{48} \\ H12 = h_{33} \oplus h_{34} \oplus \dots \oplus h_{47} \oplus h_{48} \\ H13 = \min(h_{49}, h_{50}, \dots, h_{63}, h_{64}) \\ H14 = \max(h_{49}, h_{50}, \dots, h_{63}, h_{64}) \\ H15 = h_{49} + h_{50} + \dots + h_{63} + h_{64} \\ H16 = h_{49} \oplus h_{50} \oplus \dots \oplus h_{63} \oplus h_{64} \end{array} \right. \tag{18}$$

The intermediate keys K1, K2, ..., K8 are calculated by H1, H2, ..., H16 and the external keys  $t_1, t_2, \dots, t_7, t_8 (t_i \in [0, 1])$ , which are described as

$$\left\{ \begin{array}{l} K1 = (t_1 \times t_3 + t_7) + \frac{1}{2 \times 512} \times \frac{H1}{H2} \\ K2 = (t_2 + t_6 \times t_7 + t_8) + t_7 \times \frac{H4}{H3} \\ K3 = (t_1 + t_3 + t_5) \times \frac{H8}{H7} \\ K4 = (t_4 \times t_7) \times \left( \frac{H5}{H6} - H5 \right) \\ K5 = (t_1 \times t_7 + t_5) - \frac{1}{2 \times 512} \times \frac{H9}{H10} \\ K6 = (t_2 \times t_3 + t_6) - \frac{1}{2 \times 512} \times \frac{H11}{H12} \\ K7 = (t_1 \times t_7 + t_2) + t_4 \times \frac{H13}{H14} \\ K8 = (t_2 \times t_3 + t_8) + \frac{1}{3 \times 512} \times \frac{H15}{H16} \end{array} \right. \tag{19}$$

Further generate keys  $(x_0, y_0, a, b, n_0)$  and  $(x_0', y_0', a', b', n_1)$  of the 2D-SACALS chaotic map by the following equation

$$\left\{ \begin{array}{l} x_0 = \text{mod}(|K1 + K2|, 1) \\ y_0 = \text{mod}(|K3 + K4|, 1) \\ a = \text{mod}\left(\left| (K1 \times K2 + K5) \times 10^{16} \right|, 10\right) \\ b = \text{mod}\left(\left| (K3 \times K4 + K6) \times 10^{16} \right|, 10\right) \\ n_0 = \text{fix}\left(\text{mod}\left(\left| (K1 + K2 + K3 + K4) \right| \times 10^{32}, 100\right) + 200\right) \\ x_0' = \text{mod}(|K5 + K6|, 1) \\ y_0' = \text{mod}(|K7 + K8|, 1) \\ a' = \text{mod}\left(\left| (K5 \times K6 + K7) \times 10^{16} \right|, 10\right) \\ b' = \text{mod}\left(\left| (K7 \times K8 + K8) \times 10^{16} \right|, 10\right) \\ n_1 = \text{fix}\left(\text{mod}\left(\left| (K5 + K6 + K7 + K8) \right| \times 10^{32}, 100\right) + 200\right) \end{array} \right. \tag{20}$$

### 4.2 Encryption scheme

The detailed encryption steps of this scheme with the 2D-SACALS map are specified as follows.

**Step 1.** Extract the pre-cryptographic image *P* with size  $N \times N$ , and calculate the keys grounded on the

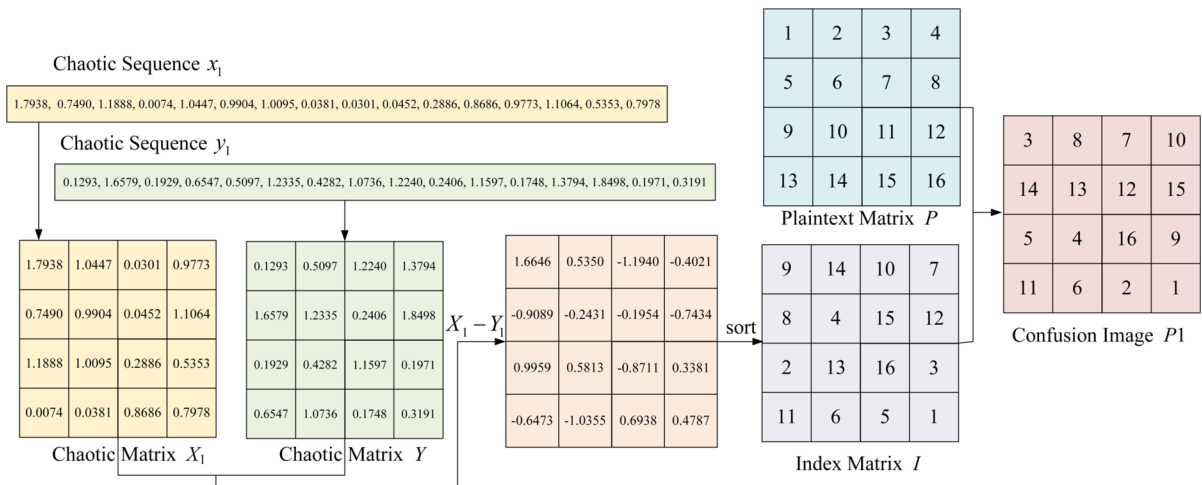


Fig. 9 Confusion process of the original 4×4 image matrix

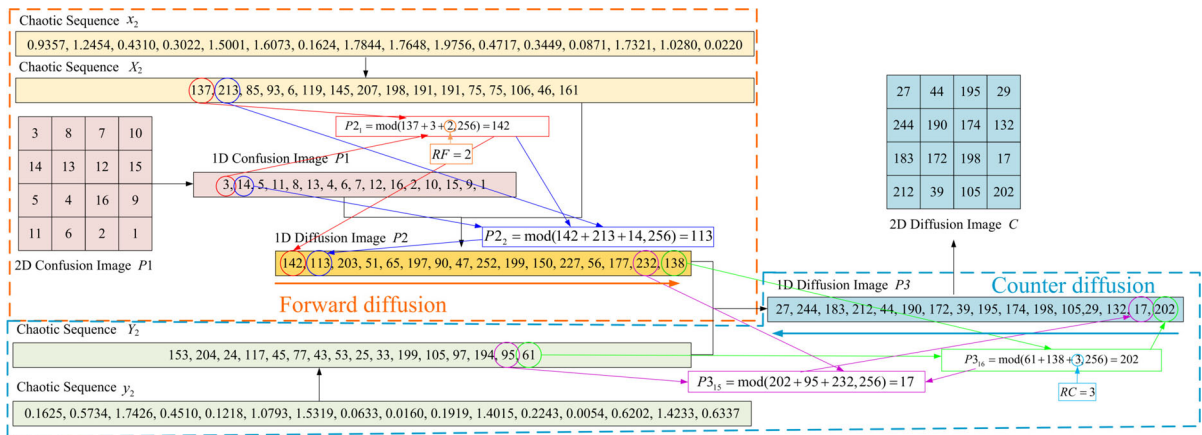


Fig. 10 Diffusion process of the original 4×4 image matrix

original image  $P$  with SHA-512 function according to Sect. 4.1.

**Step 2.** The chaotic sequences are derived by substituting the initial conditions of the 2D-SACALS map. Using  $(x_0, y_0, a, b, n_0)$  to generate the 2D-SACALS chaotic sequences  $(x_1, y_1)$  for chaotic confusion, where  $(x_0, y_0)$  are the chaotic initial values and  $(a, b)$  are the chaotic parameters. The  $(x_0, y_0, a, b, n_0)$  are substituted into the 2D-SACALS map to iterate  $N \times N + n_0$  times, and the previous  $n_0$  sequence values are deleted to eliminate transient effects. Similarly,  $(x'_0, y'_0, a', b', n_1)$  are replaced into 2D-SACALS chaotic map to iterate  $N \times N + n_1$  times, and the former  $n_1$  sequence values are dropped to derive chaotic

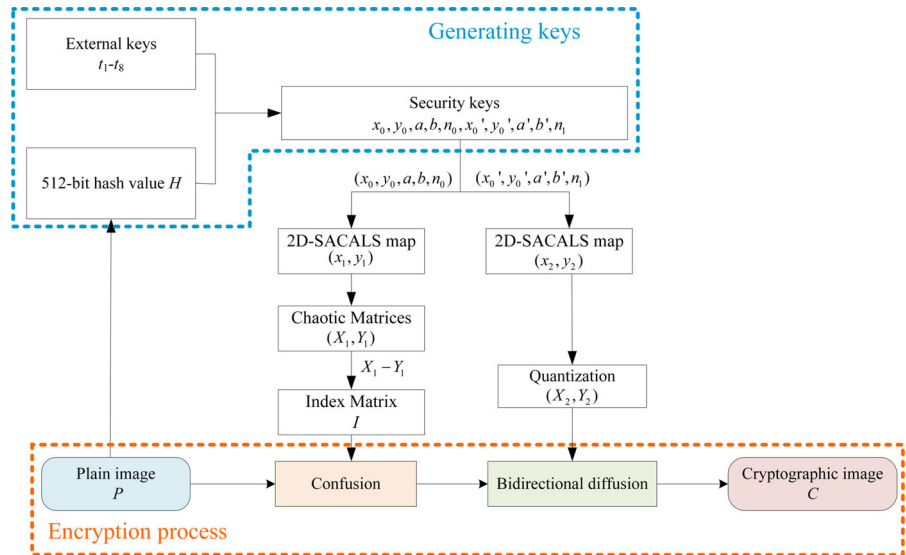
sequences  $(x_2, y_2)$ , which are applied to the diffusion stage.

**Step 3.** Confusion process. Chaotic sequences  $(x_1, y_1)$  are transformed into 2D matrices  $(X_1, Y_1)$  with dimension  $N \times N$ , and matrix  $Z = X_1 - Y_1$  is calculated. The matrix  $Z$  is sorted in ascending order to acquire an index matrix  $I$ , and the original image  $P$  is interfered with the index matrix to obtain a confusing image  $P1$ . The process is represented as

$$P1 = P(I) \tag{21}$$

The confusion process of the original 4×4 image matrix is given in Fig. 9.

**Fig. 11** Encryption flow chart of the proposed approach



**Step 4.** Bidirectional diffusion. Before the diffusion, chaotic sequences  $(x_2, y_2)$  are quantized into  $(X_2, Y_2)$ , and the confusion image  $P1$  is transformed into a 1D matrix. The quantization process is performed as

$$\begin{cases} X_2 = \text{mod}(\text{floor}(x_2 \times 10^{16}), 256) \\ Y_2 = \text{mod}(\text{floor}(y_2 \times 10^{16}), 256) \end{cases} \quad (22)$$

The arbitrary information of the plaintext image should be hidden in the entire cryptographic image, and it needs to be circulated twice, that is, forward diffusion and counter diffusion. The forward diffusion operation process is described as follows

$$P2_i = \begin{cases} \text{mod}(RF + X_{2_i} + P1_i, 256), & i = 1 \\ \text{mod}(P2_{i-1} + X_{2_i} + P1_i, 256), & i = 2, \dots, N \times N \end{cases} \quad (23)$$

where  $RF$  is a random number. Then counter diffusion is performed by Eq. (24).

$$P3_i = \begin{cases} \text{mod}(RC + Y_{2_i} + P2_i, 256), & i = N \times N \\ \text{mod}(P3_{i+1} + Y_{2_i} + P1_i, 256), & i = N \times N - 1, \dots, 1 \end{cases} \quad (24)$$

where  $RC$  is a random number.

Converting  $P3$  into a 2D matrix  $C$  is a cryptographic image. The diffusion process is disclosed in Fig. 10. The encryption procedure is illustrated in Fig. 11. The pre-cryptographic image is separated into R, G, and B channels if it is a color image with size  $N \times N \times 3$ , and the same encryption processing is implemented on these three channels to acquire a color cryptographic image.

### 4.3 Decryption scheme

Decryption procedures are presented below.

**Step 1.** Receive the cryptographic image  $C$  and the keys sent by the sender. Substitute keys  $(x_0, y_0, a, b, n_0)$  and  $(x_0', y_0', a', b', n_1)$  into the 2D-SACALS map, and generate chaotic sequences  $(x_1, y_1)$  and  $(x_2, y_2)$  respectively.

**Step 2.** Bidirectional diffusion recovery. The same quantization operation is performed on the chaotic sequences  $(x_2, y_2)$  to obtain  $(X_2, Y_2)$ , and the cryptographic image  $C$  is arranged in a 1D matrix. The recovery process of counter diffusion operation is given by

$$C1_i = \begin{cases} \text{mod}(256 \times 2 + C_i - Y_{2_i} - RC, 256), & i = N \times N \\ \text{mod}(256 \times 2 + C_i - C_{i+1} - Y_{2_i}, 256), & i = N \times N - 1, \dots, 1 \end{cases} \quad (25)$$

Then the forward diffusion recovery process is

$$C2_i = \begin{cases} \text{mod}(256 \times 2 + C2_i - X_{2_i} - RF, 256), & i = 1 \\ \text{mod}(256 \times 2 + C2_i - C2_{i-1} - X_{2_i}, 256), & i = 2, \dots, N \times N \end{cases} \quad (26)$$

Convert  $C2$  to a 2D matrix, and get the restored image after bidirectional diffusion.

**Step 3.** Reverse confusion. The same operation is performed on the chaotic sequences  $(x_1, y_1)$  to obtain  $(X_1, Y_1)$ , and the index matrix  $I$  is obtained. The inverse index matrix  $I^{-1}$  is derived from index matrix  $I$ , and the inverse confusion operation is indicated as

$$P' = C3(I^{-1}) \quad (27)$$

where  $P'$  is the decrypted image. Similarly, if a color cryptographic image is received, it is separated into R, G, and B channels, and then decryption operations are implemented.

## 5 Simulation and evaluation

The secure image encryption scheme of the proposed maps is simulated and evaluated using MATLAB R2020a. And select the images of different dimensions and categories for the encryption test. The external keys are  $t_1 = 0.9092$ ,  $t_2 = 0.1938$ ,  $t_3 = 0.4480$ ,  $t_4 = 0.6178$ ,  $t_5 = 0.5942$ ,  $t_6 = 0.6659$ ,  $t_7 = 0.2677$ , and  $t_8 = 0.4239$ . The test gray images are Tiffany ( $256 \times 256$ ), Woman ( $256 \times 256$ ), Lena ( $512 \times 512$ ), Baboon ( $512 \times 512$ ), Cameraman ( $1024 \times 1024$ ) and Room ( $1024 \times 1024$ ). The color images are Peppers ( $256 \times 256 \times 3$ ), House ( $256 \times 256 \times 3$ ), Lena ( $512 \times 512 \times 3$ ), Airplane ( $512 \times 512 \times 3$ ), Car ( $1024 \times 1024 \times 3$ ) and Lake ( $1024 \times 1024 \times 3$ ).

### 5.1 Encryption and decryption effect

Figures 12 and 13 indicate the simulation effect of this encryption scheme on gray image encryption and color image encryption respectively. The arrangement of per

set of images is original image - original image histogram - cryptographic image - cryptographic image histogram - decrypted image. In the third columns of Figs. 12 and 13, these cryptographic images in this scheme are comparable to noise images, and any features about the original images cannot be obtained. Even if the attacker obtains cryptographic images, he cannot receive any referable information, which protects the information of the image from being leaked.

### 5.2 Histogram analysis

The histogram enables visually revealing the pixel layout of an image. Typically, the histogram of images with visual significance is unevenly distributed, while the histogram of cryptographic images with noise characteristics should be uniformly distributed [4].

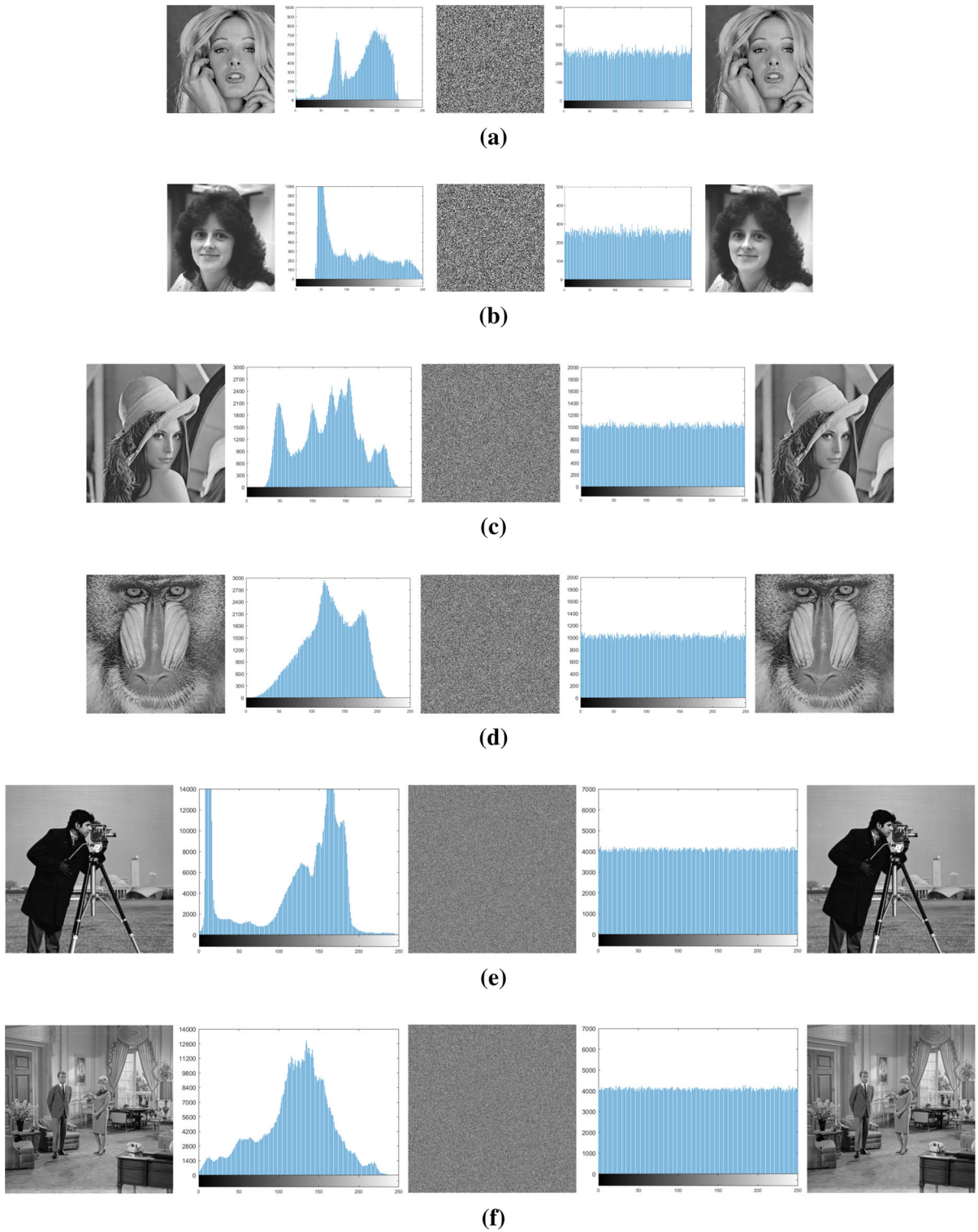
Figures 12 and 13 give the histogram analysis of gray image encryption and color image encryption by this encryption scheme respectively. The second columns of Figs. 12 and 13 are the histograms of these original images. The pixel layout of these original images is continuous and concentrated, which reflects the overwhelming majority of the information in the original images. The histogram of cryptographic images is relatively uniform and dissimilar to their original images, as depicted in the fourth columns of Figs. 12 and 13.

This encryption algorithm successfully covers up the characteristic information of the original images, and the attacker fails to acquire any available information from the histogram of cryptographic images, improving the probability of resistance to statistical attacks. By using this encryption scheme, original images with non-uniform pixel distribution become consistent after encryption, and the feature information of the original images is effectively concealed. Consequently, it is proved that this encryption approach has excellent confidentiality in protecting information and strong anti-statistical attacks.

### 5.3 Key space analysis

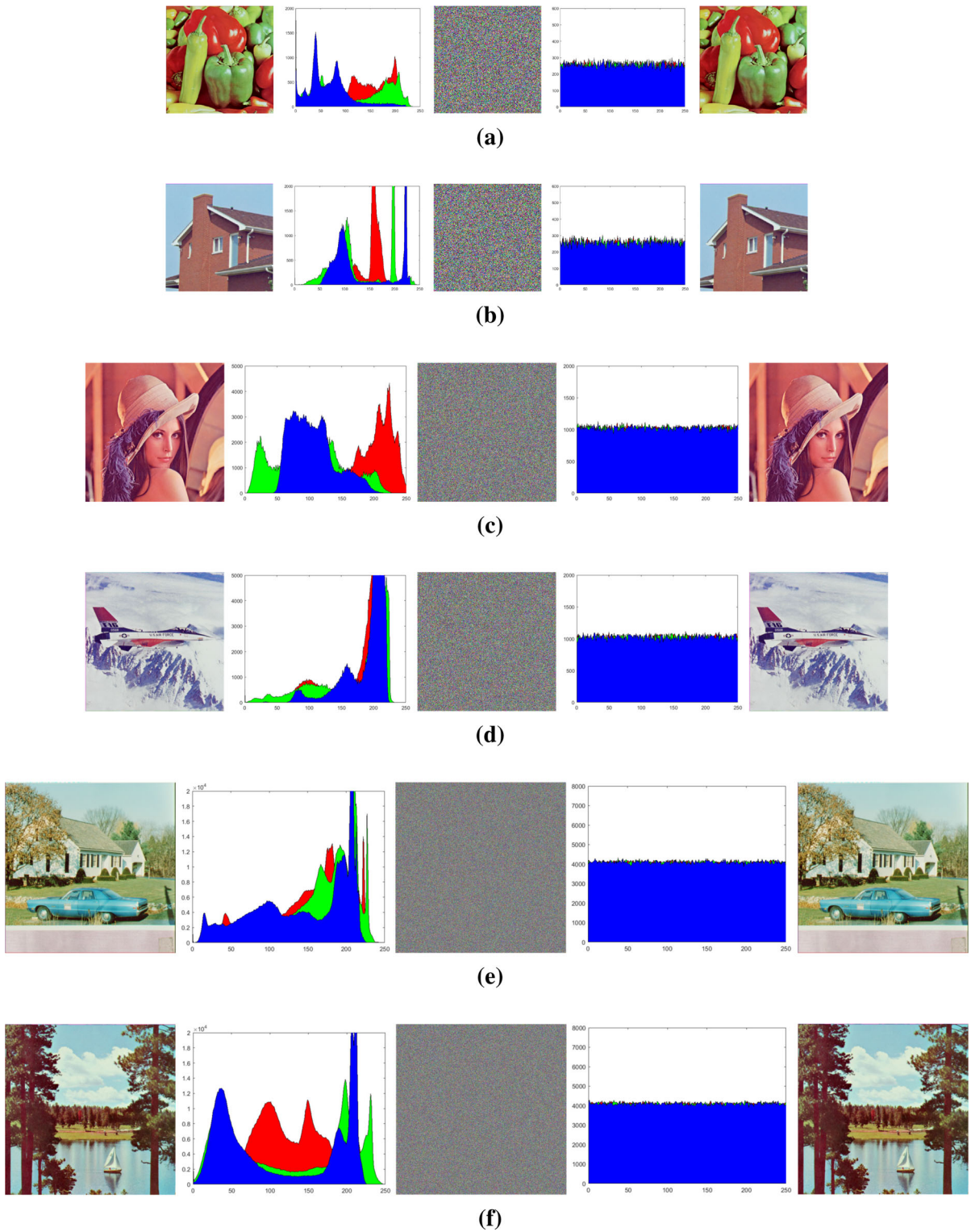
The key space indicates the sum of all key sets. With the enlargement of key space, the more selective keys are, and the enhanced effectiveness of withstanding brute force attacks. Commonly, the key space requirement is greater than  $2^{100}$  [30].





**Fig. 12** Encryption and decryption effect diagrams of gray images. The arrangement is original image - original image histogram - cryptographic image - cryptographic image histogram - decrypted image. **a** Tiffany ( $256 \times 256$ ), **b** Woman ( $256 \times 256$ ), **c** Lena ( $512 \times 512$ ), **d** Baboon ( $512 \times 512$ ), **e** Cameraman ( $1024 \times 1024$ ), **f** Room ( $1024 \times 1024$ )





**Fig. 13** Encryption and decryption effect diagrams of color images. The arrangement is original image - original image histogram - cryptographic image - cryptographic image his-

togram - decrypted image. **a** Peppers ( $256 \times 256 \times 3$ ), **b** House ( $256 \times 256 \times 3$ ), **c** Lena ( $512 \times 512 \times 3$ ), **d** Airplane ( $512 \times 512 \times 3$ ), **e** Car ( $1024 \times 1024 \times 3$ ), **f** Lake ( $1024 \times 1024 \times 3$ )

**Table 4** Key space analysis

Scheme	Key space	Scheme	Key space
Ref.[6]	$2^{209}$	Ref.[23]	$2^{512}$
Ref.[10]	$10^{64}$	Ref.[25]	$2^{186}$
Ref.[12]	$2^{128}$	Ref.[29]	$2^{240}$
Ref.[14]	$2^{260}$	Proposed	$> 2^{912}$

The keys in this scheme are  $t_1, t_2, \dots, t_7, t_8$ , and SHA-512. If the accuracy is taken as  $10^{-16}$ , the key space of eight external keys is  $10^{16 \times 8} > 10^{3 \times 40} \approx 2^{10 \times 40}$ , and the key space in the key generation stage using SHA-512 is  $2^{512}$ . Thus the total key space is  $> 2^{912} \gg 2^{100}$ , which satisfies the requirements. The comparative analysis of the key space between this scheme and previous schemes is indicated in Table 4, from which it concludes that the key space of this approach is the largest in all the comparative literature, indicating that it has the strongest immunity to brute force attacks.

#### 5.4 Correlation analysis

The correlation indicates the association between pixels in adjacent positions. The correlation of the original image is exceedingly strong and approaches 1. In contrast, the correlation of the cryptographic image obtained by the superior security cryptography system is expected to be close to 0 [29]. The correlation is computed by

$$r_{PC} = \frac{\frac{1}{N} \sum_{i=1}^N (P_i - E(P))(C_i - E(C))}{\sqrt{\left(\frac{1}{N} \sum_{i=1}^N (P_i - E(P))^2\right) \left(\frac{1}{N} \sum_{i=1}^N (C_i - E(C))^2\right)}} \quad (28)$$

where  $E(P) = \frac{1}{N} \sum_{i=1}^N P_i$  and  $E(C) = \frac{1}{N} \sum_{i=1}^N C_i$ .

Table 5 enumerates the correlation analysis results of this encryption scheme. By comparing the original images, the correlation of cryptographic images is approaching 0, which verifies that the above security theoretical scheme has an excellent encryption effect. Figure 14 illustrates the correlation between the original images and cryptographic images of Lena

(512×512) in three directions. It is known that all components of original images have intense correlation, while the components of cryptographic images are evenly distributed and have low correlation, which implies that the proposed approach enables invalid statistical attacks.

#### 5.5 Information entropy analysis

Information entropy provides a criterion for uncertain features of images. Larger information entropy indicates a higher degree of information uncertainty in digital images. An effective encryption algorithm demands that the information entropy of the cryptographic image is approaching 8 [45]. Information entropy expression is evaluated as

$$H = - \sum_{i=1}^{N \times N} P(m_i) \log_2 P(m_i) \quad (29)$$

where  $P(m_i)$  is the probability of pixel  $m_i$ .

Table 6 tabulates the results of information entropy analysis. These data conclude that all cryptographic images in this scheme approach to 8, proving that the pixel layout of these cryptographic images is more uniform and random than that of the original images, and it is less likely to reveal information during encryption.

#### 5.6 Differential attack analysis

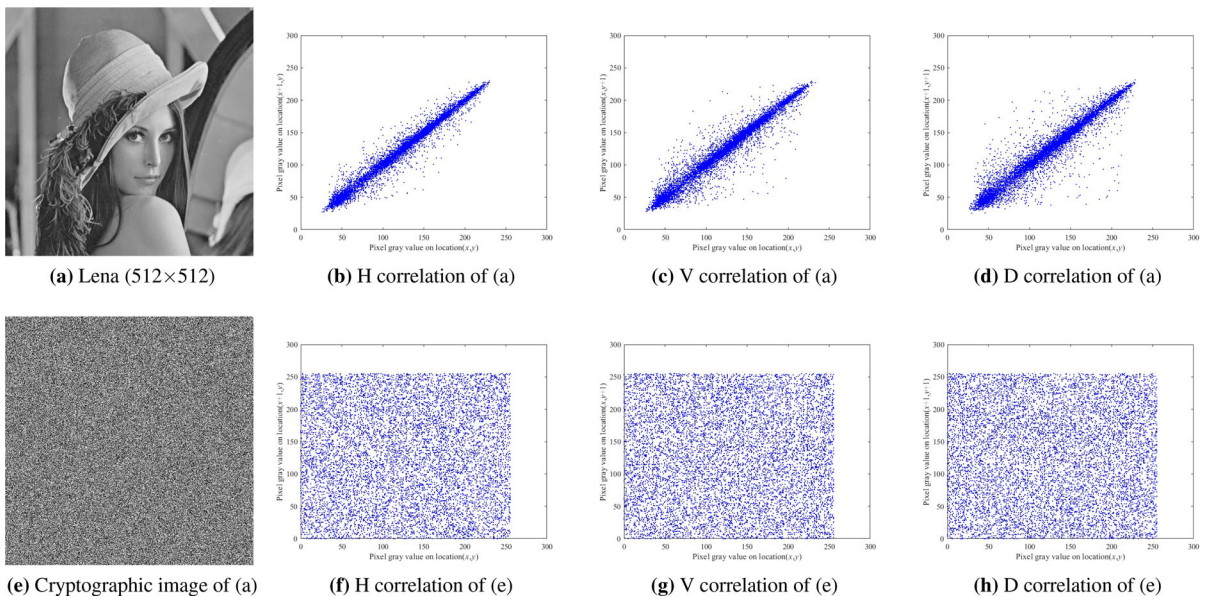
The cryptography system has to be exceedingly sensitive to slight variations in plaintext information to withstand differential cryptanalysis. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are introduced to assess the sensitivity of the cryptography system to plaintext information [46]. Given two plaintext images  $P_1$  and  $P_2$ , which are only slightly modified, the cryptographic images  $C_1$  and  $C_2$  are acquired by encrypting the two plaintexts with the same encryption algorithm. Then NPCR and UACI are evaluated as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times N} \times 100\% \quad (30)$$

$$UACI = \frac{1}{N \times N} \left[ \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \quad (31)$$

**Table 5** Correlation analysis

Images			Horizontal (H)	Vertical (V)	Diagonal (D)		
Original images	Gray images	Tiffany (256×256)	0.9189	0.9558	0.8861		
		Woman (256×256)	0.9893	0.9887	0.9798		
		Lena (512×512)	0.9680	0.9841	0.9565		
		Baboon (512×512)	0.9322	0.9088	0.863		
		Cameraman (1024×1024)	0.9955	0.9966	0.9919		
		Room (1024×1024)	0.9856	0.9871	0.9742		
		Peppers (256×256×3)	0.9713	0.9770	0.9494		
	Color images	House (256×256×3)	0.9756	0.9495	0.9368		
		Lena (512×512×3)	0.9614	0.9821	0.9452		
		Airplane (512×512×3)	0.9576	0.9533	0.9203		
		Car (1024×1024×3)	0.9376	0.9348	0.8849		
		Lake (1024×1024×3)	0.9556	0.9563	0.9265		
		Cryptographic images	Gray images	Tiffany (256×256)	-0.0004	0.0010	-0.0005
				Woman (256×256)	-0.0001	0.0006	0.0003
Lena (512×512)	-0.0003			0.0008	0.0009		
Baboon (512×512)	-0.0004			-0.0009	-0.0008		
Cameraman (1024×1024)	0.0006			-0.0007	-0.0001		
Room (1024×1024)	-0.0001			0.0001	-0.0001		
Peppers (256×256×3)	0.0003			-0.0002	-0.0006		
Color images	House (256×256×3)		-0.0003	0.0001	-0.0007		
	Lena (512×512×3)		0.0000	0.0002	0.0008		
	Airplane (512×512×3)		0.0006	0.0010	0.0000		
	Car (1024×1024×3)		0.0002	0.0004	-0.0001		
	Lake (1024×1024×3)		0.0005	-0.0010	-0.0005		



**Fig. 14** Correlation analysis. **b–d** original image, **f–h** cryptographic image

**Table 6** Information entropy analysis

Images		Original images	Cryptographic images
Gray images	Tiffany (256×256)	7.1416	7.9973
	Woman (256×256)	7.2684	7.9970
	Lena (512×512)	7.4451	7.9993
	Baboon (512×512)	7.2925	7.9993
	Cameraman (1024×1024)	7.0539	7.9998
	Room (1024×1024)	7.4314	7.9998
Color images	Peppers (256×256×3)	7.7028	7.9991
	House (256×256×3)	7.0686	7.9989
	Lena (512×512×3)	7.7329	7.9998
	Airplane (512×512×3)	6.6787	7.9998
	Car (1024×1024×3)	7.4794	7.9999
	Lake (1024×1024×3)	7.7391	7.9999

**Table 7** NPCR and UACI analysis

Images		NPCR (%)	UACI (%)
Gray images	Tiffany (256×256)	99.6124	33.4636
	Woman (256×256)	99.6109	33.4624
	Lena (512×512)	99.6105	33.4642
	Baboon (512×512)	99.6098	33.4632
	Cameraman (1024×1024)	99.6097	33.4638
	Room (1024×1024)	99.6104	33.4638
Color images	Peppers (256×256×3)	99.6109	33.4637
	House (256×256×3)	99.6109	33.4639
	Lena (512×512×3)	99.6098	33.4653
	Airplane (512×512×3)	99.6105	33.4632
	Car (1024×1024×3)	99.6098	33.4632
	Lake (1024×1024×3)	99.6096	33.4639

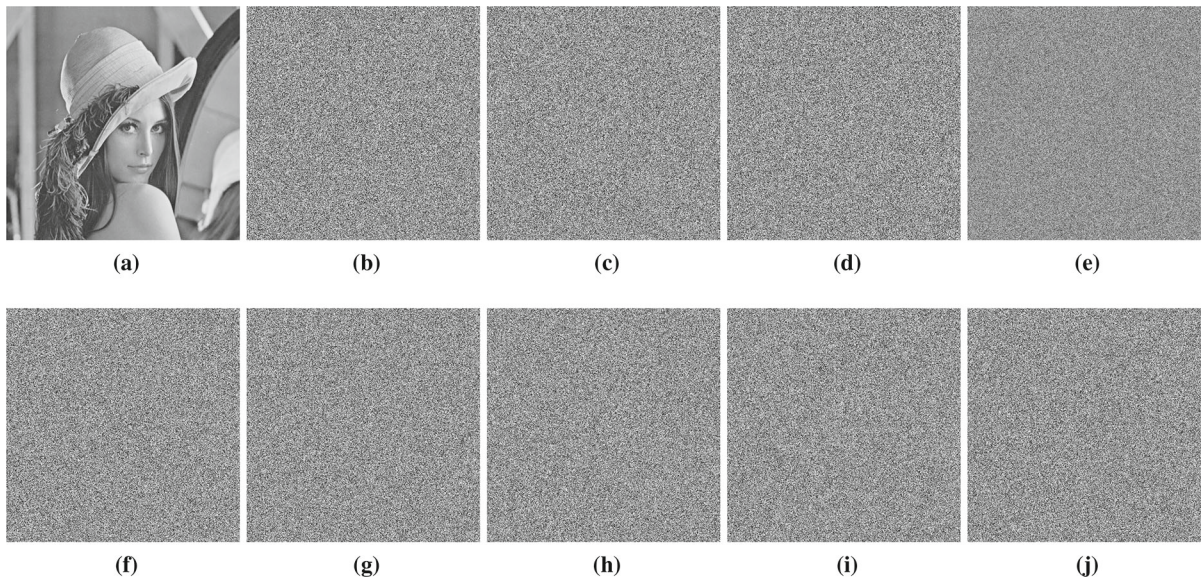
If  $C_1(i, j) \neq C_2(i, j)$ , then  $D(i, j) = 1$ , otherwise  $D(i, j) = 0$ .

The ideal values of NPCR and UACI are 99.6094% and 33.4635% individually. The closer to the ideal values, the more sensitive the encryption algorithm is, and the stronger the capability to withstand differential cryptanalysis [47]. The analysis of NPCR and UACI is disclosed in Table 7. The NPCR and UACI of the proposed algorithm are approaching perfect values in Table 7, which is sufficient to effectively avoid differential cryptanalysis.

### 5.7 Key sensitivity analysis

An ideal multimedia encryption scheme requirements are extremely sensitive to key changes, and even if one bit of the key changes, the encryption or decryption results should be completely different [48]. We use a decryption scheme to verify the sensitivity of the key, that is, the slight modification in the decryption key will make the decryption fail, and the correct original image cannot be obtained. The key sensitivity of this approach is verified with Lena (512×512) as the original image.





**Fig. 15** Key sensitivity analysis. Decryption with **a** Correct key, **b**  $T_1 = t_1 + 10^{-16}$ , **c**  $T_2 = t_2 + 10^{-16}$ , **d**  $T_3 = t_3 + 10^{-16}$ , **e**  $T_4 = t_4 + 10^{-16}$ , **f**  $T_5 = t_5 + 10^{-16}$ , **g**  $T_6 = t_6 + 10^{-16}$ , **h**  $T_7 = t_7 + 10^{-16}$ , **i**  $T_8 = t_8 + 10^{-16}$  and **j**  $Hash + 1$

Firstly, the Lena cryptographic image is decrypted with the correct decryption keys  $t_1, t_2, \dots, t_7, t_8$  ( $t_i \in [0, 1]$ ),  $Hash$ , and the correct decryption image can be obtained, as depicted in Fig. 15a. Then the decryption key  $t_1$  is modified to  $T_1 = t_1 + 10^{-16}$ , and the remaining decryption keys are consistent with the correct decryption keys to decrypt the cryptographic image. The decryption result is Fig. 15b, indicating that even if only one external key is different from the correct decryption key, the decryption image will be significantly different from the original image. Similarly, only one external key is fine-tuned and other decryption keys are kept unchanged for decryption verification each time, and the decryption images are still obviously different. The decryption images are given in Fig. 15c–i. Finally, keep the external keys  $t_1, t_2, \dots, t_7, t_8$ , ( $t_i \in [0, 1]$ ) consistent with the correct decryption keys, and change  $Hash$  to  $Hash + 1$  for decryption. The decryption result is present in Fig. 15j, and the correct original images cannot be obtained.

In the simulation experiment of Fig. 15, the original images can be successfully decrypted only by utilizing the correct decryption keys, but when the decryption key changes vary extremely slightly, the decryption of the cryptographic image fails. Through the analysis of NPCR after minor changes in the decryption keys, as given in Table 8. It is found that all NPCRs are above

**Table 8** NPCR with a slightly changed decryption keys

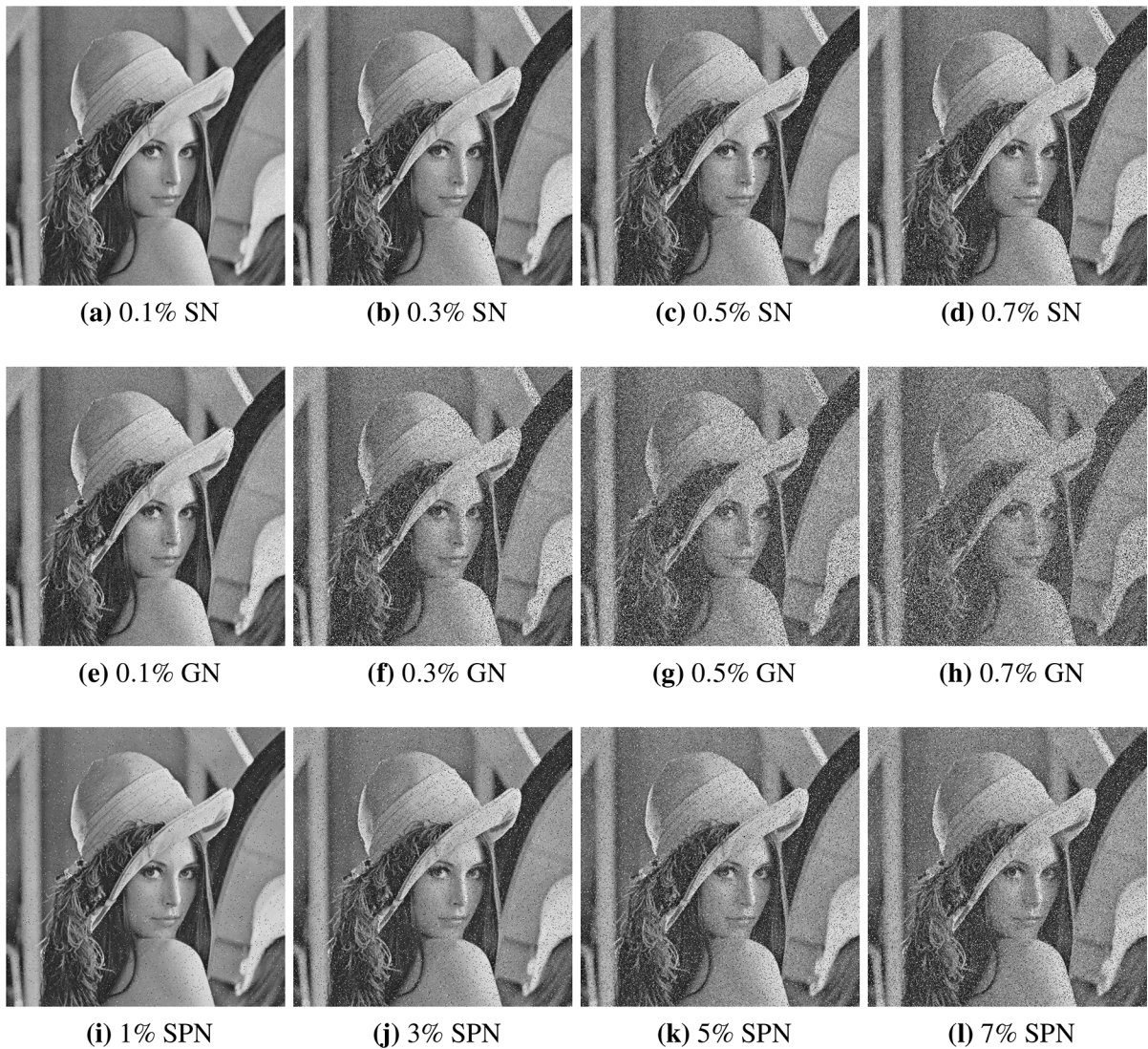
Decryption keys	NPCR (%)
Correct key	0
$T_1 = t_1 + 10^{-16}$	99.6342
$T_2 = t_2 + 10^{-16}$	99.5972
$T_3 = t_3 + 10^{-16}$	99.6078
$T_4 = t_4 + 10^{-16}$	99.3580
$T_5 = t_5 + 10^{-16}$	99.6140
$T_6 = t_6 + 10^{-16}$	99.6078
$T_7 = t_7 + 10^{-16}$	99.5975
$T_8 = t_8 + 10^{-16}$	99.6014
$Hash + 1$	99.6239

99%. This means that under the incorrect decryption key, the decryption image is completely dissimilar to the original image, revealing that the result of changing the decryption keys to a small extent has changed remarkably in the decryption image. Consequently, the proposed scheme is extremely sensitive to the key.

### 5.8 Noise attack analysis

During communication, the cryptographic image is occasionally subject to different types of noise pol-





**Fig. 16** Decryption images under different types and levels of noise attack. **a–d** SN, **e–h** GN, **i–l** SPN

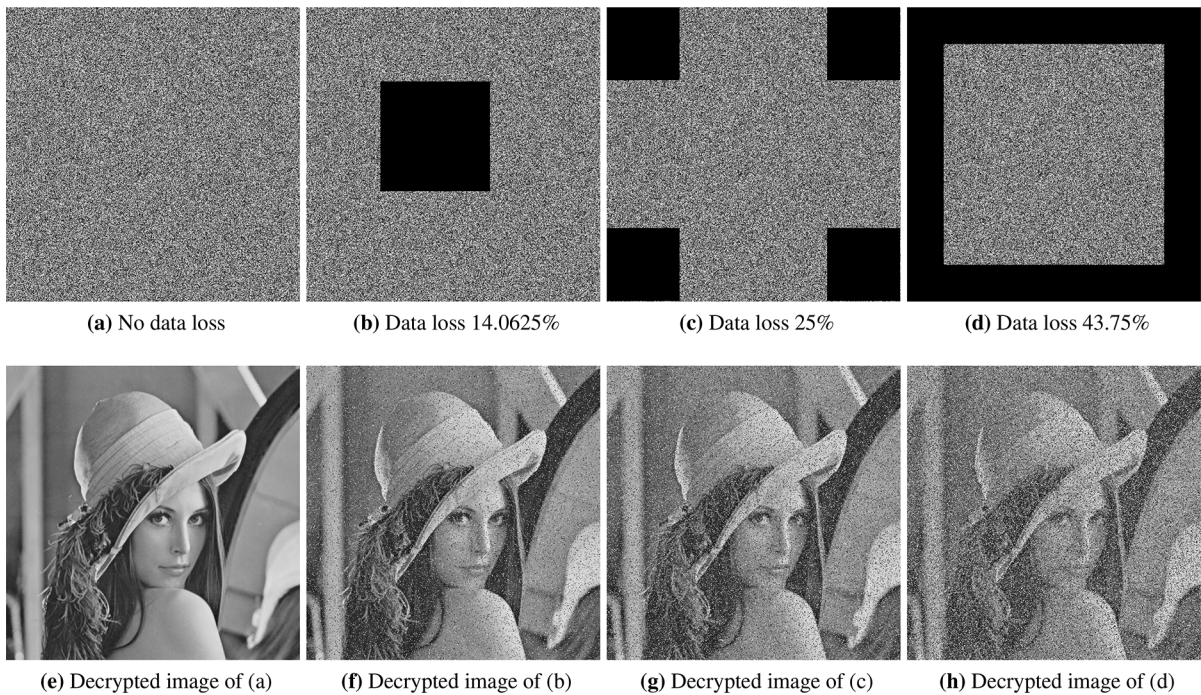
lution. The cryptographic image may not be able to restore the original image after being polluted by noise. Therefore, an illustrious encryption solution must be able to against the attack of noise pollution [49].

Figure 16 exhibits the decryption images of this algorithm under different types and levels of noise to demonstrate the noise immunity of this proposed approach. In Fig. 16, when different levels of Speckle Noise (SN), Gaussian Noise (GN), and Salt and Pepper Noise (SPN) are applied to the cryptographic image, the massive features of the initial image are recoverable, although the cryptographic image is polluted by noise to different degrees.

### 5.9 Cropping attack analysis

The transmitted cryptographic images will be impacted by data loss during communication. An effective encryption algorithm allows for resisting these influences. The correct original features are reconstructed even if the cryptographic image is disturbed by these factors [49].





**Fig. 17** Cropping attacks with different degrees. **a–d** cryptographic images, **e–h** decrypted images

The anti-cropping performance of the algorithm is tested for different degrees of cropping attacks. The test results against cropping attacks are given in Fig. 17, and the more data is discarded in the cryptographic image, the more unclear the recovered image becomes. Though different degrees of cropping, the restored image is always able to be clearly identified visually because it preserves the majority of features of the original image.

#### 5.10 Time efficiency analysis

A superior image encryption approach requires real-time communication while guaranteeing excellent security and efficiency [50]. The time-consuming evaluation of this scheme is provided in Table 9. The time-consuming comparison between the proposed approach and other encryption schemes for different sizes and category images is detailed in Table 10. It can be found that the proposed schemes have spent a

short time in encryption and decryption, indicating the high efficiency of the scheme.

#### 5.11 Computational complexity analysis

Computational complexity analysis is an essential criterion to estimate the efficiency of the algorithm. In the proposed encryption scheme, the encrypted image with  $N \times N$  size mainly includes two time-consuming parts: chaotic sequence generation and bidirectional diffusion. In the stage of generating chaotic sequences, two chaotic sequences are obtained by the SACALS map, and the maximum iteration length is  $\max(N \times N + n_0, N \times N + n_1)$ , so the complexity of this stage is  $O(\max(N \times N + n_0, N \times N + n_1))$ . The bidirectional DNA diffusion stage includes forward and counter diffusion and its complexity is  $O(N \times N)$ . So the complexity of the proposed scheme is  $O(\max(N \times N + n_0, N \times N + n_1))$ . In conclusion, the computational complexity of our scheme depends on the number of iterations of the chaotic system.

**Table 9** Time efficiency analysis

Images		Encryption (s)	Decryption (s)	Total (s)
Gray images	Tiffany (256×256)	0.003341	0.003067	0.006408
	Woman (256×256)	0.003359	0.003259	0.006618
	Lena (512×512)	0.014390	0.013964	0.028354
	Baboon (512×512)	0.014317	0.013785	0.028102
	Cameraman (1024×1024)	0.059442	0.059663	0.119105
	Room (1024×1024)	0.059394	0.059815	0.119209
Color images	Peppers (256×256×3)	0.012002	0.011522	0.023524
	House (256×256×3)	0.012032	0.010930	0.022962
	Lena (512×512×3)	0.051991	0.049961	0.101952
	Airplane (512×512×3)	0.052330	0.047522	0.099852
	Car (1024×1024×3)	0.215374	0.203884	0.419258
Average	Lake (1024×1024×3)	0.214917	0.213816	0.428733
	256×256	0.003350	0.003163	0.006513
	512×512	0.014354	0.013875	0.028228
	1024×1024	0.059418	0.059739	0.119157
	256×256×3	0.012017	0.011226	0.023243
	512×512×3	0.052161	0.048742	0.100902
	1024×1024×3	0.215146	0.208850	0.423996

**Table 10** Time comparative analysis

Image size		Ref.[7]	Ref.[21]	Ref.[22]	Ref.[23]	Ref.[36]	Ref.[24]	Ref.[35]	Proposed
256×256	Encryption (s)	0.004500	0.060600	0.077900	–	–	–	–	0.003350
	Decryption (s)	0.004400	–	–	–	–	–	–	0.003163
512×512	Encryption (s)	0.019700	0.251300	0.326100	–	–	–	–	0.014354
	Decryption (s)	0.019300	–	–	–	–	–	–	0.013875
1024×1024	Encryption (s)	0.086800	1.013500	1.314600	–	–	–	–	0.059418
	Decryption (s)	0.091700	–	–	–	–	–	–	0.059739
256×256×3	Encryption (s)	–	–	–	0.385700	0.337324	0.125300	0.062800	0.012017
	Decryption (s)	–	–	–	0.244300	0.326756	–	–	0.011226
512×512×3	Encryption (s)	–	–	–	1.211400	1.332898	0.510100	0.207800	0.052161
	Decryption (s)	–	–	–	0.738700	1.308241	–	–	0.048742
1024×1024×3	Encryption (s)	–	–	–	–	–	2.380200	0.672800	0.215146
	Decryption (s)	–	–	–	–	–	–	–	0.208850

## 5.12 Comparative analysis

The performance comparison analysis of the proposed approach and other approaches are summarized in Tables 11 and 12. Among them, Table 11 compares the performance of the Lena gray cryptographic image (512×512), and Table 12 presents the compar-

ative analysis of the Lena color cryptographic image (512×512×3).

In the comparative outcome of information entropy, the proposed approach is the largest for gray cryptographic images, which is 7.9993. For the R and B components of color cryptographic images, the proposed approach is the largest and approaches the ideal value,

**Table 11** Performance comparison analysis on Lena gray cryptographic image (512×512)

Scheme	Information entropy	Correlation			NPCR (%)	UACI (%)
		H	V	D		
Ref.[4]	7.9991	0.0018	0.0011	0.0008	99.6813	33.4852
Ref.[5]	7.9965	0.0029	0.0080	-0.0003	99.6170	33.3918
Ref.[7]	7.9993	-0.0014	0.0001	0.0003	99.6056	33.4608
Ref.[12]	7.9988	0.0013	0.0025	0.0011	99.4830	33.4166
Ref.[13]	7.9992	0.0007	0.0017	0.0008	99.6289	33.5420
Ref.[14]	7.9993	0.0065	0.0051	-0.0005	99.6130	33.4540
Ref.[29]	7.9025	-0.0006	0.0010	-0.0012	99.6098	33.4544
Ref.[33]	7.9914	-0.0016	0.0003	0.0006	99.6060	33.4689
Proposed	7.9993	-0.0003	0.0008	0.0009	99.6105	33.4642

**Table 12** Performance comparison analysis on Lena color cryptographic image (512×512×3)

Scheme		Ref.[6]	Ref.[10]	Ref.[11]	Ref.[23]	Ref.[25]	Ref.[30]	Proposed	
Information entropy	R	7.9993	7.9980	7.9993	7.9993	7.9917	7.9992	7.9993	
	G	7.9992	7.9979	7.9994	7.9995	7.9912	7.9999	7.9992	
	B	7.9993	7.9978	7.9993	7.9993	7.9918	7.9992	7.9993	
Correlation	H	R	0.0011	0.0092	-0.0048	-0.0040	0.0014	-0.0061	-0.0007
		G	-0.0056	0.0002	0.0016	0.0074	0.0033	-0.0040	-0.0001
		B	-0.0008	0.0076	0.0022	-0.0002	0.0021	-0.0018	-0.0005
	V	R	0.0004	0.0203	0.0031	0.0015	0.0048	0.0042	0.0001
		G	0.0005	-0.0025	0.0002	0.0016	-0.0006	-0.0003	0.0009
		B	-0.0047	0.0006	0.0006	-0.0041	0.0002	-0.0013	0.0000
	D	R	0.0020	-0.0073	-0.0029	0.0025	0.0002	-0.0007	0.0007
		G	0.0004	-0.0131	0.0002	-0.0024	0.0048	-0.0045	-0.0003
		B	0.0001	0.0111	-0.0039	0.0011	-0.0040	-0.0032	-0.0003
NPCR (%)	R	99.6058	99.6531	99.6094	99.6002	99.6243	99.6000	99.6098	
	G	99.6096	99.6522	99.6055	99.6059	99.6185	99.5900	99.6098	
	B	99.6105	99.6518	99.6122	99.6121	99.6281	99.6100	99.6098	
UACI (%)	R	33.4562	33.4572	33.4511	33.4550	33.4224	33.4700	33.4378	
	G	33.4783	33.4715	33.4850	33.5295	33.4362	33.4200	33.4947	
	B	33.4560	33.4384	33.5177	33.5006	33.4604	33.4600	33.4634	

while the G component is lower than [11, 23], and [30], indicating the high degree of information uncertainty of cryptographic images in this paper. For correlation coefficient analysis, compared with other encryption schemes, the correlation coefficient of our encryption scheme is approaching 0 whether it is a gray cryptographic image or a color cryptographic image. Like correlation coefficient analysis, by comparing the results of previous methods for NPCR and UACI analysis, these data revealed that the NPCR and UACI of the

proposed approach are approaching the perfect values, which can prevent the attack of differential cryptanalysis more effectively. From Tables 11 and 12, the information entropy, correlation analysis, NPCR and UACI performance of our encryption approach are relatively superior, and approaching optimal value, no matter the gray cryptographic image or the color cryptographic image. These results reveal that the proposed approach is safe, effective, and universal.

## 6 Conclusion

To protect digital images, a novel 2D chaotic model with excellent chaotic features is designed to develop new image encryption algorithms. This article first constructs a 2D chaotic structure model with a universal and superior chaotic performance to solve the problems of uneven distribution of chaotic trajectories and limited chaotic range in existing chaotic maps. For the existing 2D systems, the derived chaotic systems have better chaotic performance, more random chaotic sequences, and extensive chaotic parameter space. For verifying the effectiveness of the designed chaotic maps, it is implemented in image cryptography. The proposed approach first utilizes the SHA-512 function to calculate the keys according to the original image and further generates the chaotic sequence for confusion and diffusion to acquire the cryptographic image. Simulation evaluation indicated that the proposed encryption approach has illustrious encryption performance, high decryption quality, wide key space, extreme sensitivity to the key, and anti-various attacks.

**Acknowledgements** This research was supported by the National Key Research and Development Program of China (Grant No. 2020YFB1805403), the National Natural Science Foundation of China (Grant No. 62032002), BUPT Excellent Ph.D. Students Foundation (Grant No. CX2022141) and the 111 Project (Grant No. B21049).

**Funding** The authors have not disclosed any funding.

**Data Availability** The used datasets are available from <https://sipi.usc.edu/database/>, and <https://www.imageprocessingplace.com/>, and the data generated during this study are available from the corresponding author on reasonable request.

## Declarations

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

## References

- Zhou, R., Yu, S.: Break an enhanced plaintext-related chaotic image encryption algorithm. *Chaos, Solitons Fractals* **181**, 114623 (2024)
- Zhao, R., Zhang, Y., Nan, Y., Wen, W., Chai, X., Lan, R.: Primitively visually meaningful image encryption: a new paradigm. *Inf. Sci.* **613**, 628–648 (2022)
- Zhou, S., Wang, X., Zhang, Y.: Novel image encryption scheme based on chaotic signals with finite-precision error. *Inf. Sci.* **621**, 782–798 (2023)
- Golalipour, K.: A novel permutation-diffusion technique for image encryption based on the Imperialist Competitive Algorithm. *Multimed. Tools Appl.* **82**(1), 725–746 (2023)
- Zou, C., Wang, X., Li, H.: Image encryption algorithm with matrix semi-tensor product. *Nonlinear Dyn.* **105**, 859–876 (2021)
- Zhang, Z., Tang, J., Zhang, F., Ni, H., Chen, J., Huang, Z.: Color image encryption using 2D sine-cosine coupling map. *IEEE Access* **10**, 67669–67685 (2022)
- Sun, X., Zhong, C.: A fast image encryption algorithm with variable key space. *Multimed. Tools Appl.* **83**(12), 35427–35447 (2023)
- Zhang, X., Wang, Y., Wei, Q., He, A., Salhi, S., Yu, B.: DRBPPred-GAT: accurate prediction of DNA-binding proteins and RNA-binding proteins based on graph multi-head attention network. *Knowl. Based Syst.* **285**, 111354 (2024)
- Wang, X., Feng, L., Zhao, H.: Fast image encryption algorithm based on parallel computing system. *Inf. Sci.* **486**, 340–358 (2019)
- Kang, X., Guo, Z.: A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Process.* **80**, 115670 (2020)
- Liu, J., Chang, H., Ran, W., Wang, E.: Research on improved DNA coding and multidirectional diffusion image encryption algorithm. *Entropy* **25**(5), 746 (2023)
- Rezaei, B., Ghanbari, H., Enayatifar, R.: An image encryption approach using tuned Henon chaotic map and evolutionary algorithm. *Nonlinear Dyn.* **111**, 9629–9647 (2023)
- Nematzadeh, H., Enayatifar, R., Yadollahi, M., Lee, M., Jeong, G.: Binary search tree image encryption with DNA. *Optik* **202**, 163505 (2020)
- Li, L., Luo, Y., Qiu, S., Ouyang, X., Cao, L., Tang, S.: Image encryption using chaotic map and cellular automata. *Multimed. Tools Appl.* **81**, 40755–40773 (2022)
- Yousefian Darani, A., Khedmati Yengejeh, Y., Pakmanesh, H., Navarro, G.: Image encryption algorithm based on a new 3D chaotic system using cellular automata. *Chaos, Solitons Fractals* **179**, 114396 (2024)
- Zhou, S., Qiu, Y., Wang, X., Zhang, Y.: Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. *Nonlinear Dyn.* **111**, 9571–9589 (2023)
- Ning, H., Zhao, G., Li, Z., Gao, S., Ma, Y., Dong, Y.: A novel method for constructing dynamic S-boxes based on a high-performance spatiotemporal chaotic system. *Nonlinear Dyn.* **112**, 1487–1509 (2024)
- Gan, Z., Xiong, B., Pang, Z., Chai, X., Jiang, D., He, X.: A visually secure image encryption scheme using newly designed 1D sinusoidal chaotic map and P-tensor product compressive sensing. *Nonlinear Dyn.* **112**, 2979–3001 (2024)
- Wang, X., Shao, Z., Li, B., Fu, B., Shang, Y., Liu, X.: Color image encryption based on discrete trinomial Fourier transform and compressive sensing. *Multimed. Tools Appl.* **618**, 227–252 (2022)
- Wang, C., Song, L.: An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios. *Inf. Sci.* **642**, 119166 (2023)
- Zhang, Z., Tang, J., Ni, H., Huang, T.: Image adaptive encryption algorithm using a novel 2D chaotic system. *Inf. Sci.* **111**, 10629–10652 (2023)



22. Xian, Y., Wang, X.: Fractal sorting matrix and its application on chaotic image encryption. *Inf. Sci.* **547**, 1154–1169 (2021)
23. Demirtas, M.: A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. *Optik* **265**, 169430 (2022)
24. Hua, Z., Zhu, Z., Yi, S., Zhang, Z., Huang, H.: Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **546**, 1063–1083 (2020)
25. Zhang, Y., He, Y., Li, P., Wang, X.: A new color image encryption scheme based on 2DNLCML system and genetic operations. *Opt. Lasers Eng.* **128**(3), 106040 (2020)
26. Mohamadi, H.E., Lahlou, L., Kara, N., et al.: A versatile chaotic cryptosystem with a novel substitution-permutation scheme for internet-of-drones photography. *Nonlinear Dyn.* **112**, 4977–5012 (2024)
27. Liang, B., Hu, C., Tian, Z., Wang, Q., Jian, C.: A 3D chaotic system with multi-transient behavior and its application in image encryption. *Phys. A* **616**, 128624 (2023)
28. Liu, X., Tong, X., Wang, Z., Zhang, M.: A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption. *Chaos, Solitons Fractals* **154**, 111693 (2022)
29. Jiang, X., Jiang, G., Wang, Q., Shu, D.: Image encryption algorithm based on 2D-CLICM chaotic system. *IET Image Process* **17**(7), 2127–2141 (2023)
30. Liu, Z., Liu, J., Zhang, L., Zhao, Y., Gong, X.: Performance of the 2D Coupled Map Lattice Model and Its Application in Image Encryption. *Complexity* **2022**(1), 5193618 (2022)
31. 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**, 1859–1876 (2021)
32. Hua, Z., Zhu, Z., Chen, Y., Li, Y.: Color image encryption using orthogonal Latin squares and a new 2D chaotic system. *Nonlinear Dyn.* **104**, 4505–4522 (2021)
33. Teng, L., Wang, X., Xian, Y.: Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. *Inf. Sci.* **605**, 71–85 (2022)
34. Qiu, H., Xu, X., Jiang, Z., Sun, K., Xiao, C.: A color image encryption algorithm based on hyperchaotic map and Rubik's Cube scrambling. *Nonlinear Dyn.* **110**, 2869–2887 (2022)
35. Zhou, Z., Xu, X., Yao, Y., Jiang, Z., Sun, K.: Novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model. *Chaos, Solitons Fractals* **173**, 113630 (2023)
36. Wang, X., Xu, X., Sun, K., Jiang, Z., Li, M., Wen, J.: A color image encryption and hiding algorithm based on hyperchaotic system and discrete cosine transform. *Nonlinear Dyn.* **111**, 14513–14536 (2023)
37. Wang, X., Guan, N., Yang, J.: Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map. *Chaos, Solitons Fractals* **150**, 111117 (2021)
38. Hua, Z., Jin, F., Xu, B., Huang, H.: 2D Logistic-Sine-coupling map for image encryption. *Signal Process.* **149**, 148–161 (2018)
39. Murillo-Escobar, D., Murillo-Escobar, M.A., CruzHernández, C., Arellano-Delgado, A., López-Gutiérrez, R.M.: Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation. *Nonlinear Dyn.* **111**, 6773–6789 (2023)
40. Richman, J.S., Moorman, J.R.: Physiological time-series analysis using approximate entropy and sample entropy. *Am. J. Physiol. Heart Circ. Physiol.* **278**(6), 2039–49 (2000)
41. Yang, M., Dong, C., Pan, H.: Generating multi-directional hyperchaotic attractors: A novel multi-scroll system based on Julia fractal. *Phys. A* **636**, 129586 (2024)
42. Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.C., Hassan, Z.: Pseudo random number generator based on quantum chaotic map. *Commun. Nonlinear Sci. Numer. Simulat.* **19**, 101–111 (2014)
43. Bolos, V.J., Benitez, R., Ferrer, R.: A new wavelet tool to quantify non-periodicity of non-stationary economic time series. *Mathematics* **8**, 844 (2020)
44. Guo, Y., Ding, J., Mi, L.: Statistical complexity and stochastic resonance of an underdamped bistable periodic potential system excited by Ivy noise. *Chaos, Solitons Fractals* **179**, 114380 (2024)
45. Dong, Y., Zhao, G., Ma, Y., Pan, Z., Wu, R.: A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. *Inf. Sci.* **593**, 121–154 (2022)
46. Wang, X., Yang, J.: Spatiotemporal chaos in multiple coupled mapping lattices with multi dynamic coupling coefficient and its application in color image encryption. *Chaos, Solitons Fractals* **147**, 110970 (2021)
47. Liu, H., Liu, J., Ma, C.: Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. *Multimed. Tools Appl.* **82**, 23899–23914 (2023)
48. Yu, J., Xie, W., Zhong, Z., Wang, H.: Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation. *Chaos, Solitons Fractals* **162**, 112456 (2022)
49. Sun, J., Wang, W., Zhang, J.: Color image quantum steganography scheme and circuit design based on DWT+DCT+SVD. *Phys. A* **617**, 128688 (2023)
50. Patel, S., Vaish, A.: Block based visually secure image encryption algorithm using 2D-compressive sensing and nonlinearity. *Optik* **272**, 170341 (2023)

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.