Soft Computing (2023) 27:1223–1240
https://doi.org/10.1007/s00500-022-07706-4

FOUNDATION, ALGEBRAIC, AND ANALYTICAL METHODS IN SOFT COMPUTING

# An image encryption scheme using bit-plane cross-diffusion and spatiotemporal chaos system with nonlinear perturbation

Xingyuan Wang[1,2] · Maochang Zhao[1] · Sijia Feng[1] · Xuan Chen[1]

Accepted: 26 November 2022 / Published online: 4 January 2023

**Abstract**

In this paper, a dynamic coupled map lattices with nonlinear perturbations (NPDCML) is proposed. The test results show that the new spatiotemporal chaotic system has more obvious advantages than CML system in spatiotemporal performance and chaotic characteristics, and NPDCML system has larger parameter space and better cryptographic characteristics. Based on NPDCML system, a new image encryption scheme is proposed, which adopts the method of diffusion before confusion. After a round of diffusion, the image is scrambled by decomposing the bit plane, and the image is further encrypted by the way of mutual diffusion of high bit plane and low bit plane. Through the analysis of various test results, the encryption scheme can resist most common attacks, and it is proved that NPDCML system has good chaotic characteristics and cryptographic advantages.

**Keywords** NPDCML · Cryptographic characteristics · Image encryption · Bit plane · Diffusion–confusion

## 1 Introduction

With the rapid development of Internet and communication technology (Anand et al. 2020; Xu et al. 2021), especially the appearance of 5G technology and the expansion of bandwidth, the speed of information interactive transmission is also increasing. As a language which can convey visual information most quickly and has the strongest expressive power, multimedia information has the advantages that other data types do not have in the process of information exchange. As a carrier of information, image contains many important information (Hu and Li 2021). Improving the security of image information in the process of transmission, storage and processing has become a hot issue (Xian and Wang 2021). The methods of image protection mainly include image encryption (Su and Wang 2022; Khan et al. 2020), image steganography (Wang et al. 2021a) and image watermarking (Ma et al. 2020; Quan et al. 2020). As an easy to implement and efficient protection method, image encryption has received the attention of many scholars, and the most common way of image encryption is chaos encryption technology.

Chaotic system has been widely used because of its initial value sensitivity and pseudo-randomness (Zou et al. 2020). It is mainly divided into temporal chaos, hyperchaos and spatiotemporal chaos. Compared with one-dimensional time chaotic system, multidimensional or spatiotemporal chaotic system has multiple Lyapunov exponents, better chaotic performance, and more complex behavior. In 1989, Kaneko first proposed the coupled map lattice (CML) of spatiotemporal chaotic model and applied it to the field of fluid mechanics (Kaneko 1989). In the follow-up research, the characteristics of spatiotemporal chaos have also been explored by scholars, and its application in cryptography is also very bright. Since then, because the application scenarios of this model have been discovered continuously, people have carried out a large number of extensions and applications on the basis of CML model.

Some scholars extend CML model and propose one-way coupled map lattice (OCML) (Meherzi et al. 2006), global nonlocal coupled map lattice (GNCML) (Khellat et al.

✉ Xingyuan Wang
xywang@dlmu.edu.cn

✉ Maochang Zhao
17853117953@163.com

[1] School of Information Science & Technology, Dalian Maritime University, Dalian 116026, China

[2] Guangxi Key Lab of Multi-Source Information Mining & Security, Guangxi Normal University, Guilin 541004, China

2011) and other systems. Most of these systems are designed in linear coupling mode, but the nonlinear random coupling mode is not considered. Zhang et al. (Zhang and Wang 2013, 2014) proposed ACLML and mixed linear nonlinear coupling map lattice (MLNCML). The spatiotemporal chaos randomly selects the positions where the spatial coupling is qualified. The non-adjacent coupled spatiotemporal chaotic system enhances its chaotic characteristics, but there are still some defects, such as the coupling coefficient remains static, which also leads to the model's chaotic characteristics not obvious when the coupling coefficient is small. Subsequently, another scholar proposed SMDMCML (Wang and Yang 2021), which is similar to MLNCML, coupling adjacent terms and non-adjacent terms, and improving the coupling coefficient to eliminate the previous shortcomings. However, the performance of the model in time and space is not satisfactory. When the chaotic value is large, it is dense, and when it is small, it is sparse. Du et al. Wang and Du (2022) proposed the one-dimensional Logistic Chebyshev map (1DLCM). The model adopts the improved Chebyshev map with stronger chaotic characteristics to make the coupling coefficient dynamic, which makes it significantly improved in bifurcation diagram and other indicators. However, the performance of the model in Kolmogorov–Sinai entropy is also defective, and it shows overall non chaos in some parameters.

Image encryption has received the attention of many scholars in recent years. The most important encryption method is divided into two parts: diffusion and scrambling. Based on this method, many excellent and fast encryption methods are proposed (Wang and Gao 2020; Liu et al. 2012; Belazi et al. 2016). For diffusion, its main purpose is to change the value of a pixel while affecting and changing the value of all other pixels. The common methods include XOR diffusion, DNA coding, Boolean network, neural network and so on (Wang and Zhao 2021; Xian et al. 2021). Confusion is mainly to change the image pixel position, mainly through Arnold map, sorting index, cyclic shift and other ways (Mansouri and Wang 2021a; Qu et al. 2021). Using these technologies, scholars have carried out a lot of research. Wang (Wang and Du 2022) proposed an algorithm, which can perform parallel diffusion in the diffusion phase, and has higher encryption speed. Xian (Xian and Wang 2021) proposed a matrix with fractal characteristics, which was used for scrambling to obtain better encryption effect and lower complexity. Zhang (Zhang et al. 2013) used image fusion and DNA operation to encrypt the image. However, these encryption schemes are not all secure. For example, (Zhang et al. 2013) has been cracked (Zhang et al. 2014; Zhang 2015). The attacker obtains the encryption secret key by comparing the encrypted image of a special image with the plaintext image, and completes the cracking. In this paper, based on NPDCML system, an encryption algorithm based on bit-plane decomposition is proposed. The algorithm adopts the structure of diffusion before confusion, decomposes bit plane to disturb the position of binary value in high and low bit planes, and the binary of two bit planes diffuse each other between the two planes to complete encryption. Experimental results show that this is a secure encryption algorithm with low time complexity and strong robustness. The overall contribution of the proposed work can be summarized as follows:

(1) A spatiotemporal chaotic system with nonlinear coupling disturbance and dynamic coupling coefficient is proposed.
(2) The new system has a larger parameter space and further enhances the chaotic characteristics and range.
(3) An image encryption strategy based on bit-plane segmentation is proposed, which makes the diffusion between pixels more sufficient and improves the security of encryption.
(4) It has a good performance in the test of images in USC-SIPI image database.

The remainder of the paper is organized as follows. Second 2 introduces and analyzes the NPDCML system. Section 3 introduces the application of NPDCML system in image encryption. Section 4 is the experimental results and safety analysis. Section 5 is the conclusion.

## 2 Dynamic coupled map lattices with nonlinear perturbations

In Kaneko (1989), Kaneko proposed the spatiotemporal chaos model CML system for the first time, as shown in Eq. (1).

$$\begin{cases} f(x_n) = \mu x_n(1 - x_n) \\ x_{n+1}(i) = (1 - e)f(x_n(i)) + \frac{e}{2}(f(x_n(i-1)) + f(x_n(i+1))) \end{cases} \tag{1}$$

where $f(x)$ is a Logistic map and is chaotic when the range of $\mu$ is in (3.57, 4]. $L$ is the number of lattices, $n$ and $i$ represent temporal index and spatial index, respectively, and $i$ belongs to $[1, L]$. $e$ is the coupling coefficient between lattice and adjacent lattices and $0 \le e \le 1$.

In order to further optimize the dynamic behavior of CML system, Zhang (Zhang and Wang 2014) proposed MLNCML, which has stronger spatial chaotic behavior. The mathematical expression is as follows:

$$\begin{cases} \begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} (\mathrm{mod} L) \\ f(x_n) = \mu x_n(1-x_n) \\ x_{n+1}(i) = (1-e)f(x_n(i)) + (1-\eta)\frac{e}{2}((f(x_n(i-1)) \\ \quad +(f(x_n(i+1)))) + \eta\frac{e}{2}(f(x_n(j)) + f(x_n(k))) \end{cases} \tag{2}$$

where $\eta$ is the coupling coefficient of nonlinear coupling, and the position of nonlinear coupling lattices is determined by Arnold map.

In this paper, dynamic coupled map lattices with nonlinear perturbations (NPDCML) is proposed. In this model, the static coupling coefficient $e$ is replaced by the output value of the Logistic map, and two spatial sequence lattices are selected nonlinearly to disturb the adjacent coupling terms, which further improves the spatiotemporal chaos. The mathematical expression is as follows:

$$\begin{cases} \begin{bmatrix} j \\ k \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} (\mathrm{mod}\, L) \\ e_{n+1} = \varphi e_n(1-e_n) \\ f(x_n) = \mu x_n(1-x_n) \\ x_{n+1}(i) = (1-e_n)f(x_n(i)) + \frac{e_n}{2}\left(f\left(\sqrt{x_n(i-1)\times x_n(j)}\right) \right. \\ \quad \left. +f\left(\sqrt{x_n(i+1)\times x_n(k)}\right)\right) \end{cases} \tag{3}$$

where $e_n$ is the value of the $n$-th element in the time sequence generated by Logistic map. Through the nonlinear calculation of the coupling term and perturbation term, two new coupling terms are obtained.

In order to better compare the above spatiotemporal chaotic systems, their Kolmogorov–Sinai entropy, information entropy and others are tested and analyzed. The specific parameter values are set as $\varphi = 3.99$, $p = 13$, $q = 7$, $L = 100$.

## 2.1 Kolmogorov–Sinai entropy analysis

In low-dimensional chaotic system, Lyapunov exponent (LE) (Shevchenko 2014; Shen et al. 2014) is often used to judge the strength of chaos.

$$\lambda = \lim \frac{1}{n}\sum_{i=0}^{n-1} \ln\left|\frac{\mathrm{d}F(x)}{\mathrm{d}x}\right|_{x=x_i} \tag{4}$$

where $F(x)$ is the dynamic system and $i$ is the time sequence. Each lattice of spatiotemporal chaotic system outputs a time sequence, and each time sequence has a LE. Therefore, it has $L$ LEs and cannot be evaluated by only one LE. In order to analyze chaos better, some scholars put forward the concept of Kolmogorov–Sinai entropy density (KSED) and Kolmogorov–Sinai entropy breadth (KSEB). The KSED $h$ is that the positive LEs of all lattices are accumulated and divided by the number of lattices $L$, and the KSEB $hu$ is the ratio of the number of lattices with positive LE to the total number. The calculation formulas are as follows:

$$h = \frac{\sum_{i=1}^{L} \lambda_{(i)}^{+}}{L} \tag{5}$$

$$hu = \frac{L^{+}}{L} \tag{6}$$

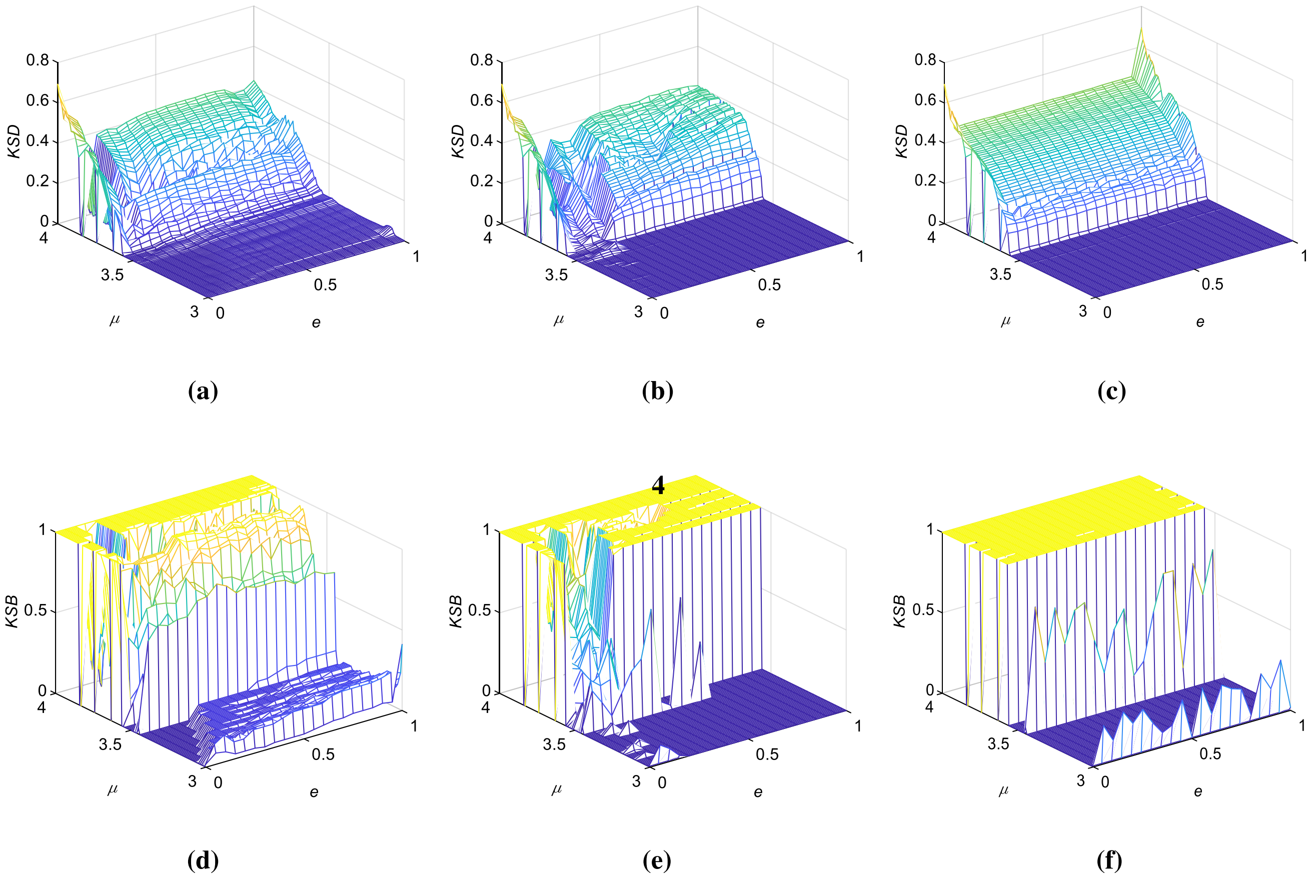
where the molecules of Eqs. (5) and (6) represent the sum of the LEs of lattices with LE greater than 0 and the total number of lattices with LE greater than 0.

Figure 1 shows the Kolmogorov–Sinai entropy of CML, MLNCML and NPDCML systems. It can be seen from Fig. 1 that the entropy density of CML and MLNCML systems is greater than 0 and the entropy breadth is mostly at 1 when $\mu$ = [3.5, 4], but both have obvious depressions at $\mu = 3.8$. Obviously, compared with the first two spatiotemporal chaotic systems, NPDCML makes up for the defects caused by the non-chaotic periodic window of Logistic map when the parameter $\mu = 3.8$ and increases the parameter space. Therefore, NDPCML is superior to CML and MLNCML.

The percentage of lattices in chaos under different parameters pairs can be seen from Fig. 2. In CML, 90% of the parameters can make 50% lattices in chaos, while in MLNCML and NPDCML, 75 and 80% of the parameters can make 50% lattices in chaos. However, the number of parameter pairs decreases with the increase in the percentage of chaotic lattices. When the lattices are 100% chaotic, the parameter pairs of CML system are reduced to 40%, MLNCML system is reduced to 65%, while NPDCML system is only reduced by 1.5, and 78.5% of the parameter pairs can make all the lattice chaotic. Therefore, the chaotic parameter space of NPDCML system is wider, and its chaotic characteristics are stronger.

## 2.2 Bifurcation diagram

The bifurcation diagram can clearly describe the ergodic range under specific parameters. The 50-th lattice is selected to analyze the bifurcation diagram. The bifurcation diagrams of CML system and NPDCML system can be seen from Fig. 3 when the initial values of coupling coefficient $e$ are set to 0.1, 0.5 and 0.9. For CML system, when $3.7 < e < 3.8$, there is an obvious period window, and the influence of $e$ on CML system is very large. For



(a)

(b)

(c)

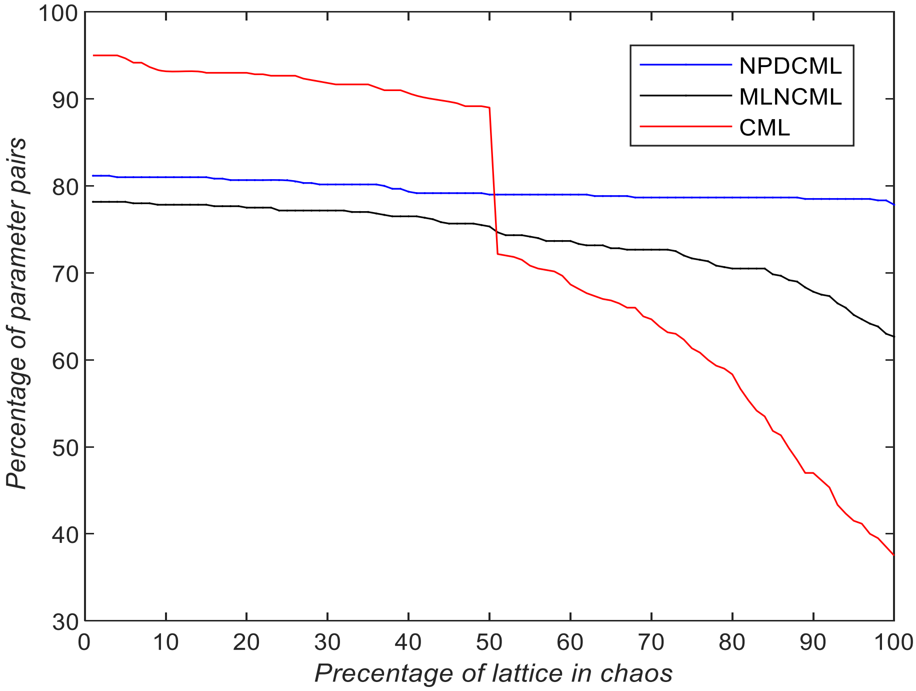
(d)

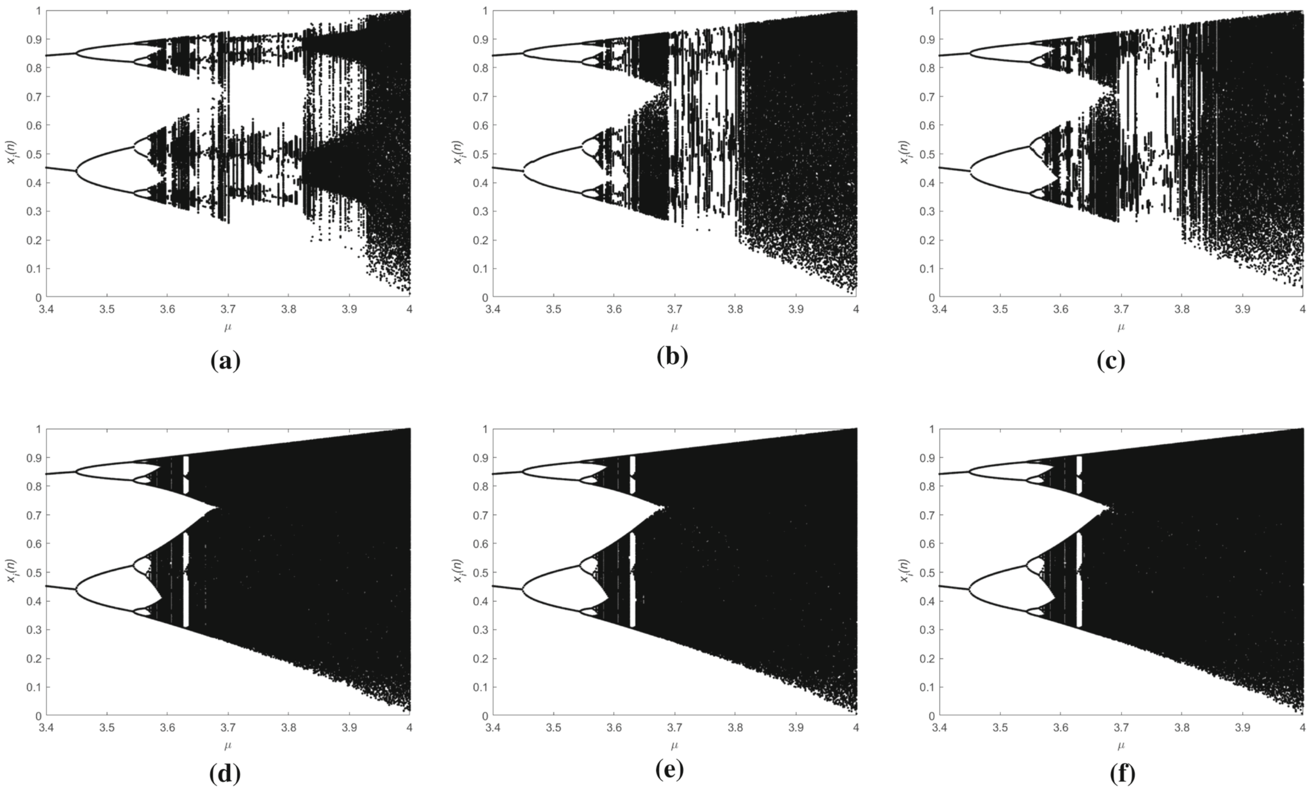
(e)

(f)

**Fig. 1** KSED and KSEB: **a** KSED of CML; **b** KSED of MLNCML; **c** KSED of NPDCML; **d** KSEB of CML; **e** KSEB of MLNCML; **f** KSEB of NPDCML

**Fig. 2** Comparison of percentage of lattices in chaos





(a)

(b)

(c)

(d)

(e)

(f)

**Fig. 3** Bifurcation diagram: **a** CML at $e$ = 0.1; **b** CML at $e$ = 0.5; **c** CML at $e$ = 0.9; **d** NPDCML at $e$ = 0.1; **e** NPDCML at $e$ = 0.5; **f** NPDCML at $e$ = 0.9

NPDCML system, the dynamic coupling coefficient reduces the influence of $e$ on bifurcation diagram and eliminates most of the periodic windows. Therefore, NPDCML system has better characteristics than CML system.

## 2.3 Information entropy

The concept of information entropy was put forward by Shannon (Shannon 1949) which is used to analyze and measure the randomness of signals. Information entropy is defined as Eq. (7):

$$H(s) = -\sum_{i=1}^{n} P(s_i)\log_2 p(s_i) \tag{7}$$

where $s_i$ is the state of the information source. In this paper, the number of information source states $n$ is 10, $s$ represents the time series of spatiotemporal chaotic system. The value of chaotic sequence is between 0 and 1, and it is divided into ten states with 0.1 step size, so the theoretical maximum value is $\log_2 10 \approx 3.32$.

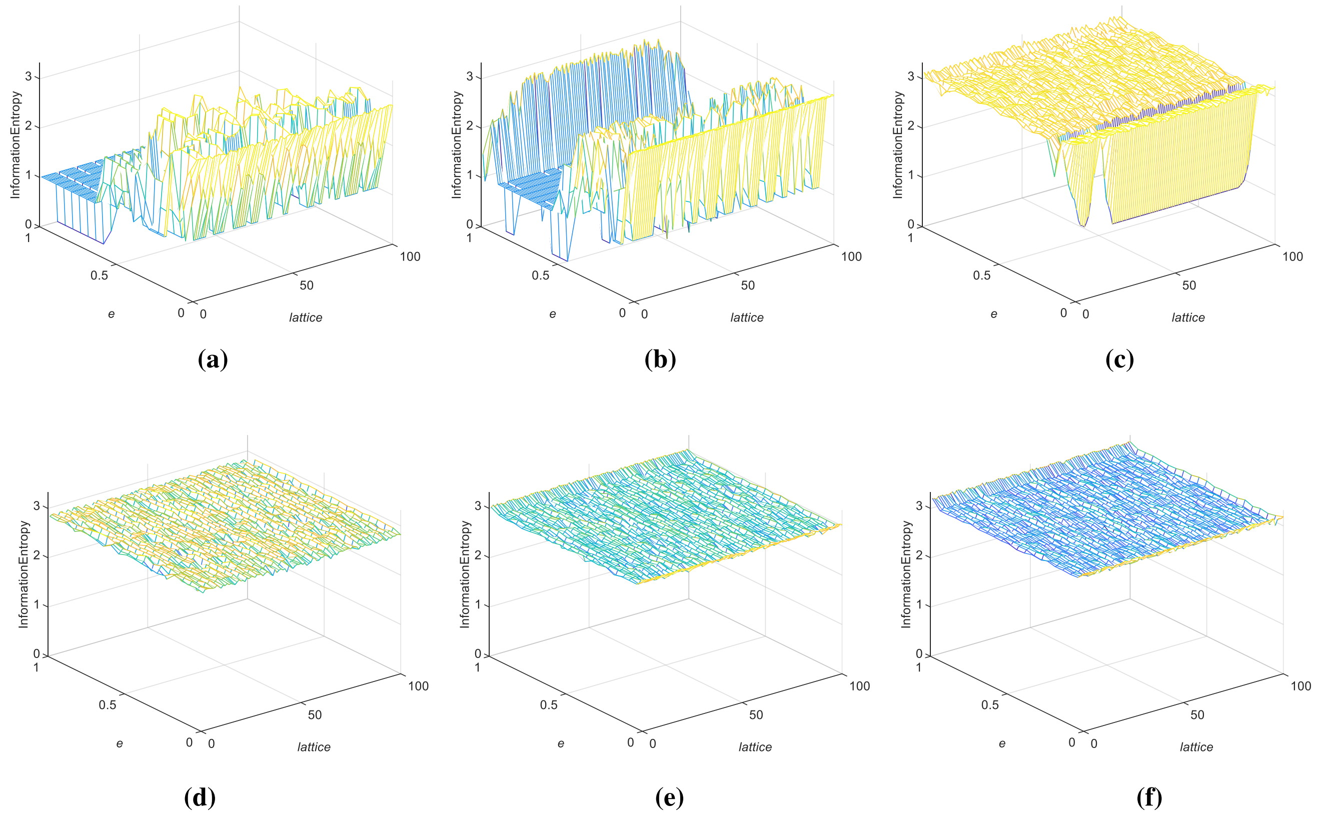
The information entropy of CML and NPDCML is shown in Fig. 4 when $\mu$ = 3.7, 3.8 and 3.99. When $\mu$ = 3.7 and $\mu$ = 3.8, the information entropy of half lattice of CML system is about 1. When $\mu$ = 3.99, the information entropy is mostly equal to 3, but it has obvious defects when $e$ = 0.1. For NPDCML system, with the increase in parameter $\mu$, the value of information entropy increases from 2.8 to 3.1. Therefore, the pseudo-randomness of NPDCML system is better than that of CML system.

## 2.4 Spatiotemporal behaviors

CML system has six spatiotemporal patterns, while NPDCML has only three spatiotemporal patterns. When $\mu$ = [0, 3.56], it is in the frozen random pattern. Figure 5 shows the spatiotemporal performance of one-period, two-period, four-period, and eight-period, respectively. When $\mu$ = [3.57, 3.76], we can see from Fig. 6 that four chaotic bands gradually become one chaotic band. When $\mu$ = [3.8, 4], the NPDCML system enters the complete turbulence pattern. With the increase in the parameter $\mu$, the chaotic band fills the whole space (Fig. 7).

# 3 Application in image encryption

The flowchart of the algorithm is shown in Fig. 8. The encryption algorithm uses the method of scrambling after diffusion, which can effectively disrupt the arrangement of pixels, weaken the correlation, and resist the attack.



**(a)** **(b)** **(c)**

**(d)** **(e)** **(f)**

**Fig. 4** Information entropy of each lattice: **a** CML at $\mu$ = 3.7; **b** CML at $\mu$ = 3.8; **c** CML at $\mu$ = 3.99; **d** NPDCML at $\mu$ = 3.7; **e** NPDCML at $\mu$ = 3.8; **f** NPDCML at $\mu$ = 3.99

### 3.1 Secret key generation

For a secure encryption algorithm, anti-attack is the most important. For image encryption algorithm, resisting violent attack requires the size of key-space to be greater than $2^{100}$ (Alvarez and Li 2006). This algorithm uses the XOR of 256-bits random string and SHA-256 to generate the secret key $K$, so the size of key-space is $2^{256}$. The required parameter of the algorithm is IEP = {$c_i$, $e$, $\mu$, $w$}, where $c_i$ ($i$ = 1, 2, …, 8) is the initial value of NPDCML system, which is calculated by $K$:

$$c_i = \frac{\sum_{j=20\times(i-1)+1}^{20\times i} K_j \times 2^{j-1}}{2^{20}} \tag{8}$$

other parameters required by the algorithm are shown in Eq. (9):

$$\begin{cases} e = \sum_{j=161}^{192} K_j \times 2^{j-1} \Big/ 2^{32} \\ \mu = 3.999 + 0.001 \times \left( \sum_{j=193}^{224} K_j \times 2^{j-1} \Big/ 2^{32} \right) \\ w = 256 \times \left\lfloor \left( \sum_{j=225}^{256} K_j \times 2^{j-1} \Big/ 2^{32} \right) \right\rfloor \end{cases} \tag{9}$$

According to the generated initial value, the NPDCML system is iterated $MN$+500 times, and the matrix *cmat* is obtained after discarding the first 500 values. The sequences are processed as confusion and diffusion matrixes (Figs. 9 and 10).

$$\begin{cases} I1 = \mathrm{sort}(\mathrm{cmat}(1,:))\, I2 = \mathrm{sort}(\mathrm{cmat}(2,:)) \\ D = \mathrm{cmat}(3,:)\, D1 = [\mathrm{cmat}(4,:), \mathrm{cmat}(5,:)] \\ S = \lfloor \mathrm{cmat}(6,:) \times 8 \rfloor\, S1 = \lfloor [\mathrm{cmat}(7,:), \mathrm{cmat}(8,:)] \times 4 \rfloor \end{cases} \tag{10}$$

### 3.2 Diffusion and confusion module

For the image $P$ with the size of $M \times N$, according to the chaotic matrix $D$ and $S$ generated by NPDCML system, the linear diffusion operation is performed on $P$ using Eq. (11) to obtain the image $\hat{P}$.

$$\begin{cases} \hat{P}(1) = \mathrm{CSR}(\mathrm{mod}(\mathrm{floor}(P(1) + D(1) \times w), 256), S(1)) \\ \hat{P}(i) = \mathrm{CSR}(\mathrm{mod}(\mathrm{floor}(P(i) \oplus \hat{P}(i-1) + D(i) \times w), 256), S(i)) \end{cases} \tag{11}$$

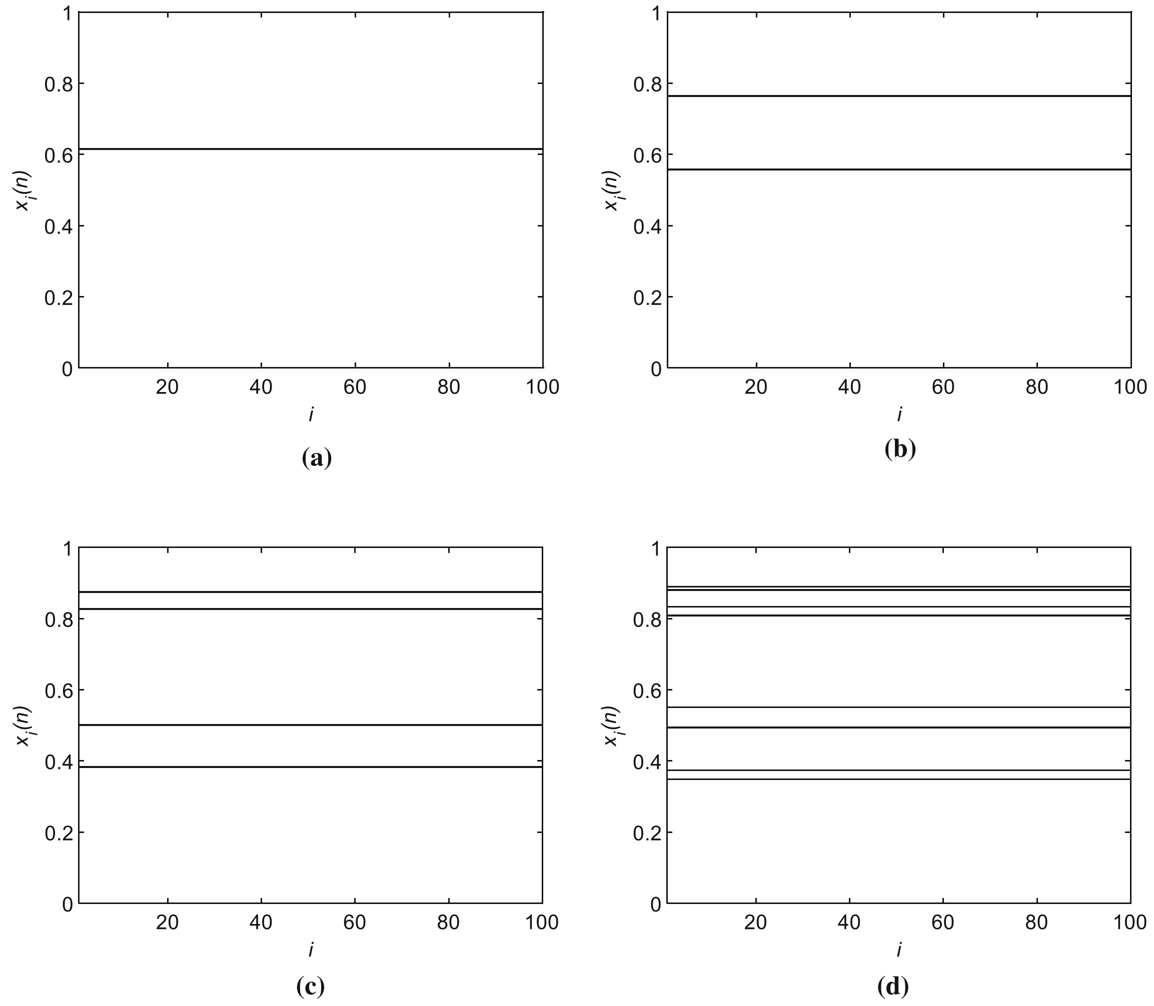


**Fig. 5** Frozen random pattern: **a** $\mu$ = 2.6; **b** $\mu$ = 3.1; **c** $\mu$ = 3.5; **d** $\mu$ = 3.56

where CSR represents cyclic shift to the right, mod represents remainder operation, floor represents rounding down, and $\oplus$ represents the XOR operation.

Before scrambling, the diffused image $\hat{P}$ is decomposed into eight bit planes. Then, the higher four bit planes and the lower four bit planes are merged, respectively, to obtain $H$ and $L$. The chaotic sequences generated by NPDCML system are sorted to obtain index matrices $I1$ and $I2$, and then the two planes are scrambled according to $H1(I1(i)) = H(i)$, $L1(I2(i)) = L(i)$, and $i \in \{1, 2, ..., M \times N\}$. The scrambled matrix $H1$ and $L1$ are crossed and merged in rows to obtain a plane $HL$ with the size of $2M \times N$. After zigzag transformation of the combined matrix $HL$, the transformed matrix is divided into two parts to obtain $HM$ and $LM$. Cross-diffusion operation is carried out for the two parts. Finally, the ciphertext image $C$ is obtained. This algorithm can be described as in Algorithm 1.

```
Algorithm 1: Bit-planes confusion and diffusion.
Input: Image $\hat{P}$ with the size of $M \times N$, matrixes $I1$, $I2$, $D1$, and $S1$.
Output: Cipher image $C$.
Decompose image $\hat{P}$ into 8 bit-planes;
$H$ and $L$ are obtained by merging the higher and lower four bit-planes respectively;
for $i = 1$ to $M \times N$ do
    $H1(I1(i)) = H(i)$; $L1(I2(i)) = L(i)$; // Two planes are scrambled
end
for $i = 1$ to $M$ do
    $HL(2i\text{-}1, :) = H1(i, :)$; $HL(2i, :) = L1(i, :)$; // Crossed and merged in rows
end
$Z$ = zigzag($HL$); // Zigzag transformation of the combined matrix $HL$
$HM = Z(1{:}M, :)$; $LM = Z(M{+}1{:}2M, :)$;
$HD(1) = \mathrm{CSR}(HM(1) \oplus \mathrm{floor}(D1(1) \times 16), S1(1))$; // Cross diffusion operation is carried out for
    the two parts
$LD(1) = \mathrm{CSR}(\mathrm{mod}(LM(1) + HD(1), 16) \oplus \mathrm{floor}(D1(2) \times 16), S1(2))$;
for $i = 2$ to $M \times N$ do
    $HD(i) = \mathrm{CSR}(\mathrm{mod}(HM(i) + LD(i\text{-}1), 16) \oplus \mathrm{floor}(D1(2i\text{-}1) \times 16), S1(2i\text{-}1))$;
    $LD(i) = \mathrm{CSR}(\mathrm{mod}(LM(i) + HD(i), 16) \oplus \mathrm{floor}(D1(2i) \times 16), S1(2i))$;
end
Combining $HD$ and $LD$ to get ciphertext image $C$;
```

### 3.3 Decryption process

Firstly, the matrixes needed for decryption are generated, and the ciphertext image is decomposed into two parts. According to Eq. (12), the inverse diffusion between *HD* and *LD* is carried out.

$$\begin{cases} L(i) = \mathrm{mod}(\mathrm{CSL}(LD(i), S1(2 \times i)) \oplus \mathit{floor}(D1(2 \times i) \times 16) - HD(i), 16) \\ H(i) = \mathrm{mod}(\mathrm{CSL}(HD(i), S1(2 \times i - 1)) \oplus \mathit{floor}(D1(2 \times i - 1) \times 16) - LD(i - 1), 16) \\ L(1) = \mathrm{mod}(\mathrm{CSL}(LD(1), S1(2)) \oplus \mathrm{floor}(D1(2) \times 16) - HD(1), 16) \\ H(1) = \mathrm{CSL}(HD(1), S1(1)) \oplus \mathrm{floor}(D1(1) \times 16) \end{cases} \tag{12}$$

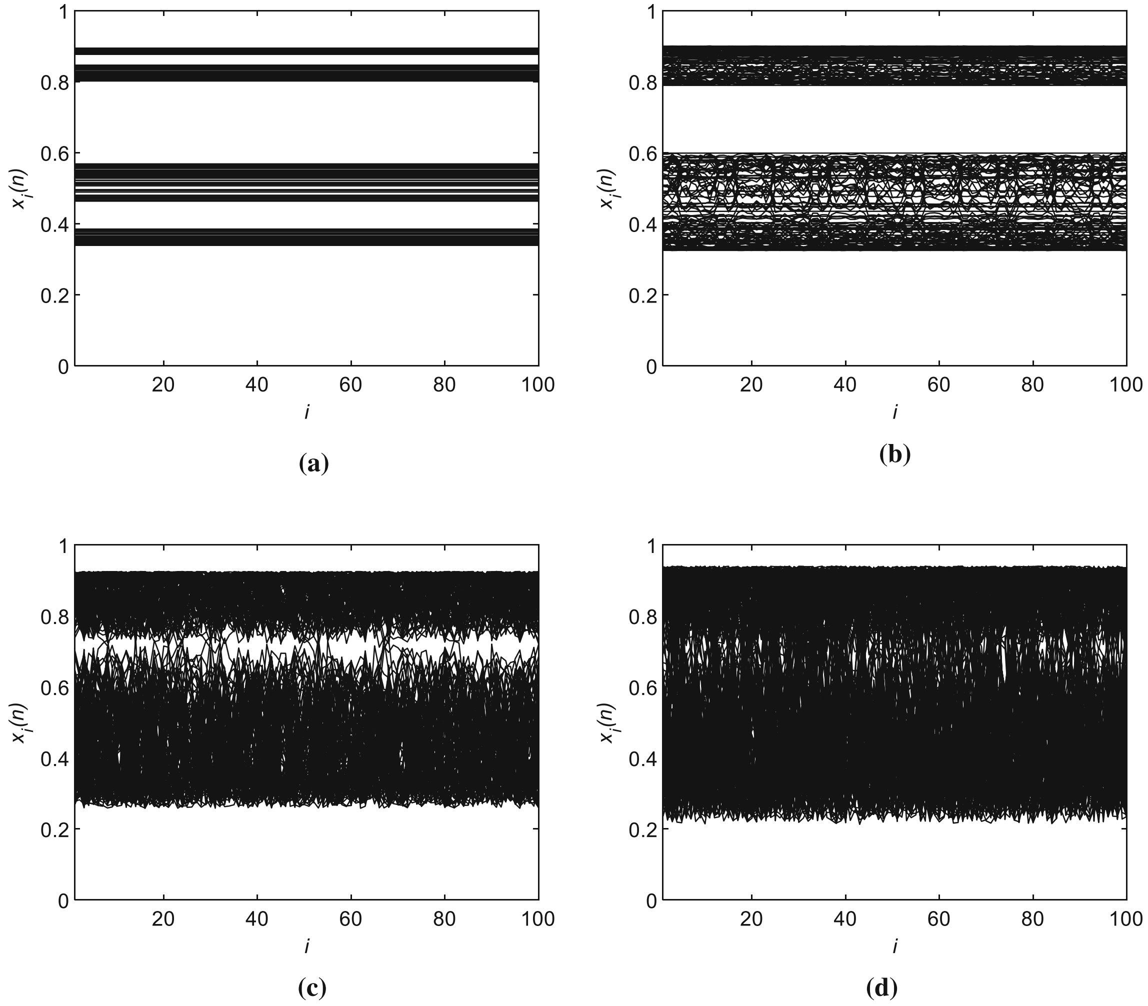
Then, the two parts of inverse diffusion are merged and inverse zigzag operation is performed on them. After decomposition, inverse scrambling is performed and bit planes are merged. Finally, *P* is obtained by inverse linear diffusion according to Eq. (13).

$$\begin{cases} P(i) = \mathrm{mod}(\mathrm{ceil}(\mathrm{CSL}(\hat{P}(i), S(i)) - D(i) \times w), 256) \oplus \hat{P}(i - 1) \\ P(1) = \mathrm{mod}(\mathrm{ceil}(\mathrm{CSL}(\hat{P}(1), S(1)) - D(1) \times w), 256) \end{cases} \tag{13}$$

## 4 Simulation results and security analysis

### 4.1 Simulation results

In Fig. 11a, four different types and sizes of images are selected for simulation. They are gray and color "Lena" image, binary image, and the upper half of the cropped color pepper image. Figure 11c is encrypted noise-like images, which has almost no association with the plaintext images. Figure 11b and d shows their histograms. Comparing the two groups of images, the number of each gray-level pixel of the encrypted image is almost the same, indicating that the pixel distribution is relatively uniform, and the pixel value of the image is more random. The last group is the decrypted image, which can be restored to the state before encryption without being destroyed.



(a)

(b)

(c)

(d)

**Fig. 6** Competitive intermittent chaos pattern: **a** $\mu$ = 3.57; **b** $\mu$ = 3.6; **c** $\mu$ = 3.7; **d** $\mu$ = 3.76

## 4.2 Secret key analysis

The key used in this algorithm is generated by the combination of random string and SHA-256 function. Due to the sensitivity of SHA-256 function to the input value, the secret key of this algorithm is also highly sensitive. The original parameters and slightly changed parameters are used for encryption, and the pixel number change rate (NPCR) is used as an index to evaluate the key sensitivity and the difference of encrypted images. Use *IEP* = $\{c_i, e, \mu, w\}$ and *IEP*' after minor changes to encrypt and calculate the difference between ciphertext images. In Table 1, NPCR is close to 99.6%. Therefore, this algorithm is very sensitive to the key.

## 4.3 Correlation analysis

Each pixel in the image does not exist independently, because it contains a lot of valuable information, resulting in a certain correlation between pixels in the same area, mainly in that their pixel values are very close. The calculation formula is as follows:

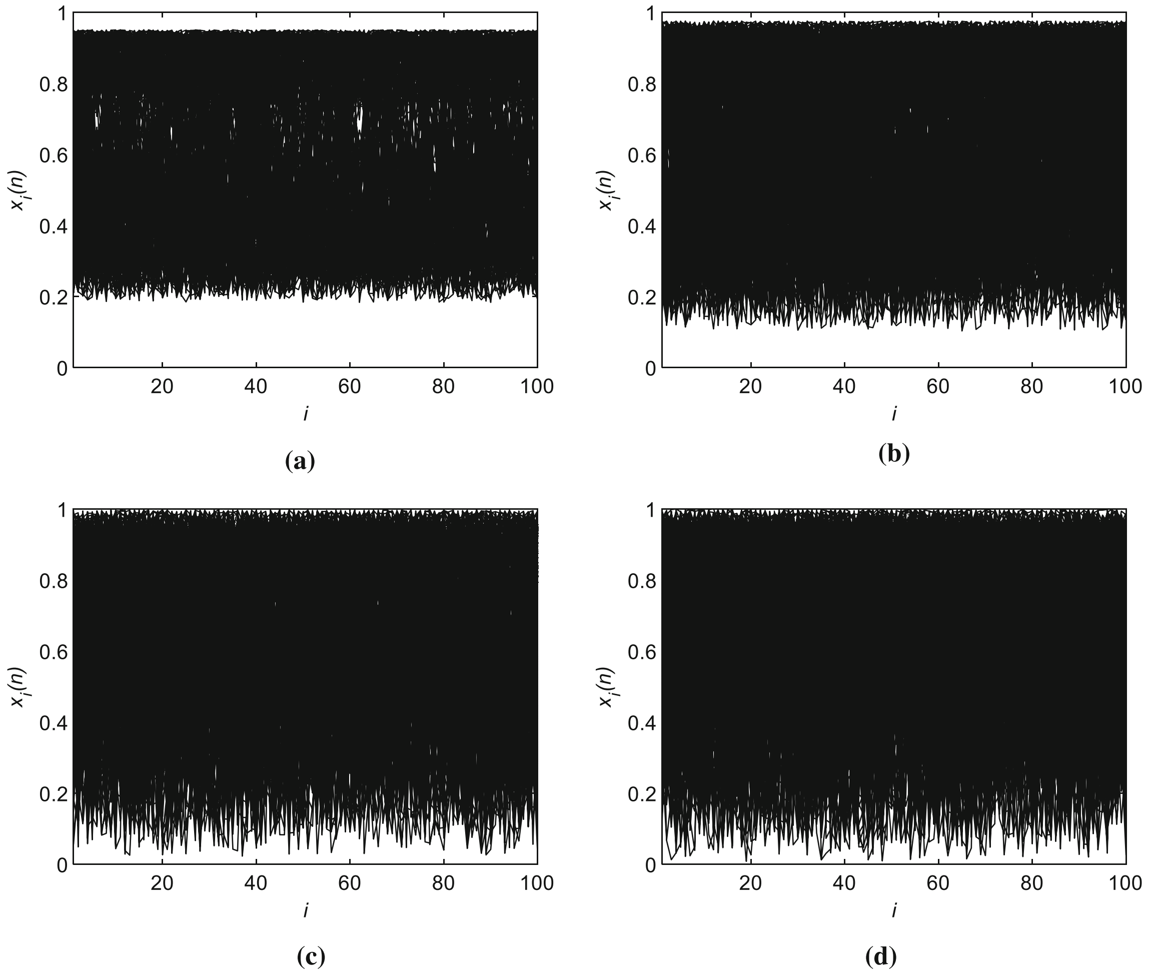
$$\mathrm{Corr}_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}} \tag{14}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{16}$$

where $x$ represents a pixel and $y$ is its adjacent pixel, $N$ is the total number of the selected pixels. In this paper, $N = 5000$.

In Fig. 12, the two coordinate axes are the values of two pixels, respectively. The values of two adjacent pixels of Pepper's original image are distributed near the diagonal, which indicates that the values of X-axis and Y-axis are very close, so the correlation is strong. However, the distribution of ciphertext image is uniform, which indicates



(a)

(b)

(c)

(d)

**Fig. 7** Complete turbulence pattern: **a** $\mu$ = 3.8; **b** $\mu$ = 3.9; **c** $\mu$ = 3.99; **d** $\mu$ = 4

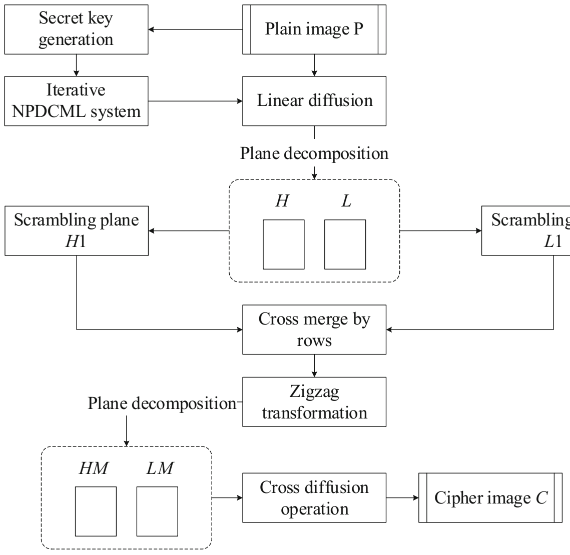


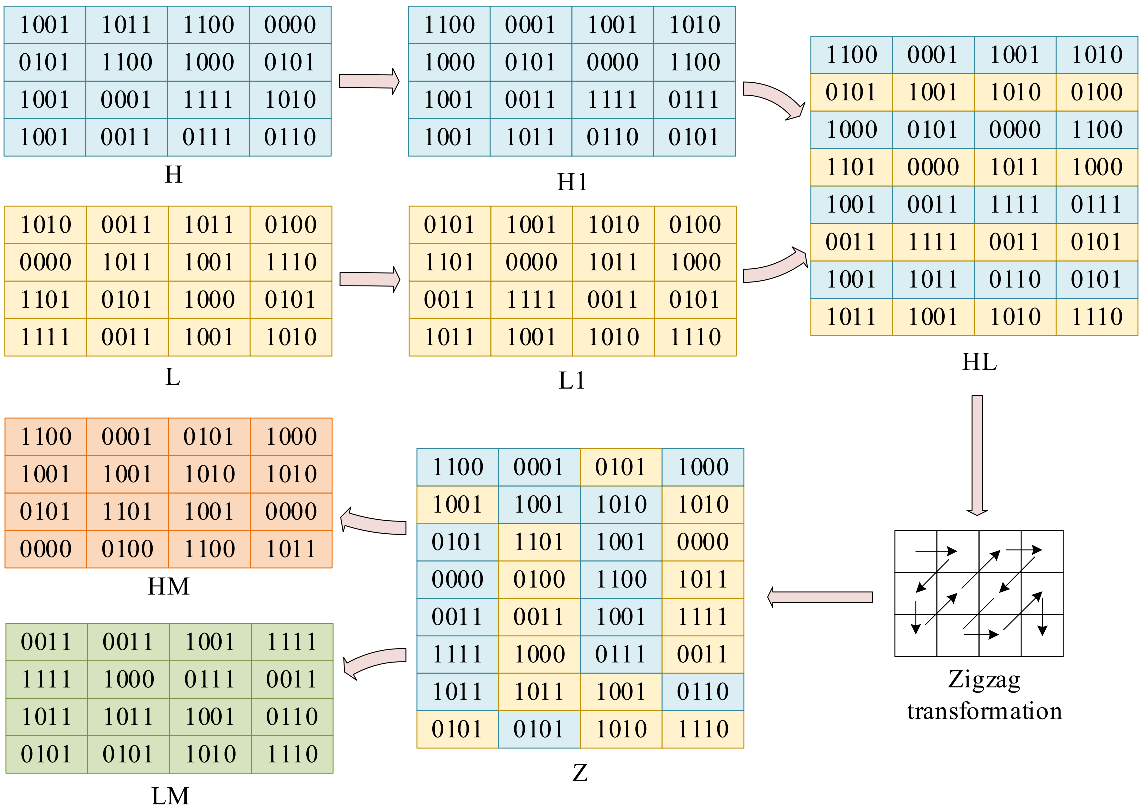
**Fig. 8** Encryption flowchart

that there is little correlation between pixel values and its correlation is very small.

The left side of Table 2 shows the correlation of Lena, pepper, house and other images from USC-SIPI image database, and the correlation of these images is above 0.8, which is very strong. The right side of Table 2 shows the correlation of cipher images corresponding to these images, most of which are below 0.02. The comparison shows that the average correlation of this algorithm is lower and closer to 0.

## 4.4 Information entropy

The encrypted ciphertext image is similar to the matrix composed of random values, and the randomness performance of this matrix can be measured by information entropy. According to the measurement results, whether the encrypted image has randomness can be determined. In this paper, 256 Gy level images are used for simulation test. The specific tests are shown in the Table 3. The image information entropy after encryption of the algorithm in



H

| | | | |
|---|---|---|---|
| 1001 | 1011 | 1100 | 0000 |
| 0101 | 1100 | 1000 | 0101 |
| 1001 | 0001 | 1111 | 1010 |
| 1001 | 0011 | 0111 | 0110 |

H1

| | | | |
|---|---|---|---|
| 1100 | 0001 | 1001 | 1010 |
| 1000 | 0101 | 0000 | 1100 |
| 1001 | 0011 | 1111 | 0111 |
| 1001 | 1011 | 0110 | 0101 |

L

| | | | |
|---|---|---|---|
| 1010 | 0011 | 1011 | 0100 |
| 0000 | 1011 | 1001 | 1110 |
| 1101 | 0101 | 1000 | 0101 |
| 1111 | 0011 | 1001 | 1010 |

L1

| | | | |
|---|---|---|---|
| 0101 | 1001 | 1010 | 0100 |
| 1101 | 0000 | 1011 | 1000 |
| 0011 | 1111 | 0011 | 0101 |
| 1011 | 1001 | 1010 | 1110 |

HL

| | | | |
|---|---|---|---|
| 1100 | 0001 | 1001 | 1010 |
| 0101 | 1001 | 1010 | 0100 |
| 1000 | 0101 | 0000 | 1100 |
| 1101 | 0000 | 1011 | 1000 |
| 1001 | 0011 | 1111 | 0111 |
| 0011 | 1111 | 0011 | 0101 |
| 1001 | 1011 | 0110 | 0101 |
| 1011 | 1001 | 1010 | 1110 |

Z

| | | | |
|---|---|---|---|
| 1100 | 0001 | 0101 | 1000 |
| 1001 | 1001 | 1010 | 1010 |
| 0101 | 1101 | 1001 | 0000 |
| 0000 | 0100 | 1100 | 1011 |
| 0011 | 0011 | 1001 | 1111 |
| 1111 | 1000 | 0111 | 0011 |
| 1011 | 1011 | 1001 | 0110 |
| 0101 | 0101 | 1010 | 1110 |

HM

| | | | |
|---|---|---|---|
| 1100 | 0001 | 0101 | 1000 |
| 1001 | 1001 | 1010 | 1010 |
| 0101 | 1101 | 1001 | 0000 |
| 0000 | 0100 | 1100 | 1011 |

LM

| | | | |
|---|---|---|---|
| 0011 | 0011 | 1001 | 1111 |
| 1111 | 1000 | 0111 | 0011 |
| 1011 | 1011 | 1001 | 0110 |
| 0101 | 0101 | 1010 | 1110 |

**Fig. 9** Bit-plane scrambling

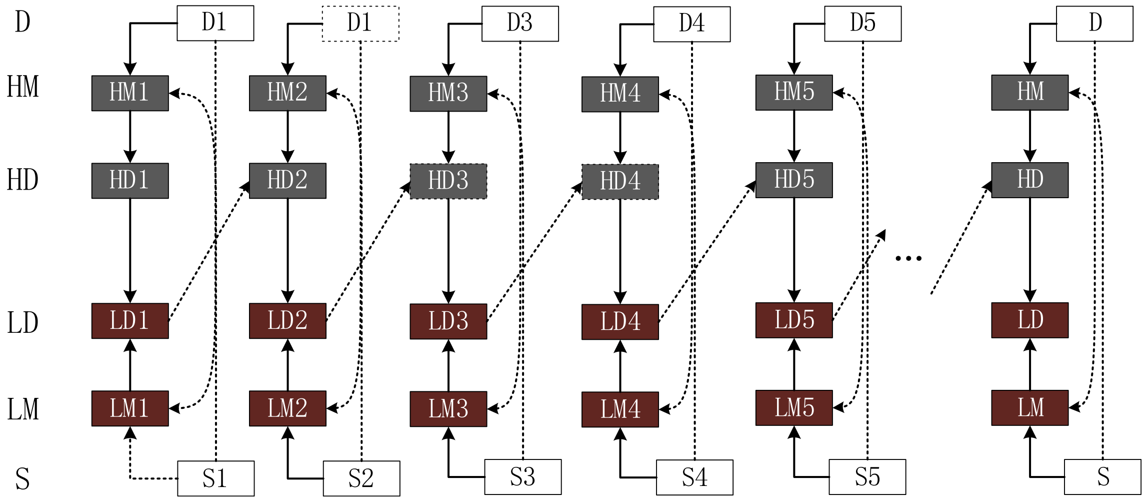


**Fig. 10** Bit-plane cross-diffusion

this paper is above 7.997, indicating that the randomness of the ciphertext image is very good. A comparison is made in Table 4.

## 4.5 Differential cryptanalysis

The way of differential attack on image encryption algorithm is to compare and analyze the propagation of different images with small specific differences after encryption. For example, select an image $P$ to obtain $C_1$ after encryption, then randomly change a pixel value of image $P$, and then encrypt it to obtain $C_2$. By comparing the differences between $C_1$ and $C_2$, it is used to judge and calculate the encryption process of the encryption algorithm. NPCR and UACI are defined as Eqs. (17)–(19):

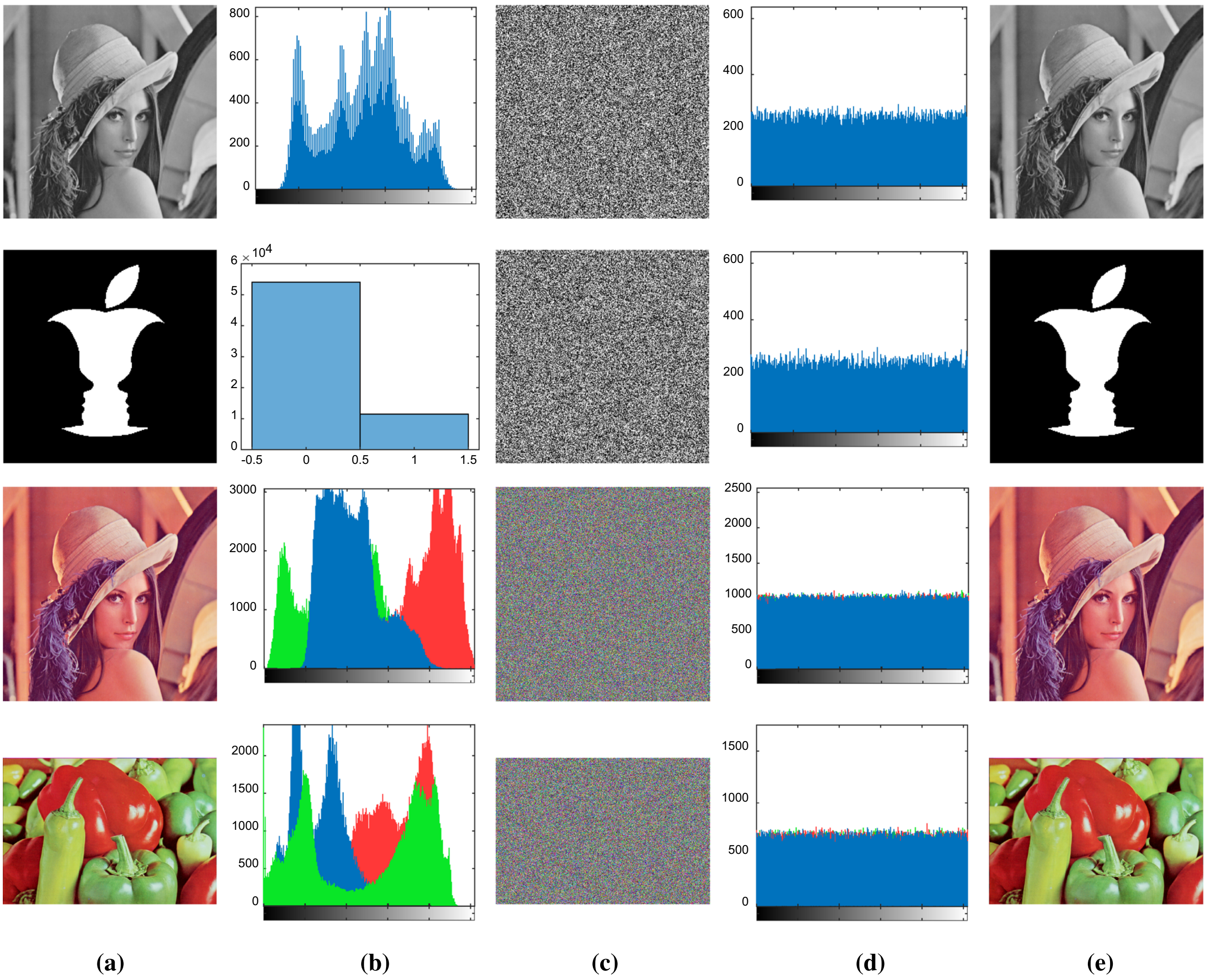


**Fig. 11** Simulation results: **a** Images; **b** Histogram; **c** Cipher images; **d** Histogram; **e** Decryption of the **c**

**Table 1** Key sensitivity

| Secret Key | Lena (256 × 256) | Pepper (256 × 256) | Plane (256 × 256) |
|---|---|---|---|
| $c'_1 = c_1 + 10^{-14}$ | 99.6201 | 99.6323 | 99.5773 |
| $c'_2 = c_2 + 10^{-14}$ | 99.5773 | 99.6216 | 99.6353 |
| $c'_3 = c_3 + 10^{-14}$ | 99.6048 | 99.6246 | 99.6063 |
| $c'_4 = c_4 + 10^{-14}$ | 99.6155 | 99.6262 | 99.5789 |
| $c'_5 = c_5 + 10^{-14}$ | 99.6155 | 99.6017 | 99.6109 |
| $c'_6 = c_6 + 10^{-14}$ | 99.5865 | 99.6094 | 99.6552 |
| $c'_7 = c_7 + 10^{-14}$ | 99.6246 | 99.5911 | 99.6429 |
| $c'_8 = c_8 + 10^{-14}$ | 99.6247 | 99.6262 | 99.6201 |
| $e' = e + 10^{-14}$ | 99.6033 | 99.6048 | 99.5804 |
| $\mu' = \mu+10^{-14}$ | 99.6414 | 99.5987 | 99.6170 |
| Avg. of all | 99.6114 | 99.6137 | 99.6124 |

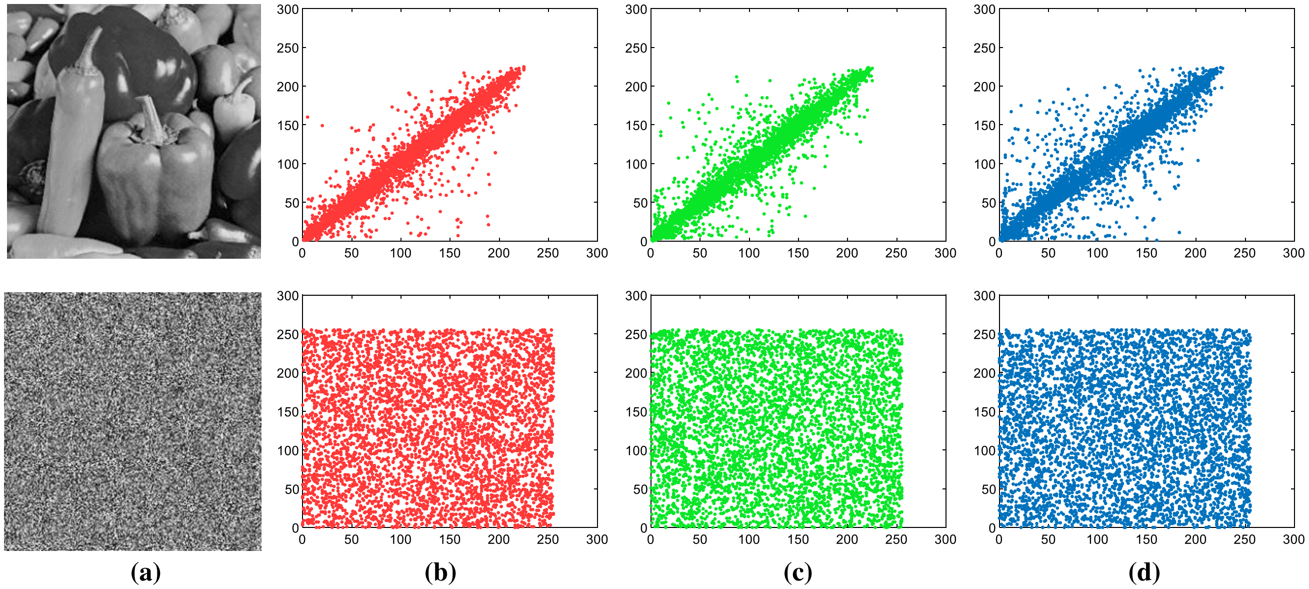


**Fig. 12** Correlation: **a** Pepper; **b** Horizontal correlation; **c** Vertical correlation; **d** Diagonal correlation

**Table 2** Correlation

| Image | Size | Plain image | | | Cipher image | | |
|---|---|---|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| 5.1.09 | 256 × 256 | 0.9041 | 0.9401 | 0.9081 | −0.0199 | 0.0114 | −0.0217 |
| 5.1.10 | 256 × 256 | 0.9050 | 0.8442 | 0.8081 | −0.0013 | −0.0102 | −0.0097 |
| 5.2.08 | 512 × 512 | 0.9282 | 0.9019 | 0.8707 | 0.0008 | −0.0326 | 0.0126 |
| 5.2.09 | 512 × 512 | 0.9063 | 0.8666 | 0.8199 | −0.0135 | 0.0102 | −0.0016 |
| 5.2.10 | 512 × 512 | 0.9354 | 0.9249 | 0.8904 | 0.0053 | −0.0005 | 0.0039 |
| 5.3.01 | 1024 × 1024 | 0.9786 | 0.9803 | 0.9672 | 0.0210 | −0.0047 | 0.0057 |
| 5.3.02 | 1024 × 1024 | 0.9080 | 0.9074 | 0.8563 | −0.0142 | −0.0005 | −0.0157 |
| 7.1.01 | 512 × 512 | 0.9610 | 0.9198 | 0.9046 | 0.0278 | −0.0150 | 0.0056 |
| 7.1.02 | 512 × 512 | 0.9486 | 0.9408 | 0.8968 | −0.0092 | −0.0126 | −0.0129 |
| 7.1.03 | 512 × 512 | 0.9474 | 0.9317 | 0.9034 | 0.0090 | 0.0158 | −0.0043 |
| 7.1.04 | 512 × 512 | 0.9789 | 0.9702 | 0.9605 | 0.0043 | −0.0052 | 0.0027 |
| 7.1.05 | 512 × 512 | 0.9446 | 0.9093 | 0.8946 | −0.0054 | −0.0074 | −0.0077 |
| 7.1.06 | 512 × 512 | 0.9399 | 0.9124 | 0.8955 | 0.0019 | 0.0041 | −0.0089 |
| Lena | 256 × 256 | 0.9433 | 0.9666 | 0.9186 | 0.0130 | 0.0141 | −0.0258 |
| Pepper | 256 × 256 | 0.9575 | 0.9639 | 0.9338 | 0.0069 | 0.0259 | −0.0060 |
| House | 256 × 256 | 0.9698 | 0.9717 | 0.9474 | −0.0209 | 0.0176 | −0.0168 |
| Avg. of all | – | – | – | – | 0.00035 | 0.00065 | −0.00063 |
| Ref. (Liu et al. 2021) | – | – | – | – | 0.00306 | 0.00369 | 0.00361 |
| Ref. (Riyahi et al. 2021) | – | – | – | – | 0.0019 | 0.0017 | 0.0041 |
| Ref. (Wang et al. 2020) | – | – | – | – | 0.0022 | −0.0020 | 0.0018 |
| Ref. (Xiong et al. 2022) | – | – | – | – | −0.0059 | 0.0013 | 0.0003 |
| Ref. (Ding et al. 2022) | – | – | – | – | 0.0020 | −0.0046 | 0.0029 |

**Table 3** Information entropy

| Image (256 × 256) | Proposed | Ref. (Wang and Gao 2020) | Ref. (Wang and Zhao 2021) |
|---|---|---|---|
| Lena | 7.9975 | 7.9874 | 7.9939 |
| Pepper | 7.9976 | 7.9780 | 7.9972 |
| Plane | 7.9973 | 7.9860 | 7.9973 |
| Black | 7.9974 | – | 7.9976 |

**Table 4** Comparison of information entropy

| Image (256 × 256) | Avg. of all |
|---|---|
| Ref. (Es-Sabry et al. 2020) | 7.9963 |
| Ref. (Shafique 2022) | 7.9971 |
| Ref. (Gan et al. 2019) | 7.9973 |
| Proposed | 7.9976 |

$$\mathrm{NPCR} = \frac{\sum_{i,j} E(i,j)}{M \times N} \times 100\% \tag{17}$$

$$E(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{V} \tag{19}$$

**Table 5** NPCR evaluation

| File name | NPCR | | | | |
|---|---|---|---|---|---|
| | Ref. (Riyahi et al. 2021) | Ref. (Himeur and Boukabou 2018) | Ref. (Alawida et al. 2019) | Ref. (Mansouri and Wang 2021b) | Proposed |
| 256 × 256 | $N_\alpha^* \geq 99.5693\%$ | | | | |
| 5.1.09 | 99.62 | 99.5124 | 99.603 | 99.6048 | 99.6231 |
| 5.1.10 | 99.61 | 99.6121 | 99.636 | 99.6559 | 99.6094 |
| 5.1.11 | 99.64 | 99.5943 | 99.942 | 99.6394 | 99.6292 |
| 5.1.12 | 99.62 | 99.5811 | 99.792 | 99.6484 | 99.6231 |
| 5.1.13 | 99.61 | 99.5963 | 99.792 | 99.5808 | 99.6277 |
| 5.1.14 | 99.61 | 99.5945 | 99.621 | 99.6244 | 99.6063 |
| 512 × 512 | $N_\alpha^* \geq 99.5893\%$ | | | | |
| 5.2.08 | 99.59 | 99.5878 | 99.960 | 99.6093 | 99.6132 |
| 5.2.09 | 99.61 | 99.5812 | 99.876 | 99.6161 | 99.6086 |
| 5.2.10 | – | 99.6100 | 99.654 | 99.6139 | 99.6120 |
| 7.1.01 | 99.62 | 99.6028 | 99.957 | 99.5923 | 99.6239 |
| 7.1.02 | 99.61 | 99.6078 | 99.918 | 99.5999 | 99.6243 |
| 7.1.03 | 99.61 | 99.5811 | 99.849 | 99.6127 | 99.5949 |
| 7.1.04 | 99.60 | 99.5946 | 99.991 | 99.6044 | 99.6078 |
| 7.1.05 | 99.61 | 99.5937 | 99.942 | 99.5915 | 99.6197 |
| 7.1.06 | 99.59 | 99.5913 | 99.670 | 99.6230 | 99.5907 |
| 7.1.07 | 99.61 | 99.6014 | 99.983 | 99.5938 | 99.6136 |
| boat.512 | 99.60 | 99.6101 | 99.715 | 99.5961 | 99.6082 |
| gray21.512 | – | 99.6034 | 99.643 | 99.6052 | 99.6174 |
| ruler.512 | 99.62 | 99.5945 | 99.637 | 99.6067 | 99.6391 |
| 1024 × 1024 | $N_\alpha^* \geq 99.5994\%$ | | | | |
| 5.3.01 | 99.61 | 99.5931 | 99.950 | 99.6119 | 99.6094 |
| 5.3.02 | 99.61 | 99.6128 | 99.982 | 99.6124 | 99.6143 |
| 7.2.01 | – | 99.6156 | 99.980 | 99.6079 | 99.6060 |
| Mean | 99.6105 | 99.6088 | 99.8224 | 99.6119 | 99.6146 |
| Std | 0.01129 | 0.01479 | 0.14706 | 0.01730 | 0.01131 |
| Pass/All | 19/19 | 18/22 | 22/22 | 22/22 | 22/22 |

**Table 6** UACI evaluation

| File name | UACI | | | | |
|---|---|---|---|---|---|
| | Ref. (Riyahi et al. 2021) | Ref. (Himeur and Boukabou 2018) | Ref. (Alawida et al. 2019) | Ref. (Mansouri and Wang 2021b) | Proposed |
| 256 × 256 | $U_\alpha^{*-}$=33.2824%, $U_\alpha^{*+}$=33.6447% | | | | |
| 5.1.09 | 33.46 | 33.5214 | 33.552 | 33.3625 | 33.4941 |
| 5.1.10 | 33.45 | 33.4215 | 33.453 | 33.3902 | 33.4022 |
| 5.1.11 | 33.46 | 33.4014 | 33.586 | 33.4063 | 33.4251 |
| 5.1.12 | 33.44 | 33.4158 | 33.453 | 33.4420 | 33.4403 |
| 5.1.13 | 33.42 | 33.4236 | 33.520 | 33.3664 | 33.4870 |
| 5.1.14 | 33.47 | 33.3951 | 33.440 | 33.3671 | 33.4386 |
| 512 × 512 | $U_\alpha^{*-}$=33.3730%, $U_\alpha^{*+}$=33.5541% | | | | |
| 5.2.08 | 33.46 | 33.3978 | 33.692 | 33.3765 | 33.4914 |
| 5.2.09 | 33.45 | 33.4182 | 33.548 | 33.4688 | 33.4458 |
| 5.2.10 | – | 33.4263 | 33.454 | 33.4527 | 33.4222 |
| 7.1.01 | 33.46 | 33.4474 | 33.648 | 33.4610 | 33.4336 |
| 7.1.02 | 33.44 | 33.4326 | 33.465 | 33.5514 | 33.5150 |
| 7.1.03 | 33.42 | 33.4836 | 33.273 | 33.4992 | 33.4435 |
| 7.1.04 | 33.46 | 33.4782 | 33.202 | 33.4768 | 33.4129 |
| 7.1.05 | 33.48 | 33.4716 | 33.830 | 33.4172 | 33.4698 |
| 7.1.06 | 33.47 | 33.4365 | 33.627 | 33.4495 | 33.4078 |
| 7.1.07 | 33.47 | 33.4313 | 33.609 | 33.5062 | 33.4440 |
| boat.512 | 33.45 | 33.3973 | 33.374 | 33.4079 | 33.4285 |
| gray21.512 | – | 33.4089 | 33.507 | 33.4522 | 33.4940 |
| ruler.512 | 33.44 | 33.4635 | 33.415 | 33.4252 | 33.4168 |
| 1024 × 1024 | $U_\alpha^{*-}$ = 33.4183%, $U_\alpha^{*+}$=33.5088% | | | | |
| 5.3.01 | 33.45 | 33.4392 | 33.508 | 33.4263 | 33.4876 |
| 5.3.02 | 33.47 | 33.4547 | 33.514 | 33.4765 | 33.4871 |
| 7.2.01 | – | 33.4301 | 33.487 | 33.4910 | 33.4559 |
| Mean | 33.4536 | 33.4362 | 33.5071 | 33.4449 | 33.5196 |
| Std | 0.01640 | 0.03212 | 0.13498 | 0.05387 | 0.03425 |
| Pass/All | 19/19 | 22/22 | 14/22 | 22/22 | 22/22 |

where $V$ represents the maximum supported pixel value of ciphertext image, and $V = 255$ in this paper.

$N_\alpha^*$ is the minimum critical value to judge whether NPCR passes the test, $U_\alpha^{*+}$ and $U_\alpha^{*-}$ are the upper and lower bounds to judge whether UACI passes the test (Wu et al. 2011). The definition is as Eq. (20) and Eq. (21).

$$N_\alpha^* = \frac{V - \Phi^{-1}(\alpha)\sqrt{V/MN}}{V+1} \tag{20}$$

$$\begin{cases} U_\alpha^{*-} = \dfrac{V+2}{3V+3} - \Phi^{-1}(\alpha/2) \times \sqrt{\dfrac{(V+2)(V^2+2V+3)}{18(V+1)^2 \times V \times MN}} \\ U_\alpha^{*+} = \dfrac{V+2}{3V+3} + \Phi^{-1}(\alpha/2) \times \sqrt{\dfrac{(V+2)(V^2+2V+3)}{18(V+1)^2 \times V \times MN}} \end{cases} \tag{21}$$

Table 5 shows the experimental results and comparison results. The mean values of NPCR and UACI are 99.6146 and 33.5196%, respectively, and the standard deviations are 0.01131 and 0.03425, respectively. Compared with the other three algorithms proposed in Ref. (Riyahi et al. 2021), Ref. (Himeur and Boukabou 2018), Ref. (Alawida et al. 2019) and Ref. (Mansouri and Wang 2021b), the average value, standard deviation and pass rate of the proposed algorithm are improved (Table 6).

## 4.6 Robustness analysis

Image encryption algorithm should not only ensure that useful information cannot be obtained from the encrypted image, but also ensure the robustness of anti-interference in transmission. This section simulates two ways of clipping attack and noise attack. As can be seen from Fig. 13, the

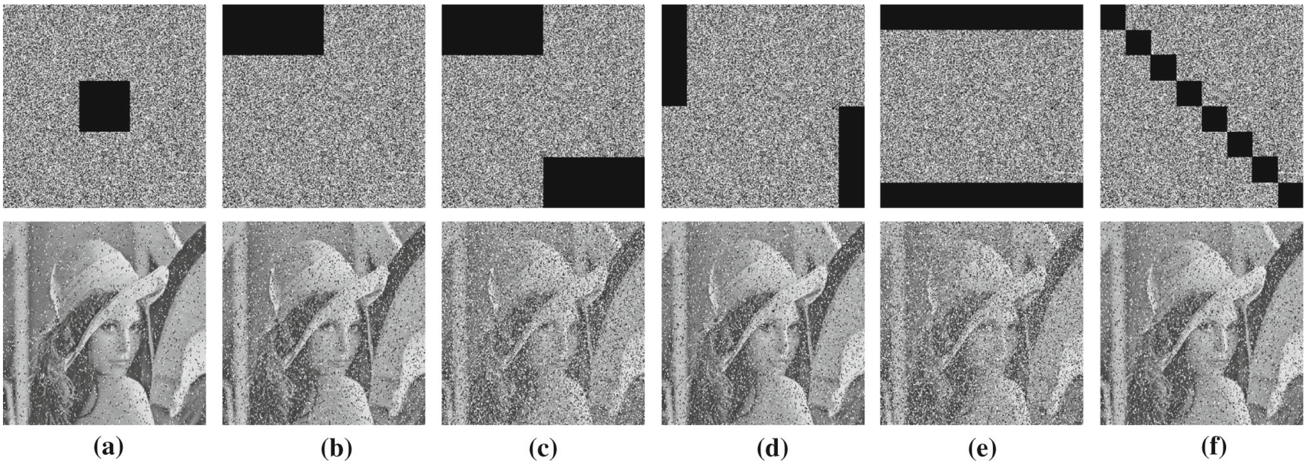


**Fig. 13** Clipping attack: **a** Center clipping; **b** 1/8-degree clipping; **c** 1/4-degree clipping; **d** 1/16-degree edge clipping; **e** 1/8-degree edge clipping; **f** Diagonal clipping

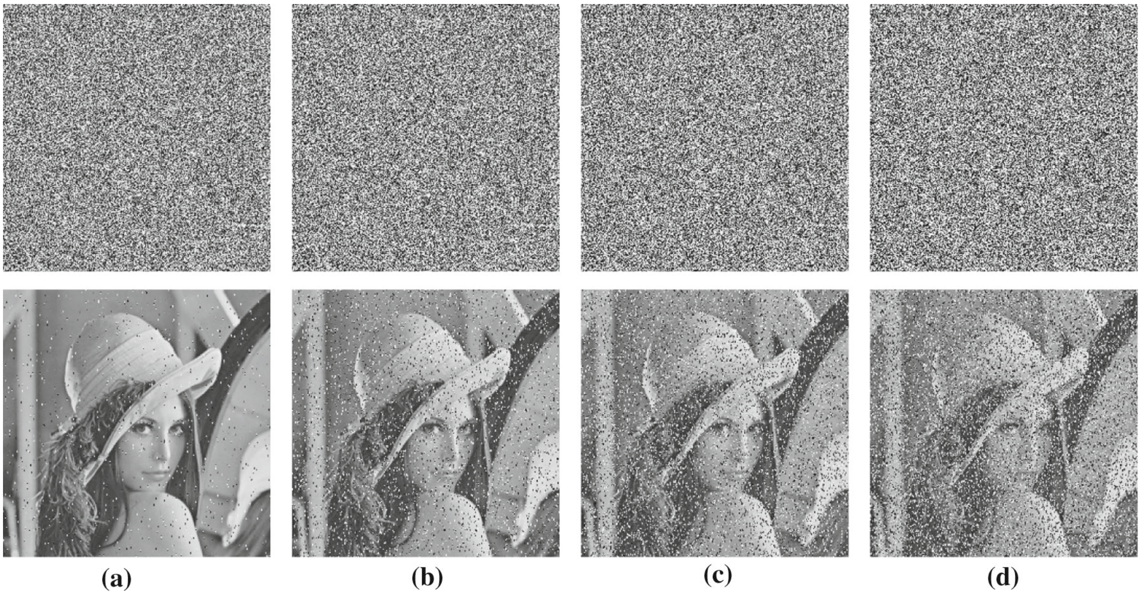


**Fig. 14** Noise attack: **a** 1% intensity noise; **b** 5% intensity noise; **c** 10% intensity noise; **d** 15% intensity noise

**Table 7** Complexity analysis

| Ref | Complexity |
|---|---|
| Wang et al. 2021b) | O(IT + 26MN + M + 8 N) |
| Belazi et al. 2022) | O(*61MN + 3 M + 3 N)* |
| Proposed | O(500 + 8MN) |

image is decrypted after center clipping, 1/8-degree clipping, 1/4-degree clipping, edge clipping and diagonal clipping. After clipping from different angles, the decrypted image can be visually distinguished, and most of the information can still be obtained. Figure 14a–d shows salt & pepper noise with density of 1, 5, 10 and 15% and its decrypted image, respectively. Although there is some noise in the decrypted image, the content can still be visually distinguished. Therefore, the algorithm has certain anti-interference ability, strong robustness, and can resist attacks such as clipping and noise attacks.

## 4.7 Computational complexity analysis

For this algorithm, the time complexity mainly comes from three parts: chaotic system, confusion and diffusion. The time complexity of iterative NPDCML system is O(500 + MN), the complexity of linear diffusion is O(*MN*), and the complexity of bit-plane encryption is

**Table 8** Time test results (Unit: s)

| Image size | Ref. (Wang and Zhao 2021) | Ref. (Chai et al. 2022) | Proposed |
|---|---|---|---|
| Encryption | 1.431 | 1.745 | 1.384 |
| Decryption | 1.633 | 7.101 | 1.628 |

O(5MN + MN). Therefore, the overall time complexity is O(500 + 8MN). In Ref. (Wang et al. 2021b), the image encryption algorithm based on the spatiotemporal chaos model is also used. As a comparison, the time complexity of the algorithm is O(IT + 26MN + M + 8 N), and the efficiency is less than that of the algorithm in this paper under the same size image. A comparison is made in Table 7.

Similarly, we also compare the encryption time in seconds, and the test results are given in Table 8. Under the same size 512 × 512, the encryption time of this algorithm is also low.

## 5 Conclusion

In this paper, a dynamic coupled map lattice with nonlinear perturbations (NPDCML) is proposed. The nonlinear lattice is used to perturb the linear coupled lattice, and the coupling coefficient is promoted to a dynamic function. Through several index tests, it is proved that the NPDCML system has a wider chaotic range and better characteristics. At the same time, an image encryption algorithm based on NPDCML is proposed, which supports gray, binary and color images of various sizes. The algorithm is very sensitive to secret key, has lower time complexity and higher security. Through correlation, information entropy, differential attack analysis and robustness test, it is proved that the algorithm is safe and feasible. At the same time, it is proved that NPDCML has good pseudo-randomness, large parameter space and other excellent cryptographic properties.

In the future work, we will continue to further optimize spatiotemporal chaos models, including one-dimensional or two-dimensional CML models, so as to exchange lower complexity for better performance. At the same time, it is committed to optimizing the privacy protection of key information (such as face) in image encryption algorithms and improving the security and robustness of the algorithms.

**Acknowledgements** This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), Jinan City '20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031), Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (No: MIMS20-M-02).

**Funding** This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), Jinan City '20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031), Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (No: MIMS20-M-02).

**Data availability** Enquiries about data availability should be directed to the authors.

## Declarations

**Conflict of interest** The authors declared that they have no conflicts of interest to this work.

## References

Alawida M, Teh JS, Samsudin A, Alshoura WH (2019) An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Process 164:249–266

Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifur Chaos 16(8):2129–2151

Anand A, de Veciana G, Shakkottai S (2020) Joint Scheduling of URLLC and eMBB traffic in 5G wireless networks. IEEE/ACM Trans Netw 28(2):477–490

Belazi A, El-Latif AAA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170

Belazi A, Kharbech S, Aslam MN, Talha M, Xiang W, Iliyasu AM, AbdEl-Latif AA (2022) Improved Sine-Tangent chaotic map with application in medical images encryption. J Inf Secur Appl 66:103131

Chai XL, Fu JY, Gan ZH, Lu Y, Zhang YS (2022) An image encryption scheme based on multi-objective optimization and block compressed sensing. Nonlinear Dyn 108:2671–2704

Ding Y, Duan ZK, Li SR (2022) 2D arcsine and sine combined logistic map for image encryption. Vis Comput. https://doi.org/10.1007/s00371-022-02426-0

Es-Sabry M, El Akkad N, Merras M, Saaidi A, Satori K (2020) A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators. Soft Comput 24:3829–3848

Gan ZH, Chai XL, Han DJ, Chen YR (2019) A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Comput Appl 31:7111–7130

Himeur Y, Boukabou A (2018) A robust and secure key-frames based video watermarking system using chaotic encryption. Multimed Tools Appl 77(7):8603–8627

Hu GZ, Li BB (2021) A uniform chaotic system with extended parameter range for image encryption. Nonlinear Dyn 103:2819–2840

Kaneko K (1989) Pattern dynamics in spatiotemporal chaos: Pattern selection, diffusion of defect and pattern competition intermittency. Phys D 34(1–2):1–41

Khan M, Masood F, Alghafis A (2020) Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. Neural Comput Appl 32(15):11837–11857

Khellat F, Ghaderi A, Vasegh N (2011) Li-Yorke chaos and synchronous chaos in a globally nonlocal coupled map lattice. Chaos Solitons Fractals 44(11):934–939

Liu H, Wang X, Kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466

Liu JY, Wang Y, Liu Z, Zhu H (2021) A chaotic image encryption algorithm based on coupled piecewise sine map and sensitive diffusion structure. Nonlinear Dyn 104:4615–4633

Ma B, Chang LL, Wang CP, Li J, Wang XY, Shi YQ (2020) Robust image watermarking using invariant accurate polar harmonic Fourier moments and chaotic mapping. Signal Process 172:107544

Mansouri A, Wang XY (2021a) Image encryption using shuffled Arnold map and multiple values manipulations. Vis Comput 37(1):189–200

Mansouri A, Wang XY (2021b) A novel block-based image encryption scheme using a new Sine powered chaotic map generator. Multimed Tools Appl 80:21955–21978

Meherzi S, Marcos S, Belghith S (2006) A new spatiotemporal chaotic system with advantageous synchronization and unpredictability features. System, 147–150

Qu G, Meng XF, Yin YK, Wu HZ, Yang XL, Peng X, Wenqi H (2021) Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation. Optic Lasers Eng 137:106392

Quan Y, Teng H, Chen Y, Ji H (2020) Watermarking deep neural networks in image processing. IEEE Trans Neural Netw Learn Syst 32(5):1852–1865

Riyahi M, Kuchaki Rafsanjani M, Motevalli R (2021) A novel image encryption scheme based on multi-directional diffusion technique and integrated chaotic map. Neural Comput Appl. https://doi.org/10.1007/s00521-021-06077-5

Shafique A (2022) A noise-tolerant cryptosystem based on the decomposition of bit-planes and the analysis of chaotic gauss iterated map. Neural Comput Appl. https://doi.org/10.1007/s00521-022-07327-w

Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715

Shen CW, Yu SM, Lü JH, Chen GR (2014) Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model. IEEE Trans Circuit Syst I 61(8):2380–2389

Shevchenko II (2014) Lyapunov exponents in resonance multiplets. Phys Lett A 378(1–2):34–42

Su YN, Wang XY (2022) A robust visual image encryption scheme based on controlled quantum walks. Phys A 587:126529

Wang XY, Du XH (2022) Pixel-level and bit-level image encryption method based on Logistic-Chebyshev dynamic coupled map lattices. Chaos Solitons Fractals 155:111629

Wang XY, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539:195–214

Wang XY, Yang JJ (2021) Spatiotemporal chaos in multiple coupled mapping lattices with multi-dynamic coupling coefficient and its application in color image encryption. Chaos Solitons Fractals 147:110970

Wang XY, Zhao MC (2021) An image encryption algorithm based on hyperchaotic system and DNA coding. Opt Laser Technol 143:107316

Wang J, Liu WY, Zhang S (2020) Adaptive encryption of digital images based on lifting wavelet optimization. Multimed Tools Appl 79:9363–9386

Wang XY, Liu C, Jiang DH (2021a) A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf Sci 574:505–527

Wang MX, Wang XY, Zhao TT, Zhang C, Xia ZQ, Yao NM (2021b) Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme. Inf Sci 544:1–24

Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber J Multidiscip J Sci Technol J Sel Areas Telecommun 1(2):31–38

Xian YJ, Wang XY (2021) Fractal sorting matrix and its application on chaotic image encryption. Inf Sci 547:1154–1169

Xian YJ, Wang XY, Teng L (2021) Double parameters fractal sorting matrix and its application in image encryption. IEEE Trans Circuits Syst Video Technol. https://doi.org/10.1109/TCSVT.2021.3108767

Xiong L, Yang FF, Mou J, An XL, Zhang XG (2022) A memristive system and its applications in red–blue 3D glasses and image encryption algorithm with DNA variation. Nonlinear Dyn 107:2911–2933

Xu WW, Zhang H, Cao XH, Deng RL, Li HR, Zhang J (2021) Securing wireless relaying communication for dual unmanned aerial vehicles with unknown eavesdropper. Inf Sci 546:871–882

Zhang Y (2015) Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik 126(2):223–229

Zhang YQ, Wang XY (2013) Spatiotemporal chaos in Arnold coupled logistic map lattice. Nonlinear Anal Model Control 18(4):526–541

Zhang YQ, Wang XY (2014) Spatiotemporal chaos in mixed linear-nonlinear coupled logistic map lattice. Phys A 402:104–118

Zhang Q, Ling G, Wei XP (2013) A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik 124(18):3596–3600

Zhang YS, Wen WY, Su MT, Li M (2014) Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik 125(4):1562–1564

Zou CY, Wang XY, Li HF, Wang YZ (2020) Enhancing the kinetic complexity of 2-D digital coupled chaotic lattice. Nonlinear Dyn 102:2925–2943

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