Neural Computing and Applications (2020) 32:247–260
https://doi.org/10.1007/s00521-018-3577-z

ORIGINAL ARTICLE

A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system

Yi He[1] · Ying-Qian Zhang[2] · Xing-Yuan Wang[3,4]

Received: 3 October 2017 / Accepted: 30 May 2018 / Published online: 1 August 2018

Abstract
In this paper, a new image encryption algorithm based on the two-dimensional spatiotemporal chaotic system is proposed.This system mixes linear neighborhood coupling and the nonlinear chaotic map coupling of lattices, and it has more cryptographic features in dynamics than the system of coupled map lattices does. The two-dimensional coupled map lattices (2DCML) system is only a special case in this chaotic system. In addition, bit-level permutation is employed to strengthen security of the cryptosystem. Simulations have been carried out, and the results demonstrate that the proposed algorithm has properties of large key space, high sensitivity to key, strong resisting attack. So, it is more secure and effective algorithm for encryption of digital images.

Keywords Spatiotemporal chaos · Coupled map lattices · Bit-level · Image encryption

1 Introduction

In recent years, a variety of chaos-based digital image encryption algorithms have been investigated [1–27, 29–31, 35, 37–40]. Spatiotemporal chaotic system is gradually regarded with better properties suitable for image encryption than one-dimensional chaotic system, such as larger parameter space, better randomness and more chaotic sequences [10–27, 35, 37–40]. Then, many researches [13–27, 34, 35] are based on the system of coupled map lattices (CML) [26, 27], which enhances the security of the encryption algorithms. Seyedzadeh et al. [13] proposed a novel image encryption algorithm based on the two-dimensional logistic map and the quantum chaotic map, which are independently coupled with nearest-neighboring coupled map lattices. Wang et al. [14] proposed an encryption algorithm for images using CML and DNA sequence operations. However, the CML system is coupled by adjacent lattices, and the parameter μ still has periodic windows in the bifurcation diagram of some lattice. Due to the adjacent coupling between lattices, parameters $\mu \in (3.87, 3.925)$ and $\varepsilon = 0.1$ can only generate local chaotic behavior of the CML system [27], which implies some of the lattices are not in chaotic behavior. The lattice should be selected carefully for image encryption because such space regular coupling of the adjacent coupling in the CML system is a linear coupling in space.

Many studies [15–18] concentrated on dynamically random links for coupling. Sinha [15] proposed the random coupling of spatiotemporal system which initiated the study of the non-neighborhood coupling in coupled map lattices. Mondal et al. [16] presented the enhancement spatiotemporal regularity by rapidly switched random links. Nag et al. [18] presented the synchronization behavior of delay-coupled chaotic smooth unmoral maps with stochastic switching of links at every time step. However, the chaotic sequences in such systems of

✉ Ying-Qian Zhang
zhangyq@dlut.edu.cn

Yi He
heyi517@dlut.edu.cn

Xing-Yuan Wang
wangxy@dlut.edu.cn

[1] City Institute, Dalian University of Technology, Dalian 116600, China

[2] School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China

[3] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

[4] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116034, China

randomness-based coupling cannot be reproduced at the second time in the same parameters, which are not suitable for applying in cryptography.

The NCML and MLNCML systems [19, 20] presented nonlinear chaotic map coupling method to achieve the non-neighborhood coupling based on one-dimensional CML. However, a two-dimensional coupled map lattice allows a more precise description of the real nature phenomena than the one-dimensional case. To the best of our knowledge, very little work was done to adapt this coupling to evaluate two-dimensional coupled map lattices. In this paper, we discover the new features of spatiotemporal chaotic systems in spatial mixed coupling with the two-dimensional CML. Furthermore, this system is also evaluated for the feasibility of the image encryption application for its superior features in dynamics.

A variety of image encryption algorithms using bit-level permutation have been investigated, which can change the position and value of a pixel simultaneously [28–33, 35, 36]. In [32], Praveenkumar et al. proposed a novel image encryption approach with chaotic sequences which are generated for each bit plane. All pixels of an image are separated into groups of bits by information of different bit planes in Zhu's scheme [29]. However, the bits in one-bit plane cannot be permuted into other bit planes in these algorithms. Therefore, the statistical information in each bit plane remains unmodified.

In this paper, we employ the two-dimensional spatiotemporal chaotic system which mixed linear–nonlinear coupled map lattices for the diffusion in the image encryption. The two-dimensional mixed system employing the spatial nonlinear coupling can generate better pseudo-random sequences than that employing adjacent coupling. The mixed system also contains the new features such as less periodic windows in bifurcations and larger range of parameters in chaotic dynamics. For the permutation phase, we employ the Arnold cat map for bit-level permutation. Furthermore, the wide range of choices for the initial conditions and control parameters lead to a large key space. The experimental results show the effectiveness of the proposed image encryption algorithm.

The remainder of this paper is organized as follows. In Sect. 2, the proposed spatiotemporal chaotic system based on two-dimensional CML is presented. The proposed image encryption scheme is described in Sect. 3. Simulation results and performance analyses are reported in Sect. 4.

2 The proposed spatiotemporal chaotic system

The proposed spatiotemporal chaotic system based on two-dimensional CML can be represented by

$$\begin{aligned} x_{(n+1)}(i,j) &= (1-\varepsilon)f[x_n(i,j)] + (1-\eta)\frac{\varepsilon}{4}\{f[x_n(i-1,j)] \\ &\quad + f[x_n(i+1,j)] + f[x_n(i,j-1)] + f[x_n(i,j+1)]\} \\ &\quad + \eta\frac{\varepsilon}{4}\{f[x_n(a,j)] + f[x_n(b,j)] + f[x_n(i,c)] + f[x_n(i,d)]\}, \end{aligned} \tag{1}$$

where i, j, a, b, c, d are the lattices $(1 \le i,j,a,b,c,d \le L)$, ε is the coupling parameter $(0 \le \varepsilon \le 1)$, η is the coupling parameter $(0 \le \eta \le 1)$, n is the time index $(n = 1, 2, 3...)$ and $f(x) = \mu x(1-x)$, $\mu \in (0, 4]$. The relations of i, j, a, b, c, d are defined by the Arnold cat map described by

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i+1 \\ i-1 \end{bmatrix} (\text{mod } L), \tag{2}$$

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} j+1 \\ j-1 \end{bmatrix} (\text{mod } L), \tag{3}$$

where p and q are the parameters of Arnold cat map.

The parameters p, q and η make the proposed system into diverse dynamics systems. When selecting $\eta = 0$, Eq. (1) can be degenerated as the 2DCML system [26] as

$$\begin{aligned} x_{(n+1)}(i,j) &= (1-\varepsilon)f[x_n(i,j)] + \frac{\varepsilon}{4}\{f[x_n(i-1,j)] \\ &\quad + f[x_n(i+1,j)] + f[x_n(i,j-1)] + f[x_n(i,j+1)]\}. \end{aligned} \tag{4}$$

The bifurcation diagram without periodic windows in the proposed system is the new feature for cryptography. The CML system is regarded as a suitable spatiotemporal chaotic system for cryptography partially because of its less periodic windows than low-dimension chaotic map. Thus, the proposed system is more suitable for cryptography for the same reason. The parameter as a secret key has a larger key space than logistic map or the CML system. Besides, the parameter can be designed as one of the secret keys.

Without loss of generality, the proposed system assigns the same $L = 100$ as the CML system does [26]. Figure 1b–e indicates that the periodic windows are reduced compared with the 2DCML system in Fig. 1a when increasing the parameter η. When increasing the value of η, the number of bifurcation points is varying larger and the gaps between bifurcation points are varying closer. Due to the nonlinear coupling leading to the instability of the possible periods of orbits, the times of period doubling bifurcations is misled and unobvious. Therefore, periodic windows are reduced and when increasing the value of the parameter η, the nonlinear coupling is strengthened and periodic windows are vanished eventually. The nonlinear coupling decreases the times of period doubling bifurcations, and the proposed system becomes chaotic after a point.

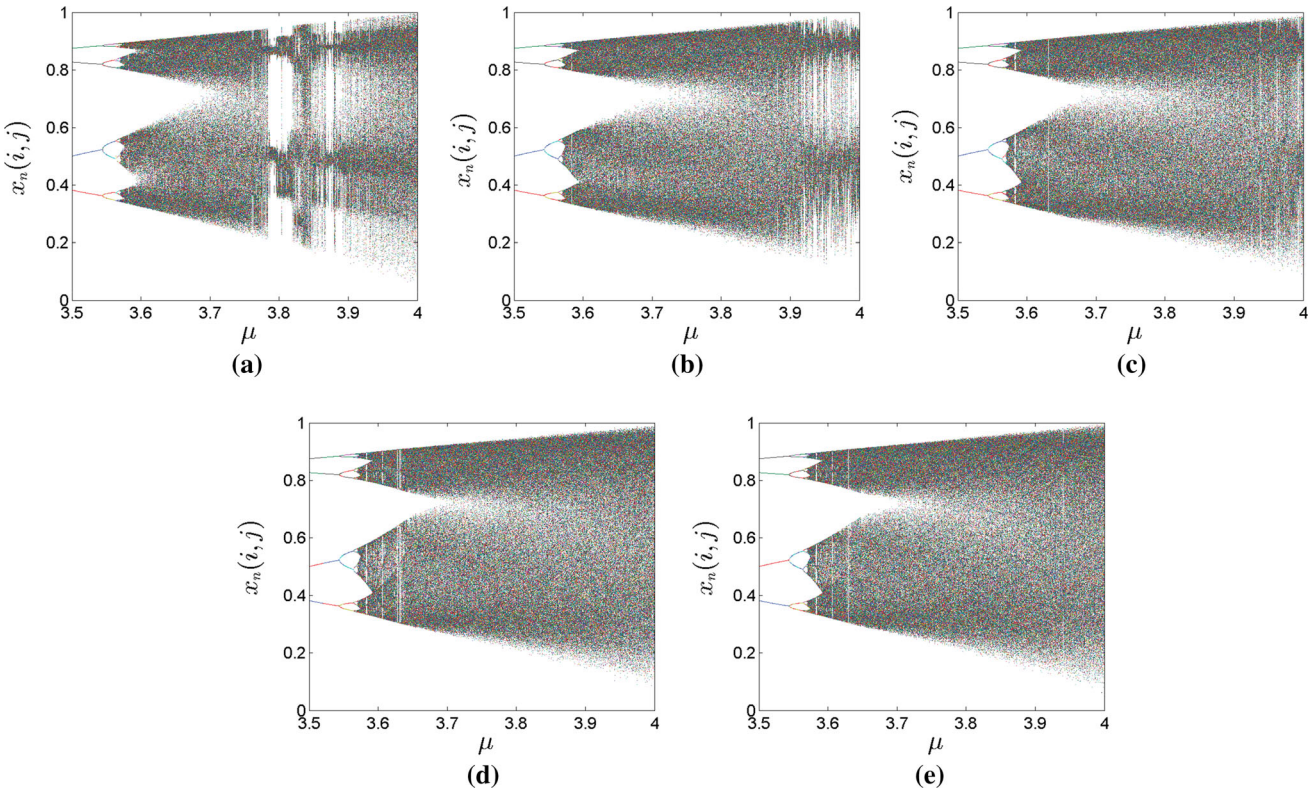


Fig. 1 Bifurcation diagrams when $\mu \in [3.5, 4.0]$. **a** The 2DCML system, **b** The proposed system ($\eta = 0.3$), **c** The proposed system ($\eta = 0.5$), **d** The proposed system ($\eta = 0.7$), **e** The proposed system ($\eta = 0.9$)

Any system holding chaotic behavior presented at least one positive Lyapunov exponent. The proposed system can be considered as L dimensions dynamics; the Kolmogorov-Sinai entropy density h of the L dimensions dynamics is average of positive Lyapunov exponents [34]. When $\eta = 0.3$, Fig. 2b shows that there are only two valleys at $3.6 < \mu < 3.8$ and $\varepsilon = 0.1$, $3.6 < \mu < 3.8$ and $\varepsilon = 0.2$ in the proposed system while the 2DCML system has three valleys at $3.6 < \mu < 3.8$ and $\varepsilon = 0.1$, $3.6 < \mu < 3.8$ and $\varepsilon = 0.2$, $3.6 < \mu < 3.8$ and $\varepsilon = 0.6$, which are shown in Fig. 2a. Therefore, the proposed system characterizes stronger chaotic behaviors at the range of $3.6 < \mu < 3.8$ and $\varepsilon = 0.6$ than the 2DCML system. During increasing the value of η, Fig. 2b–e indicates that the proposed system has higher Kolmogorov-Sinai entropy density than the 2DCML system [26] and the MLNCML system [19] do, which is shown in Fig. 2a, f.

Without loss of generality, we focus on the proposed system by assuming a grid of $L = 64$, $L \times L = 4096$ as the 2DCML system [26] assigned the same value. When the value of η increases, nonlinear coupling strengthens the diffusions between lattices harder than neighborhood coupling does. The local inhomogeneous trend becomes stronger, and the reactions dominate the system behavior. At the same time, the orderly trend of diffusion is obviously weakened because most of lattices are in chaos and turbulence. Figure 3a indicates that the same parameters μ and ε which lead the proposed system in fully turbulence can only lead the 2DCML system in defect turbulence pattern shown in Fig. 3b. Therefore, compared with the 2DCML system, the proposed system contains larger range of parameters for this pattern. Figure 4a, b indicates that the proposed system is chaos fully compared with the 2DCML.

3 The proposed image encryption algorithm

Firstly, the image is permuted by the Arnold cat map for bit-level permutation and then diffused by the chaotic sequences of the proposed system. The permutation and diffusion phases can be encrypted in many rounds for higher security.

3.1 Secret key formulation

The proposed algorithm process utilizes a more than 4000 bit-long secret key. The secret key is composed of: K, $\mu(\mu \in [3.87, 4])$, $\varepsilon(\varepsilon \in [0.1, 1])$, $\eta(\eta \in [0.5, 1])$. The secret key K includes 100 components denoted as $K = \{K(1,1),$

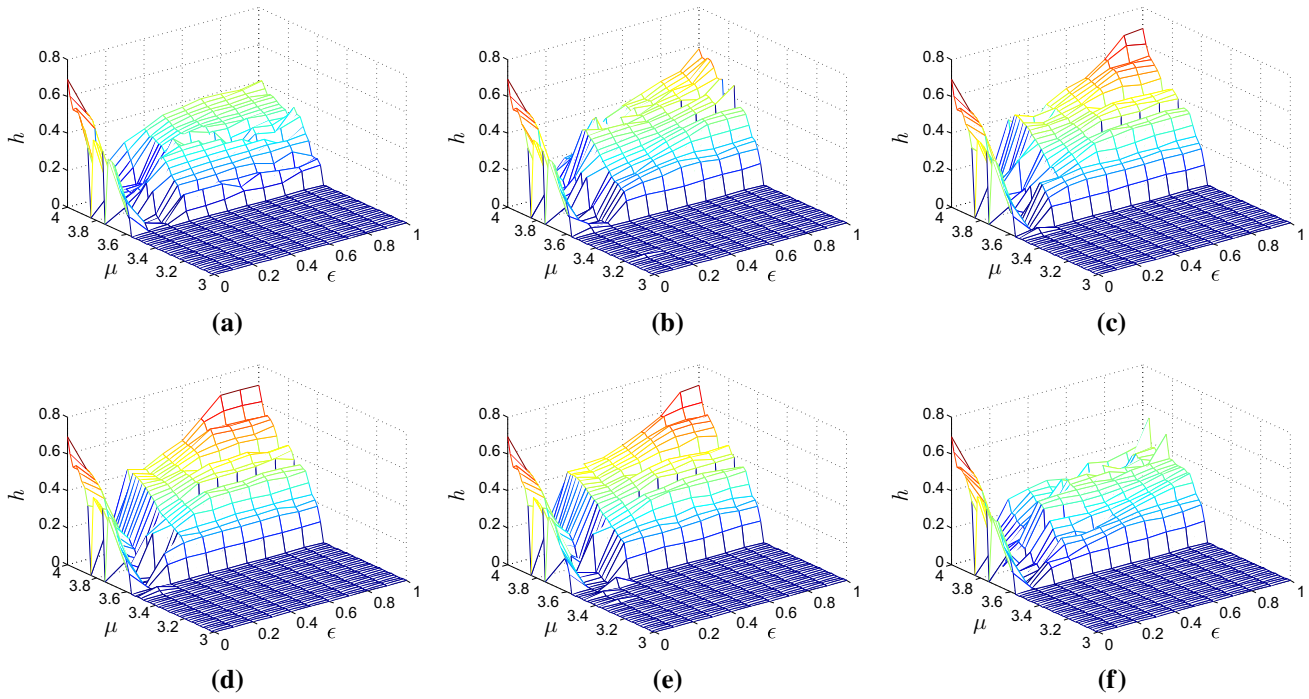


Fig. 2 Kolmogorov-Sinai entropy density for different parameters. **a** The 2DCML system, **b** The proposed system ($\eta = 0.3$), **c** The proposed system ($\eta = 0.5$), **d** The proposed system ($\eta = 0.7$), **e** The proposed system ($\eta = 0.9$), **f** The MLNCML system

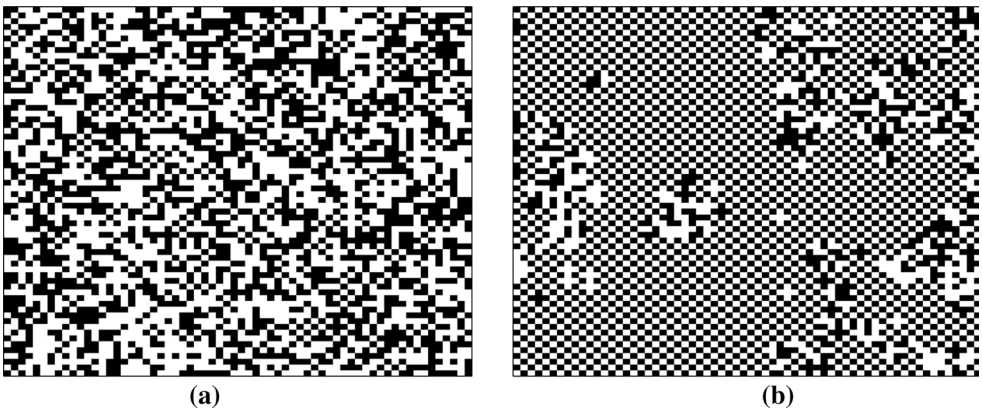


Fig. 3 Snapshot patterns for the proposed system and 2DCML when *times* = 1000. **a** The proposed system ($\mu = 3.93$, $\eta = 0.3$ and $\varepsilon = 0.1$), **b** The 2DCML system ($\mu = 3.93$ and $\varepsilon = 0.1$)

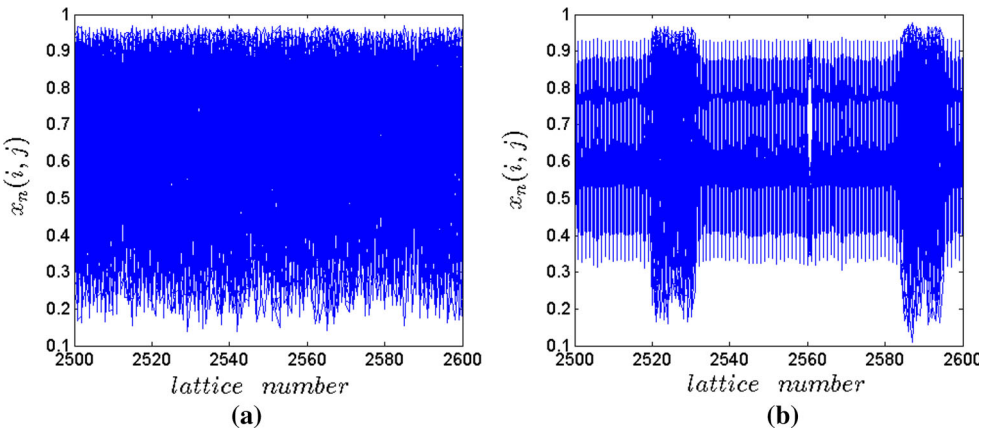


Fig. 4 Regular behaviors when $\mu = 3.93$. **a** The proposed system zoomed ($\mu = 3.93$, $\eta = 0.3$ and $\varepsilon = 0.1$), **b** The 2DCML system zoomed ($\mu = 3.93$ and $\varepsilon = 0.1$)

$K(1, 2)$, $K(1,3)\ldots$, $K(10,10)\}$ where each component of $K(i, j)$ is a 40-bit-long unit. The secret keys μ, ε and η refer to the parameters μ, ε and η in Eq. (1).

3.2 Permutation phase

Pixel-level confusion can only change the locations of the original pixels. For bit-level permutation, the situation is quite different. A pixel in a grayscale image usually consists of eight bits, but these bits carry different amount of information. For example, if the eight bits among the eight pixels are permuted, $2^7/255$ of the total information of each pixel is exchanged. In other words, 50.2% of the information of each pixel is changed if the eight bits of the pixels are permuted. Therefore, bit-level permutation not only modifies the pixel values but also exchanges the information of the pixels. A plain image with 256 gray levels can be extended to eight binary images, in which only two values (0 and 1) exist for each pixel [28, 29].

The plain image is firstly extended to bit plane, given by: $G(x, y) = Pic8Pic7Pic6...Pic1$, where $G(x, y)$ is the value of the pixel at coordinate (x, y) and the number in parentheses indicates the bit index from highest bit 8 to the lowest bit 1. A bit can contain different amounts of information depending on its position in the pixel. The highest eighth bit carries about 50% of the total information of the image. On the other hand, the lower three bits (third, second and first) carry less than 3% of the image information. In order to modify the statistical information in each bit plane, we reorganize binary images to two groups: $P1 = \{Pic8, Pic3, Pic2, Pic1\}$ and $P2 = \{Pic7, Pic6, Pic5, Pic4\}$ in which $P1$ carries about 13.2% of the image information and $P2$ carries about 11.8% of the total information of image. After the image is reorganized, the information distribution of the image is more balanced, which is more conducive to the encryption of the image. The binary images of Lena reorganized are shown in Fig. 5.

In permutation phase, Arnold cat map for bit-level permutations can be chosen in $P1$ and $P2$ by

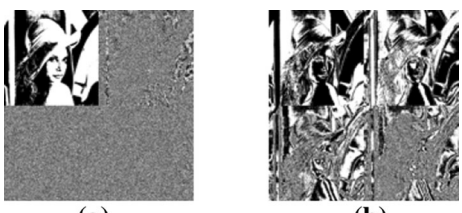


Fig. 5 Binary images reorganized. **a** $P1$, **b** $P2$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N \times 2) = \begin{bmatrix} 1 & v \\ w & vw+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N \times 2), \tag{5}$$

where (x, y) and (x', y') are the original bit position and permuted bit position, and v and w are calculated by

$$v = bin2dec(K(1,1) \oplus K(1,2) \oplus K(1,3) \oplus \cdots \oplus K(5,10)) \text{mod } N, \tag{6}$$

$$w = bin2dec(K(6,1) \oplus K(6,2) \oplus K(6,3) \oplus \cdots \oplus K(10,10)) \text{mod } N. \tag{7}$$

3.3 Diffusion phase

The proposed system in Eq. (1) is employed for the diffusion phase. The initial values $x_1(i,j)$ are calculated by

$$x_1(i,j) = bin2dec(K(i,j))/2^{40}, \tag{8}$$

where (i, j) is lattice index, $(i,j) \in [1, 10]$. The system contains 100 initial values, which contributes a large key space of $2^{4000} \approx 10^{1200}$. In addition, the parameter μ in the system can guarantee the whole system in chaotic behaviors when it varies from 3.8 to 4 continuously. However, the parameter μ in logistic map has periodic windows and a narrow value range for its corresponding chaotic behavior. The value of μ should be assigned very close to 4. Therefore, the system is superior to logistic map in cryptography.

The proposed system has better Lyapunov exponents than the 2DCML system, which indicates that each lattice can generate a chaotic sequence for encryptions when the parameter μ varies continuously. The 100 chaotic sequences in the corresponding lattices provide a sufficient amount of pseudo-random series for encryptions. Thus, the diffusion is designed by

$$c[m] = \{p[m] + c[m-1] + (x_{\text{step}+m}(i,j) \times 10^{10})\} \text{mod } 256, \tag{9}$$

where m is the pixel sequence which is formed vertically from the upper left corner to the lower right corner, $m \in [1, N \times N]$. The initial value $c[0]$ is 0; $x_{\text{step}+m}(i,j)$ is the chaotic sequence of the proposed system where the lattice index is i and j. The unfixed value i and j entirely depends on the secret key of K, which can enhance the sensitivity of the proposed algorithm for K and its security. The value step depends on the sum of pixels about original image, which can resist efficiently the chosen-plaintext attack. The values i, j and step are calculated by

$$i = 1 + v (\text{mod } 10), \tag{10}$$

$$j = 1 + w(\text{mod } 10), \tag{11}$$

$$\text{step} = 300 + \text{mod } (\text{sum}(\text{picture}), 100). \tag{12}$$

3.4 Encryption algorithm

Input: The secret keys where K is a 4000-bit-long block, $\mu(\mu \in [3.87, 4])$, $\eta(\eta \in [0.5, 1])$, $c[0](c[0] \in [0, 255])$ and $\varepsilon(\varepsilon \in [0.1, 1])$. The source image sp. The number of rounds of encryption.

Output: Returns ciphered image c.
Step 1. The variables of v and w are calculated in Eqs. (6) and (7) according to K.
Step 2. The source image sp is reorganized and arranged into the permuted image p with Eq. (5).
Step 3. The initial values $x_1(i,j)$ are calculated in Eq. (8).
Step 4. The 100 chaotic sequences in the proposed spatiotemporal chaotic system are calculated in Eq. (1).
Step 5. The permuted image p is encrypted into the ciphered image c in Eqs. (9), (10) (11) and (12) by using the above chaotic sequences. If the current round is not the final round of encryption, the above steps will repeat again. Otherwise, the encryption process completes.

3.5 Decryption algorithm

Input: The secret keys where K is a 4000-bit-long block, $\mu(\mu \in [3.87, 4])$, $\eta(\eta \in [0.5, 1])$, $c[0](c[0] \in [0, 255])$ and $\varepsilon(\varepsilon \in [0.1, 1])$. The ciphered image c. The number of rounds of decryption.

Output: Returns the recovery plaintext image sp.
Step 1. The initial values $x_1(i,j)$ are calculated in Eq. (8).
Step 2. The 100 chaotic sequences in the proposed spatiotemporal chaotic system are calculated in Eq. (1).
Step 3. The variables of v and w are calculated in Eqs. (6) and (7) according to K.
Step 4. The permuted image p is decrypted, and the corresponding equation is represented by

$$p[m] = \{c[m] - (x_{\text{step}+m}(i,j) \times 10^{10}) - c[m-1]\} \text{mod } 256. \tag{13}$$

Step 5. The plaintext image sp is decrypted by employing Arnold cat map. If the current round is not the final round of decryption, the above steps will repeat again. Otherwise, the decryption process completes.

For simulating experiments, we assign $p = 6$, $q = 7$, $\mu = 3.87$, $\varepsilon = 0.5$, $\eta = 0.9$. Figure 6 shows the encryption and decryption of images for one round. Figure 6u–x shows the encryption and decryption of a color image of Lena.

Fig. 6 Encryption, decryption of images. **a** Original image of Lena, **b** permuted image of Lena, **c** encrypted image of Lena, **d** decrypted image of Lena, **e** original image of Baboon, **f** permuted image of Baboon, **g** encrypted image of Baboon, **h** decrypted image of Baboon, **i** original image of Barb, **j** permuted image of Barb, **k** encrypted image of Barb, **l** decrypted image of Barb, **m** original image of Hill, **n** permuted image of Hill, **o** encrypted image of Hill, **p** decrypted image of Hill, **q** original image of Harbor, **r** permuted image of Harbor, **s** encrypted image of Harbor, **t** decrypted image of Harbor. **u** original color image of Lena, **v** permuted color image of Lena, **w** encrypted color image of Lena, **x** decrypted color image of Lena

In the proposed algorithm, the bit-level permutation and the value step depend on the sum of pixels about original image, which can resist efficiently the chosen-plaintext attack. These features strengthen the cryptosystem security.

4 Performance analyses

To evaluate the security of the encryption scheme, we employ the secret key sensitivity, histogram analysis, UACI, NPCR, correlation analysis and information entropy in experiments.

4.1 Key space

The key space should be large enough to make brute force attacks infeasible. Number of control parameters in secret key: secret key K has 4000-bit-long block, μ has a precision of 10^{-2} and $\mu \geq 3.7$, ε has a precision of 10^{-1} and η has a precision of 10^{-1}. The key space size is more than $2^{4000} \approx 10^{1200}$. It can be seen that the proposed encryption algorithm is good at resisting brute force attack.

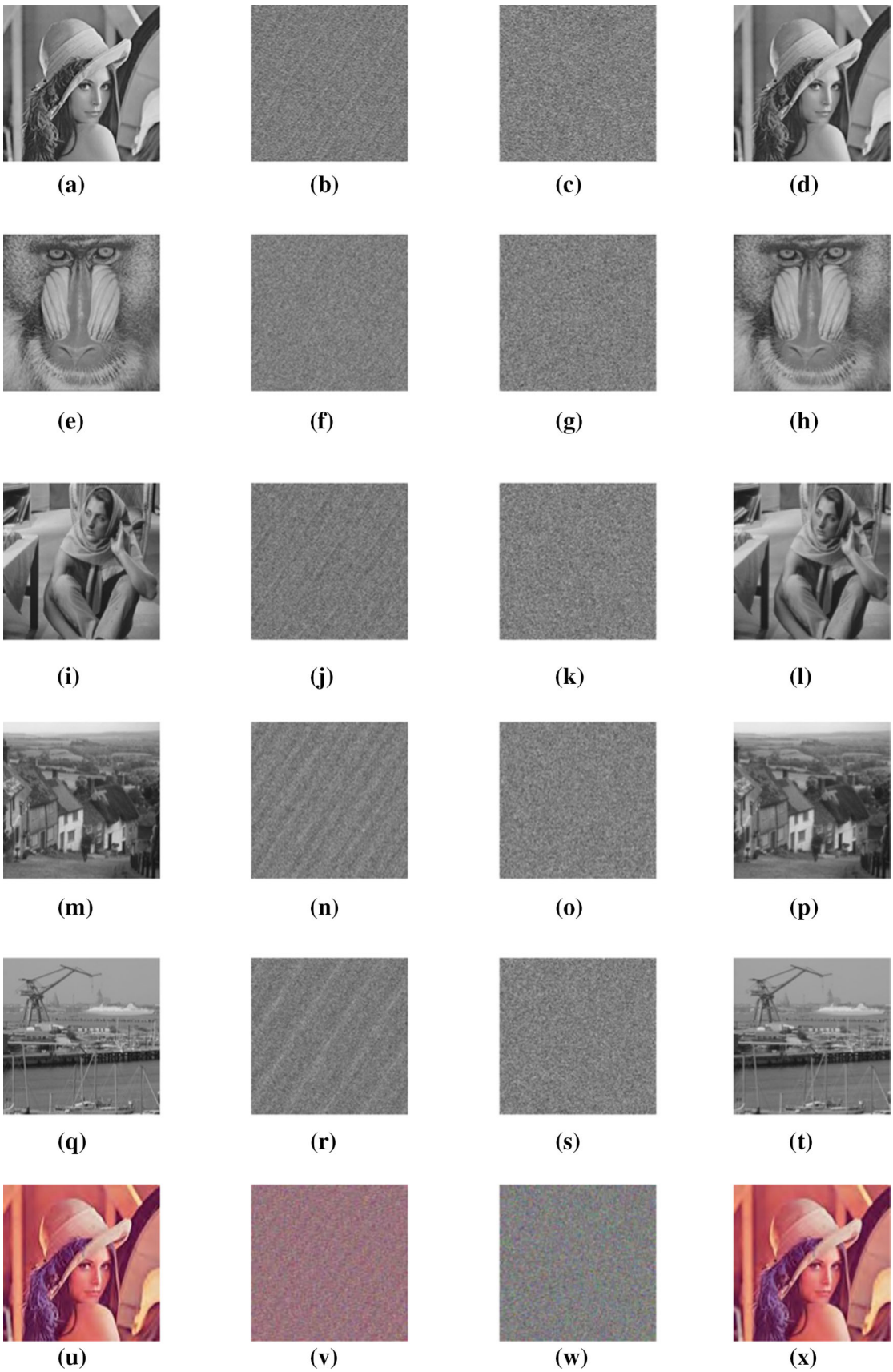
4.2 Key sensitivity

For testing the secret key sensitivity of K, without loss of generality, only the last bit of $K(10, 10)$ is changed. Figure 7 shows the two ciphered images of the Lena image generated from two security keys with only the last bit of $K(10, 10)$ difference.

For testing the secret key sensitivity of μ, without loss of generality, we assign $\mu = 3.871$. Figure 8 shows the two ciphered images of the Lena image generated from two security keys with only the μ difference.

For testing the secret key sensitivity of η, without loss of generality, we assign $\eta = 0.91$. Figure 9 shows the two ciphered images of the Lena image generated from two security keys with only the η difference.

For testing the secret key sensitivity of ε, without loss of generality, we assign $\varepsilon = 0.51$. Figure 10 shows the two


(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)
(k)
(l)
(m)
(n)
(o)
(p)
(q)
(r)
(s)
(t)
(u)
(v)
(w)
(x)

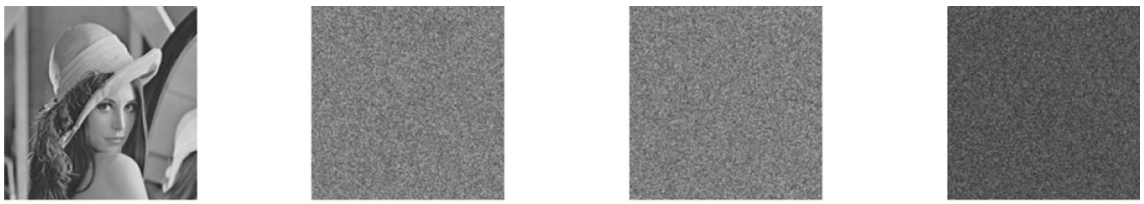


Fig. 7 Key sensitivity of K. **a** Original Lena image, **b** ciphered Lena image using original K, **c** ciphered Lena image using changed K, **d** difference between (**b**) and (**c**)

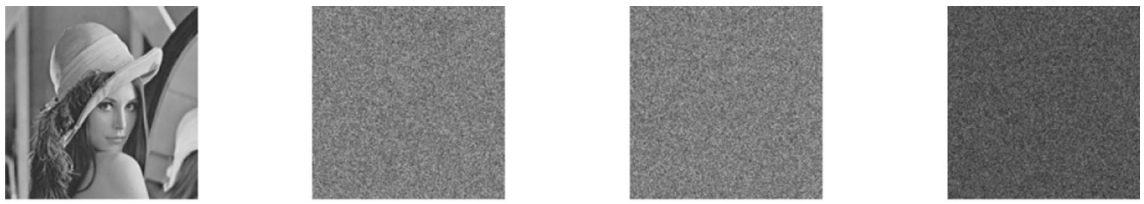


Fig. 8 Key sensitivity of μ. **a** Original Lena image, **b** ciphered Lena image using original μ, **c** ciphered Lena image using changed μ, **d** difference between (**b**) and (**c**)

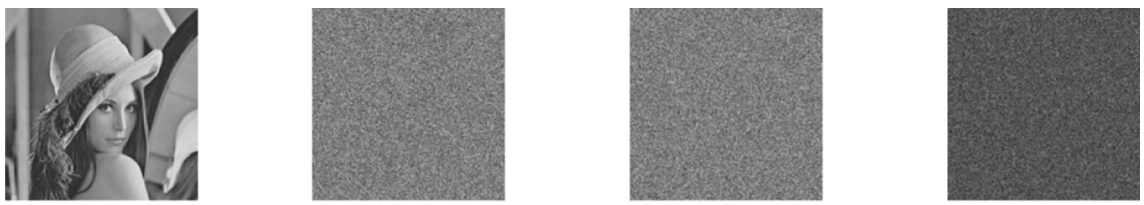


Fig. 9 Key sensitivity of η. **a** Original Lena image, **b** ciphered Lena image using original η, **c** ciphered Lena image using changed η, **d** Difference between (**b**) and (**c**)

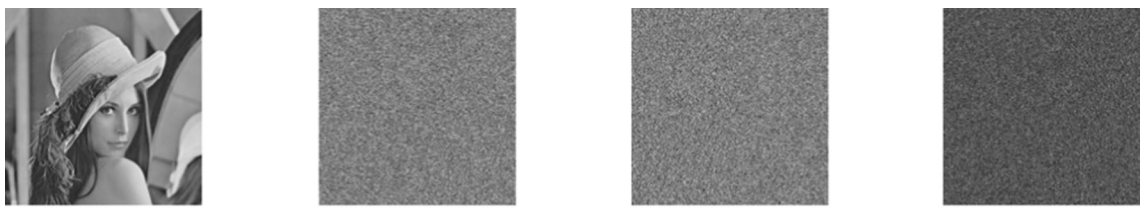


Fig. 10 Key sensitivity of ε. **a** Original Lena image, **b** ciphered Lena image using original ε, **c** ciphered Lena image using changed ε, **d** difference between (**b**) and (**c**)

ciphered images of the Lena image generated from two security keys with only the ε difference.

4.3 Histogram analysis

An ideal encrypted image should have a uniform and completely different histogram against the plain image for preventing the adversary from extracting any meaningful information from the fluctuating histogram of the cipher image.

Figures 11 and 12 show the histograms of the plain images, encrypted images using the proposed algorithm and encrypted images using 2DCML. Variances of histograms are listed in Table 1. The lower value of variances indicates the higher uniformity of ciphered images. In Table 1, the variance value is 637992.5804 for histogram of the plain image Lena, and the variance value is

1053.4431 for histogram of ciphered image Lena using 2DCML, which is greater than the variance 921.3020 for histogram of ciphered image Lena using the proposed algorithm. Therefore, the proposed algorithm is efficient.

4.4 Differential attack

To test the resistance of the differential attack of the encryption scheme, we employ the UACI (unified average changing intensity) and NPCR (number of pixels change rate), which are defined by

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}} \left[\sum_{\mathrm{ij}} \frac{|\mathrm{c}_1(\mathrm{i},\mathrm{j}) - \mathrm{c}_2(\mathrm{i},\mathrm{j})|}{255} \right] \times 100\%, \tag{14}$$

$$\begin{cases} D(i,j) = \begin{cases} 1 = c_1(i,j) \neq c_2(i,j); \\ 0 = \text{otherwise}, \end{cases} \\ \mathrm{NPCR} = \dfrac{\sum_{ij} D(i,j)}{M \times N} \times 100\%, \end{cases} \tag{15}$$

where c_1 and c_2 are the two ciphered images. Without loss of generality, we select 50 groups' images for each experimental image, and each group includes two images: One is the original image and the other is the image which changed one randomly selected pixel value by adding 1 in original image. The NPCR and UACI values with one round of encryption are shown as Fig. 13a, b, which are distributed near the ideal value (the horizontal line in Fig. 13). The average values of NPCR and UACI are NPCR = 0.996122681 and UACI = 0.334466780, which are very close to the ideal values. The NPCR and UACI performance compared with other algorithms is listed in Table 2. These comparisons confirm that the proposed algorithm is highly sensitive to a pixel change in plain image.

4.5 Correlation analysis

The correlation between adjacent pixels in the ciphered image should be significantly reduced, which is a good feature of encryption schemes. To test the correlation of plaintext image and ciphered image, the following procedures are carried out. First, randomly select 2000 pairs of two adjacent pixels from an image. Then, the correlation coefficients of adjacent pixels in vertical, horizontal and diagonal directions are evaluated by

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{16}$$

$$E(x) = \frac{1}{S}\sum_{i=1}^{S} x_i, \tag{17}$$

$$D(x) = \frac{1}{S}\sum_{i=1}^{S} (x_i - E(x))^2, \tag{18}$$

$$\mathrm{cov}(x,y) = \frac{1}{S}\sum_{i=1}^{S} (x_i - E(x))(y_i - E(y)), \tag{19}$$

where x and y denote two adjacent pixels and S is the total number of duplets (x, y) obtained from the image. $E(x)$ and $D(x)$ are the expectation and the variance of x, respectively. The calculated correlation coefficients of plaintext images and the corresponding ciphered images from the proposed encryption scheme are listed in Table 3. Comparisons of the correlation coefficients of images are listed in Table 4.

4.6 Information entropy

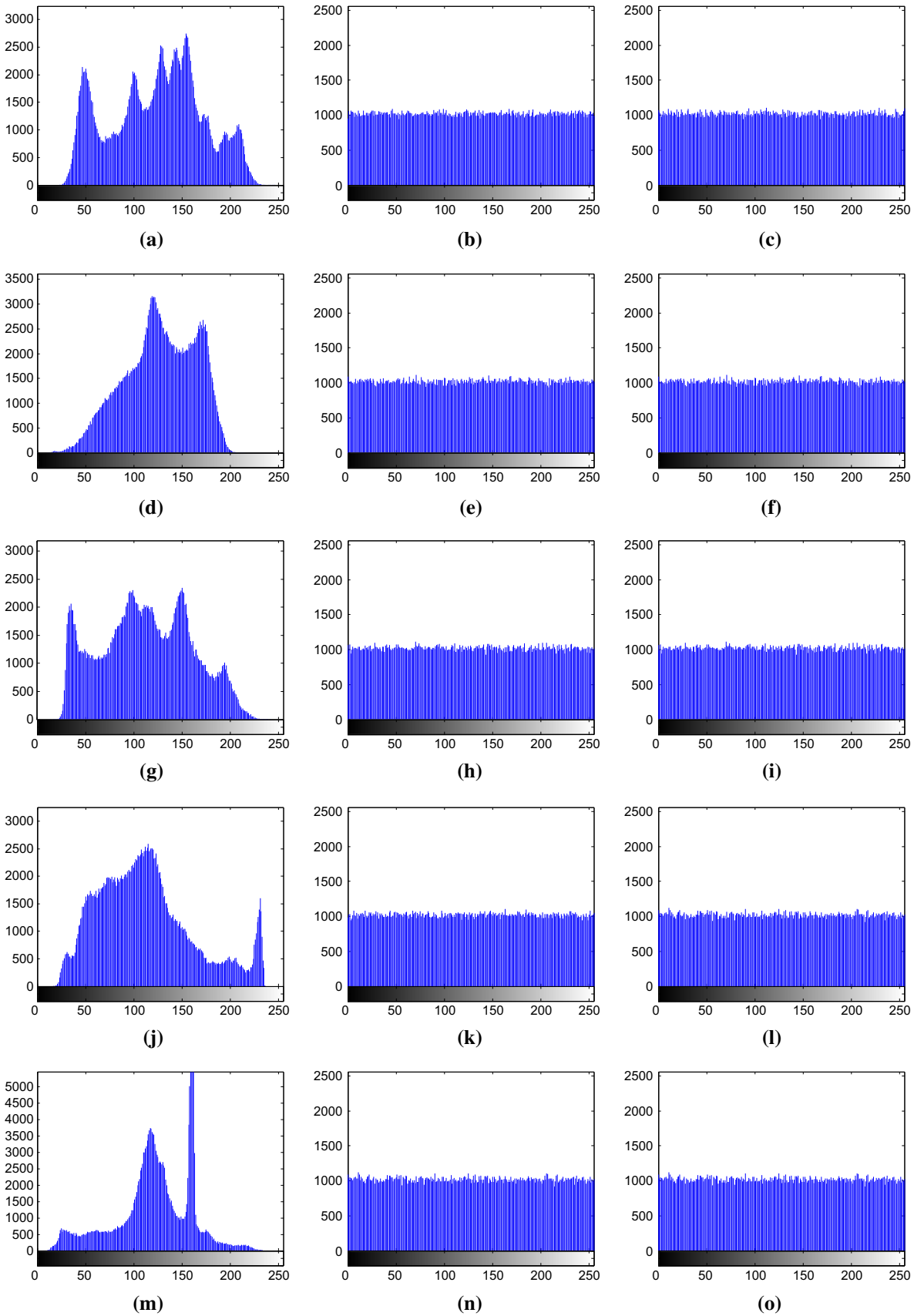
We calculate the information entropy of the plain images and the corresponding cipher images. The results are listed in Table 5. It is obvious that the entropies of the cipher images are all close to the ideal value 8, which means that the probability of accidental information leakage is very small. Meanwhile, compared with other algorithms [5, 6, 9, 22, 38], information entropy using proposed algorithm is higher. Thus, the proposed algorithm has the desired property of information entropy.

4.7 Computational and complexity analysis

All the tests are implemented in Visual Studio 2010 (Visual C++) with a Windows 7 Professional operating system, and the computer is of an Intel Core 2.5 GHz CPU, 4 GB RAM and 1000 GB hard disk, and some graphs are plotted using MATLAB 2014(a). The image of Lena, the 512×512 image with 256 gray levels, is encrypted, respectively, by the proposed algorithm, Zhang's algorithm [35] and Lian's algorithm [29, 39] for ten times. The average encryption time is 297.5 (ms), 218.4 (ms) and 336.7(ms), respectively.

For analyses of execution time in permutations, the time-consuming part in computations is the pixel moving operations. Both the proposed algorithm and Zhang's algorithm need $O\ (N^2)$ iterations of pixel moving operations. In Lian's algorithm, except the needed $O\ (N^2)$ iterations of pixel moving operations, another time-consuming part in computations is $O\ (N^2)$ iterations of calculations of a sine function, which needs more time than the proposed algorithm.

For analyses of execution time in diffusions, the time-consuming part in computations is the operation of multiplying floating-point numbers. The proposed algorithm


(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)
(k)
(l)
(m)
(n)
(o)

◀**Fig. 11** Histograms of the plain images and ciphered images. **a** Histogram of Lena, **b** histogram of ciphered Lena image using the proposed algorithm, **c** histogram of ciphered Lena image using 2DCML algorithm, **d** histogram of Baboon, **e** histogram of ciphered Baboon image using the proposed algorithm, **f** histogram of ciphered Baboon image using 2DCML algorithm, **g** histogram of Barb, **h** histogram of ciphered Barb image using the proposed algorithm, **i** histogram of ciphered Barb image using 2DCML algorithm, **j** histogram of Hill, **k** histogram of ciphered image Hill using the proposed algorithm, **l** histogram of ciphered Hill image using 2DCML algorithm, **m** Histogram of Harbor, **n** histogram of ciphered Harbor image using the proposed algorithm, **o** histogram of ciphered Harbor image using 2DCML algorithm

needs more time than the Zhang's algorithm because the proposed algorithm needs $O\ (L^2 \times N^2)$ iterations of multiplying floating-point numbers, while the Zhang's algorithm needs $O\ (L \times N^2)$ iterations of multiplying floating-point numbers. However, the proposed algorithm is more efficient compared with Lian's algorithm in total time. There is a trade-off between security and processing time. The proposed algorithm offers higher security as highlighted in previous sections, and if we decrease the size of lattices L, the proposed algorithm can run faster.

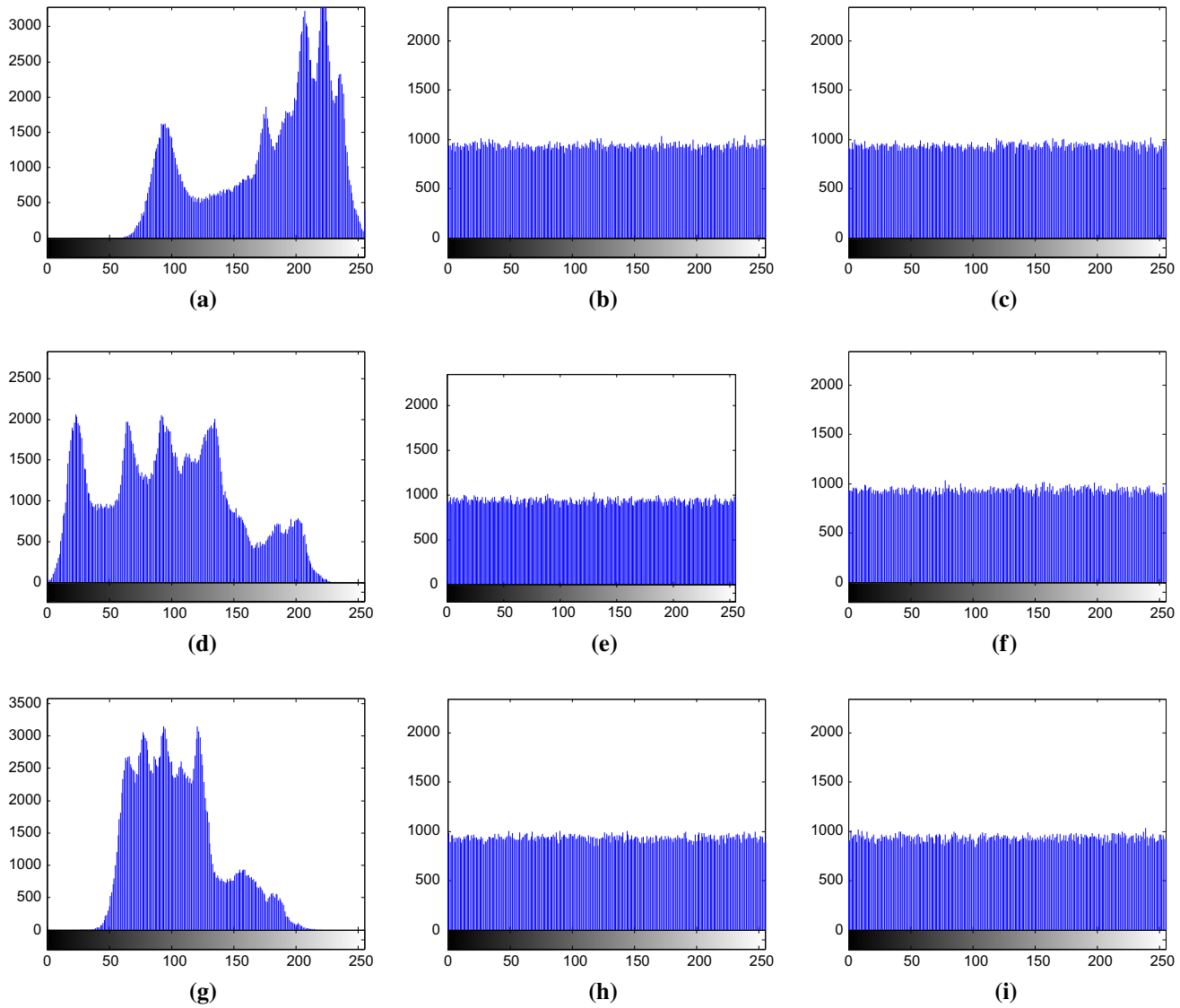


Fig. 12 Histograms of the color Lena image and ciphered color Lena image. **a** Histogram of R channel of color Lena, **b** histogram of R channel of ciphered color Lena image using the proposed algorithm, **c** histogram of R channel of ciphered color Lena image using 2DCML algorithm, **d** histogram of G channel of color Lena, **e** histogram of G channel of ciphered color Lena image using the proposed algorithm, **f** histogram of G channel of ciphered color Lena image using 2DCML algorithm, **g** histogram of B channel of color Lena, **h** histogram of B channel of ciphered color Lena image using the proposed algorithm, **i** histogram of B channel of ciphered color Lena image using 2DCML algorithm

Table 1 Variances of histograms compared the plain images and ciphered images

Image	Plain image	Ciphered image using 2DCML algorithm	Ciphered image using the proposed algorithm
Lena	637992.5804	1053.4431	921.3020
Baboon	1043803.5843	1177.5059	930
Barb	581630.0078	1048.0392	967.0196
Hill	650902.1412	1179.3961	1050.0314
Harbor	3715881.1686	1179.3960	798.8863
Color Lena(R)	844580	991.1174	962.8586
Color Lena(G)	408440	983.5174	974.3174
Color Lena(B)	1167000	1124.2	876.1292

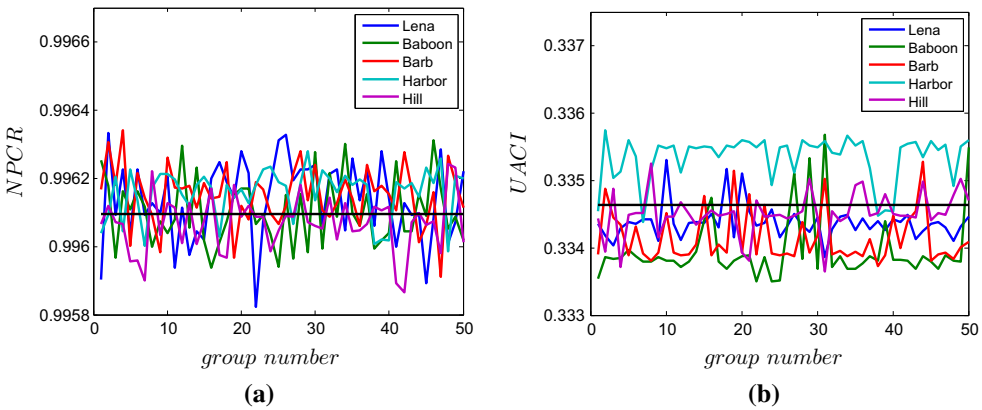


Fig. 13 NPCR and UACI values. **a** The NPCR values, **b** The UACI values

Table 2 NPCR and UACI performance compared with other algorithms

Image	Algorithm	NPCR	UACI
Lena	Proposed algorithm	0.996247610	0.334425723
Baboon	Proposed algorithm	0.996139527	0.334916632
Barb	Proposed algorithm	0.996228536	0.334903837
Lena	Reference [6]	0.0015	0.0012
Lena	Reference [32]	0.996170	0.330354
Lena	Reference [22]	0.9979	0.3339
Lena	Reference [5]	0.995894869	0.334645896
Lena	Reference [37]	0.9961	0.3346
Lena	Reference [9]	0.9961	0.3353
Lena	Reference [38]	0.996253	0.334807
Baboon	Reference [32]	0.995819	0.320972
Baboon	Reference [22]	0.9980	0.3337
Baboon	Reference [37]	0.9962	0.3344
Barb	Reference [5]	0.996078491	0.334790692
Barb	Reference [37]	0.9961	0.3346
Barb	Reference [38]	0.996215	0.334691

Table 3 Correlation coefficient of images

Image	Horizontal	Vertical	Diagonal
Plain Lena	0.969679	0.987698	0.967310
Cipher Lena	0.000581	− 0.000844	− 0.002550
Plain Baboon	0.743661	0.863635	0.705826
Cipher Baboon	− 0.000439	− 0.000307	0.001201
Plain Barb	0.888022	0.966931	0.852119
Cipher Barb	− 0.000956	0.000636	− 0.001509
Plain Hill	0.972634	0.970486	0.949966
Cipher Hill	0.000607	0.0005254	0.001266
Plain Harbor	0.816600	0.919997	0.776223
Cipher Harbor	0.000520	− 0.0005654	0.001470

5 Conclusions

We propose a new image encryption algorithm using two-dimensional spatiotemporal chaos system, which mixed linear–nonlinear coupled map lattices. The system contains the new features such as less periodic windows in bifurcations and larger range of parameters in chaotic dynamics, which is more suitable for cryptography. In addition, the image is permuted by the Arnold cat map for bit-level

Table 4 Comparison of the correlation coefficients of cipher images

Image	Algorithm	Horizontal	Vertical	Diagonal
Lena	Proposed algorithm	0.000581	− 0.000844	− 0.002550
Baboon	Proposed algorithm	− 0.000439	− 0.000307	0.001201
Barb	Proposed algorithm	− 0.000956	0.000636	− 0.001509
Lena	Reference [6]	− 0.0037	− 0.0018	0.0019
Lena	Reference [32]	− 0.0039	− 0.0072	0.000866
Lena	Reference [22]	− 0.000169	0.001153	− 0.000989
Lena	Reference [5]	− 0.0294	− 0.0014	− 0.0180
Lena	Reference [29]	0.002016	− 0.000916	0.001650
Lena	Reference [38]	− 0.0047	0.0015	0.0030
Lena	Reference [9]	− 0.0226	0.0041	0.0368
Baboon	Reference [32]	0.0033	− 0.0062	0.0046
Baboon	Reference [22]	0.002181	0.001928	0.002138
Baboon	Reference [37]	0.0057	0.00005048	0.0024
Barb	Reference [5]	− 0.0124	0.0021	− 0.0062
Barb	Reference [37]	0.0151	0.0005199	− 0.0086
Barb	Reference [38]	0.0033	0.0032	0.0025

Table 5 Information entropy of images

Image	Lena	Baboon	Barb	Hill	Harbor
Plain image	7.446091	7.145709	7.464895	7.476172	6.783396
Cipher image	7.999267	7.999191	7.999340	7.999410	7.999327

permutation, which can change the position and value of a pixel simultaneously. A more than 4000-bit-long secret key has been used to generate the initial conditions and parameters of the maps. The algorithm also includes the sum of pixels about original image, which can resist efficiently the chosen-plaintext attack. The numerical results show that the proposed algorithm has superior security and high efficiency for image encryption.

Acknowledgements This research is supported by the Program for New Century Excellent Talents in Fujian Province University, Zhangzhou Science and Technology Project (No.ZZ2018J23), the Natural Science Foundation of Fujian Province of China (No.2018J01100), National Natural Science Foundation of China (Nos: 61672124, 61173183, and 61370145), Program for Liaoning Excellent Talents in University (No:LR2012003), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203).

Compliance with ethical standards

Conflict of interest We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, and there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, this manuscript.

References

1. Khan M, Shah T (2015) An efficient chaotic image encryption scheme. Neural Comput Appl 26(5):1137–1148
2. Liu H, Kadir A, Sun X (2017) Chaos-based fast color image encryption scheme with true random number keys from environmental noise. IET Image Process 11(5):324–332
3. Bagheri P, Shahrokhi M (2016) Neural network-based synchronization of uncertain chaotic systems with unknown states. Neural Comput Appl 27:945–952
4. Li C, Lin D, Lü J, Hao F (2017) Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimedia arXiv:1711.01858v2
5. Belazi A, El-Latif A, Diaconu A, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
6. Nosrati Komeil, Volos Christos, Azemi Asad (2017) Cubature Kalman filter-based chaotic synchronization and image encryption. Signal Process-Image 58:35–48
7. Liu H, Kadir A, Sun X, Li YL (2018) Chaos based adaptive double-image encryption scheme using hash function and S-boxed. Multimed Tools Appl 77(1):1391–1407
8. Khan M, Shah T, Batool SI (2016) Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Comput Appl 27(3):677–685
9. Xu L, Gou X, Li Zh, Li J (2017) A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt Lasers Eng 91:41–52
10. Coulibaly S, Clerc MG, Selmi F, Barbay S (2017) Extreme events following bifurcation to spatiotemporal chaos in a spatially extended microcavity laser. Phys Rev A 95(2):023816

11. Liu H, Kadir A (2015) Asymmetric color image encryption scheme using 2D discrete-time map. Signal Process 113:104–112
12. Kanso A, Ghebleh M (2015) A structure-based chaotic hashing scheme. Nonlinear Dyn 81(1–2):27–40
13. Seyedzadeh SM, Norouzi B, Mosavi MR (2015) A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dyn 81(1–2):511–529
14. Wang XY, Zhang HL, Bao XM (2016) Color image encryption scheme using CML and DNA sequence operations. Biosystems 144:18–26
15. Sinha S (2002) Random coupling of chaotic maps leads to spatiotemporal synchronization. Phys Rev E 66:016209
16. Mondal A, Sinha S, Kurths J (2008) Rapidly switched random links enhance spatiotemporal regularity. Phys Rev E 78:066209
17. Kohar V, Ji P, Choudhary A, Sinha S, Kurths J (2014) Synchronization in time-varying networks. Phys Rev E 90(2):022812
18. Nag M, Poria S (2016) Synchronization in a network of delay coupled maps with stochastically switching topologies. Chaos Soliton Fract 91(33):9–16
19. Zhang YQ, Wang XY (2014) Spatiotemporal chaos in mixed linear-nonlinear coupled logistic map lattice. Phys A 402(10):104–118
20. Zhang YQ, Wang XY (2013) Spatiotemporal chaos in Arnold coupled logistic map lattice. Nonlinear Anal-Model 18(4):526–541
21. Ercan S, Cahit C (2011) Algebraic break of image ciphers based on discretized chaotic map lattices. Inf Sci 181:227–233
22. Machkour M, Saaidi A, Benmaati ML (2015) A novel image encryption algorithm based on the two-dimensional logistic map and the Latin square image cipher. 3D Res 6(4):36–54
23. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos 8:1259
24. Xie EY, Li C, Yu S (2016) On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process 132:150–154
25. Zhang YQ, Wang XY (2015) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20
26. Kaneko K (1989) Spatiotemporal chaos in one- and two-dimensional coupled map lattices. Physica D 37:60–82
27. Kaneko K (1993) Theory and application of coupled map lattices, Chapter 1. Wiley
28. Zhang W, Wong KW, Yu H, Zhu ZL (2013) A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Commun Nonlinear Sci Numer Simul 18:584–600
29. Zhu ZL, Zhang W, Wong KW, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181:1171–1186
30. Li C (2016) Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process 118:203–210
31. Kar M, Mandal MK, Nandi D (2016) Bit-plane encrypted image cryptosystem using chaotic, quadratic, and cubic maps. Iete Tech Rev 33(6):651–661
32. Praveenkumar P, Amirtharajan R, Thenmozhi K, Rayappan JBB (2017) Fusion of confusion and diffusion: a novel image encryption approach. Telecommun Syst 65(1):65–78
33. Li C, Lo KT (2011) Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process 91(4):949–954
34. Shibata H (2001) KS entropy and mean Lyapunov exponent for coupled map lattices. Phys A 292:182–192
35. Zhang YQ, Wang XY (2014) A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci 273(8):329–351
36. Li C, Lin D, Lü J (2017) Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. IEEE Multimedia 24(3):64–71
37. Chai XL, Gan ZH, Yuan K (2017) An image encryption scheme based on three-dimensional Brownian motion and chaotic system. Chinese Phys B 26(2):020504
38. Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39–49
39. Lian S, Sun J, Wang Z (2005) A block cipher based on a suitable use of the chaotic standard map. Chaos Soliton Fract 26(1):117–129
40. Özkaynak F (2018) Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn 92(2):305–313