ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

A novel pseudo-random coupled LP spatiotemporal chaos and its application in image encryption

Xingyuan Wang(王兴元), Yu Wang(王宇), Siwei Wang(王思伟), Yingqian Zhang(张盈谦), Xiangjun Wu(武相军)

Citation: Chin. Phys. B . 2018, 27(11): 110502. **doi:** 10.1088/1674-1056/27/110502

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem

Zeyu Liu(刘泽宇), Tiecheng Xia(夏铁成), Jinbo Wang(王金波)

Chin. Phys. B . 2018, 27(3): 030502. **doi:** 10.1088/1674-1056/27/3/030502

Parrondo's paradox for chaos control and anticontrol of fractional-order systems

Marius-F Danca and Wallace K S Tang

Chin. Phys. B . 2016, 25(1): 010505. **doi:** 10.1088/1674-1056/25/1/010505

A new piecewise linear Chen system of fractional-order: Numerical approximation of stable attractors

Marius-F. Danca, M. A. Aziz-Alaoui, Michael Small

Chin. Phys. B . 2015, 24(6): 060507. **doi:** 10.1088/1674-1056/24/6/060507

Complex dynamics analysis of impulsively coupled Duffing oscillators with ring structure

Jiang Hai-Bo, Zhang Li-Ping, Yu Jian-Jiang

Chin. Phys. B . 2015, 24(2): 020502. **doi:** 10.1088/1674-1056/24/2/020502

Bifurcation analysis of the logistic map via two periodic impulsive forces

Jiang Hai-Bo, Li Tao, Zeng Xiao-Liang, Zhang Li-Ping

Chin. Phys. B . 2014, 23(1): 010501. **doi:** 10.1088/1674-1056/23/1/010501

A novel pseudo-random coupled LP spatiotemporal chaos and its application in image encryption*

Xingyuan Wang(王兴元)[1,2,†], Yu Wang(王宇)[2], Siwei Wang(王思伟)[2], Yingqian Zhang(张盈谦)[3], and Xiangjun Wu(武相军)[4]

[1] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[2] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[3] School of Information Science & Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China
[4] College of Software, Henan University, Kaifeng 475004, China

(Received 11 July 2018; revised manuscript received 22 August 2018; published online 24 October 2018)

In this paper, first, we investigate a novel one-dimensional logistic-PWLCM (LP) modulation map which is derived from the logistic and PWLCM maps. Second, we propose a novel PCLML spatiotemporal chaos in pseudo-random coupling method that can accelerate the system behavior of the fully spatial chaos. Here, because the better chaotic properties include a wide range of parameter settings and better ergodicity than a logistic map, the LP is used in PCLML as $f(x)$. The Kolmogorov–Sinai entropy density and universality and the bifurcation diagram are employed to investigate the chaotic behaviors of the proposed PCLML model. Finally, we apply the LP and PCLML chaotic systems to image encryption to improve the effectiveness and security of the encryption scheme. By combining self-generating matrix model M and dynamic substitution box (S-Box) methods, we design a new image encryption algorithm. Numerical simulations and security analysis have been carried out to demonstrate that the proposed algorithm has a high security level and can efficiently encrypt several different kinds of images into random-like images.

Keywords: logistic-PWLCM map, PCLML spatiotemporal chaos, matrix model M, dynamic S-Box, image encryption

PACS: 05.45.Ac, 05.45.–a **DOI:** 10.1088/1674-1056/27/11/110502

1. Introduction

Spatiotemporal chaos is a complex phenomenon in the study of turbulence, not only in fluid dynamics but also in solid-state physics, optics, chemical reaction with diffusion, and possibly in biology.[1,2] The coupled map lattice (CML) is a model of chaotic spatial and dynamical structures, which has been investigated by many researchers and a large number of related theories are obtained. Khellat *et al.*[3] proposed a globally nonlocal couple map lattice (GNCML) of spatiotemporal chaos. A one-way coupled map lattice (OCML) of spatiotemporal chaos is presented by Meherzi *et al.*[4] Guedes *et al.*[5] investigated the spatiotemporal dynamics of coupled logistic maps. Most of the previous spatiotemporal chaotic systems are spatial linear coupling between lattices. Each map lattice is influenced by its adjacent lattices. Therefore, the chaotic sequences generated in the adjacent two lattices have a high correlation. To break this characteristic, three coupling connect methods are investigated: spatial random coupling, spatial nonlinear coupling, and spatial linear–nonlinear mixed coupling. Poria *et al.* developed a lattice of coupled chaotic maps whose coupling connections are dynamically rewired to random sites with probability p.[6] The connect methods with connections rewired randomly by varying probability p and period t are employed to create a randomly coupled spatiotemporal chaos by Chen *et al.*[7] Zhang *et al.*[8] suggested a new spatiotemporal dynamics of Arnold coupled logistic map lattice (ACLML) based on the nonlinear coupling method.

The MLNCML system used linear–nonlinear mixed coupling method and achieved better chaotic performance than CML.[9] However, those spatiotemporal chaos in this spatial random coupling method cannot be reproduced again in the same parameters, which means that it is unsuitable for use in cryptography. The ACLML and MLNCML systems changed the neighborhood coupling into non-neighborhood coupling by using the nonlinear chaotic map coupling method, although they still have the characteristic that one lattice is limited by another two lattices. Based on this above work, we employed a novel pseudo-random coupling method to design a new spatiotemporal chaotic system that we named PCLML. Two coupling lattices are selected by the chaotic sequences, which are generated with chaotic system. Hence, chaos behavior in one lattice can quickly spread to the whole space and the data in one lattice can affect all of the lattices.

These spatiotemporal chaotic systems are based on the classical logistic map, which is proven to be unsafe.[10–12] Lo-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61672124, 61370145, and 61173183), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund, China (Grant No. MMJJ20170203), the Program for New Century Excellent Talents in Fujian Province University, and the Natural Science Foundation of Fujian Province of China (Grant No. 2018J01100).

†Corresponding author. E-mail: wangxy@dlut.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

gistic chaotic orbits are quite simple and may be predicted easily. It has three security issues: blank windows, smaller parameter value space, and the non-uniform data distribution of output chaotic sequences.[11] Hence, it has unsuitable to be adopted in spatiotemporal chaos. In this paper, we design a new one-dimensional (1D) modulation chaos named logistic-PWLCM (LP) by using a combination of two existing 1D chaotic maps: logistic map and PWCLM map. In contrast to the logistic map, our simulations and performance evaluations show that the proposed LP system has larger chaotic parameter space from 0 to 4, higher Lyapunov exponent, and uniform distributed data. Consequently, we suggested LP chaotic system as $f(x)$ in PCLML spatiotemporal chaos instead of logistic map.

The motivation of our work in this paper is not only to discover the new features of spatiotemporal chaotic systems in pseudo-random coupling with LP chaotic map but also to study new characters which are suitable for image cryptography. The CML system is widely applied to image encryptions,[13–15] but the behavior of periodic window and the high values of the mutual information reduce the randomness of space and time series and restraint the design of current encryptions schemes.[16,17] Compared with the CML system, our experimental results prove that the chaotic dynamic behavior of PCLML system is more complex and it owns some new features, such as larger range of parameters for chaotic behaviors, no periodic windows in bifurcation diagrams, and higher entropy universality to overcome those drawbacks in CML. Therefore, we use PCLML system to encrypt image combining some new methods such as adding random pixels, self-generating matrix model M, and dynamic substitution box (S-Box) technology. By adding random pixels, we can ensure that each encryption result is different, even for the case of encrypting a plain-image several times with the same secret key. Matrix model M operation speeds up the encryption and can change the same pixels into different values after computing, which makes the histogram of the image uniform and able to effectively resist statistical attacks. The S-Box is one of the core nonlinear components in encryption algorithms and it is widely applied to image encryption. Liu *et al.* designed a chaos-based color image encryption scheme using bijection and S-Box.[18] Guesmi *et al.* presented a strong S-Box by using logistic chaotic and Boolean functions.[19] By calculation, they compared all of S-Boxes and selected the highest nonlinearity S-Box as the final one. Hussain *et al.* constructed chaotic linear fractional transformation (LFT) S-Boxes and made the cipher more resistant against cryptanalyst attacks.[20] In addition, we construct four dynamic S-Boxes by using chaotic sequences sort method, which has been proven to be effective.[21] We use several different kinds of analysis measures, including key space, sensitivity, information entropy, histogram, and robustness to noise, data loss, and differential attacks. The security analysis and simulation results prove that our new algorithm has large key space, is robust against potential attacks, and has excellent encryption performance.

2. The new 1D LP system

2.1. Logistic and PWLCM system

The logistic and PWLCM maps are two commonly used 1D classical chaotic maps. Their structure seems to be very simple and deterministic but they have excellent chaotic behaviors. The mathematical definition can be described by, respectively,

$$x_{i+1} = ux_i(1-x_i), \tag{1}$$

$$x_{i+1} = F_p(x_i) = \begin{cases} x_i/p, & 0 \le x_i < p, \\ (x_i-p)/(0.5-p), & p \le x_i \le 0.5, \\ F_p(1-x_i), & 0.5 < x_i \le 1, \end{cases} \tag{2}$$

where parameter u is within the range of (0, 4], parameter $p \in (0, 0.5)$, and $x_i \in [0,1]$ is an independent variable. When $p \in (0, 0.5)$, PWLCM is chaotic. The logistic map is chaotic when $u \in [3.57, 4]$ and the sequence x will be quite different even if u and p change a little.

2.2. The LP system

The logistic map and PWLCM map share some common problems, such as blank windows, weak parameter space, and uneven distribution of sequences.[22] These properties limit their application in some of the high security requirements of the scenes. According to a nonlinear combination structure,[22] a new 1D LP map is proposed and is developed from two simple chaotic systems. This can be defined by

$$x_{i+1} = F_p(x_i) = \begin{cases} ux_i(1-x_i) + 8x_i/u, & 0 \le x_i < 0.125u, \\ ux_i(1-x_i) + (x_i - 0.125u)/(0.5-0.125u), & 0.125u \le x_i \le 0.5, \\ F_p(1-x_i), & 0.5 < x_i \le 1. \end{cases} \tag{3}$$

The LP map has more complex structures than a logistic map and this makes its chaotic orbits much harder to predict. To qualify the performance of LP system, Lyapunov exponent, bifurcation, and distribution of output sequences are investigated. Figure 1(a) shows the Lyapunov exponent of LP map and it indicates that LP is chaotic and possesses higher exponents when u is within the range of (0, 4). Therefore, the key space has been increased greatly. Bifurcation of LP map is shown in Fig. 1(b)

and it is clear that there are no blank windows and the value of x can cover the whole area of (0, 1). Figure 1(c) demonstrates the data distribution of LP's output sequences and it shows that the results have a more uniform behavior between 0 and 1 than a logistic map.

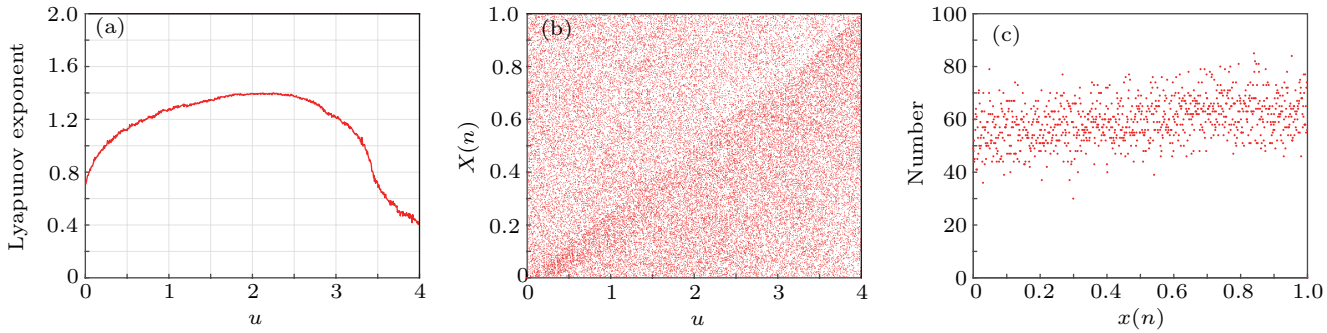


Fig. 1. (color online) The characteristics of the LP chaotic map. (a) Lyapunov exponent, (b) bifurcation, and (c) distribution of output sequences.

3. The proposed PCLML system and its new features

3.1. The proposed PCLML system

The CML is investigated as a classical model for spatiotemporal chaos and it considers a grid of L logistic maps. The definition of CML in discrete time n is given as

$$x_{n+1}(i) = (1-\varepsilon) f[x_n(i)] + \frac{\varepsilon}{2}\{f[x_n(i-1)] + f[x_n(i+1)]\}, \quad (4)$$

where ε is coupling coefficient ($0 \le \varepsilon \le 1$), i is a lattice point ($i = 1, 2, \ldots, L$) with boundary condition, and $f(x)$ represents logistic map.

Now, we randomly rewire the coupling connections of the above system in varying lattices; namely, we change the coupling lattices from $i-1$ and $i+1$ to j, k, respectively. A novel spatiotemporal chaos entitled PCLML system is designed as

$$x_{n+1}(i) = (1-\varepsilon) f[x_n(i)] + \frac{\varepsilon}{2}\{f[x_n(j)] + f[x_n(k)]\}, \quad (5)$$

where $f(x)$ represents the LP map, and j and k are decided by the pseudo-random chaotic sequences which are generated by the LP map.

Without loss of generality, we supposed that the size of L on the system of PCLML is 100. To verify the effectiveness of the proposed PCLML model, we did a comparison experiment with the CML system, which also assigned $L = 100$. All of our simulations are conducted assuming $\varepsilon \in [0,1]$ and $u \in (0,4)$. j and k are different in every iteration and they represent different kinds of couplings, changing from neighbor coupling to random non-neighbor coupling.

3.2. Kolmogorov–Sinai entropy density and universality in the PCLML system

The Kolmogorov–Sinai entropy density of proposed PCLML chaos is the average of positive Lyapunov exponents in all lattices. The Lyapunov exponent is one of the most important geometrical invariants to measure the dynamic characteristics of a chaotic system.[8] In general, the larger the Lyapunov exponents are, the more complex the chaotic dynamical behavior is. According to the calculation method in Ref. [9], we can get the Kolmogorov–Sinai entropy density and universality. Kolmogorov–Sinai entropy universality is the percentage of lattices in chaos, which depicts the space complexity in L dimensions of dynamics.

The experimental results of Kolmogorov–Sinai entropy density for different parameters ε and u in the proposed PCLML model and the CML system are shown in Fig. 2. This allows us to identify behaviors of both systems distinctly. As seen in Fig. 2(a), the Kolmogorov–Sinai entropy density (h) is zero when $\varepsilon \in [0,1]$ and $u \in (0,3.63)$, which means that the performance of the CML system is regular. When $u > 3.63$, the CML system began to possess chaotic behavior and the value of h is in the range of (0, 0.7). By calculation, in the CML system the average value of h achieves 0.2718 and most of the higher values only reach $h = 0.4$ when $u = 4$. Figure 2(b) shows the distribution of Kolmogorov–Sinai entropy density about PCLML system. We can see that h is positive no matter what, as are u and ε, which indicates that the PCLML system is chaotic at the whole parameter space. Hence, the range of parameter u or ε becomes correspondingly larger than that of the CML system, which is more suitable for application in the field of security. The value of h in PCLML is specified in (0.4, 1.5) and the average value of h realizes 1.1760, which is significantly higher than average of CML. Therefore, the dynamic behavior of the new proposed system is more complex than CML.

The values of Kolmogorov–Sinai entropy universality (hu) for different parameter values represent the space chaotic behaviors of the PCLML system and the CML system, as shown in Fig. 3. As seen in Fig. 3(b), almost all of the parameter pairs of PCLML system contain 100% lattices in chaotic behaviors with the exception of $\varepsilon \in [0.4,1]$, and $u \in (3.96,4)$. Namely, every lattice in PCLML is chaotic when $\varepsilon \in (0,1)$, and $u \in (0,3.96)$. But in CML system, as shown in Fig. 3(a), 100% lattices in chaotic behaviors are obtained only in the area of $u \in (3.75,4)$ and $\varepsilon \in (0,1)$. Even in these areas, chaotic behaviors in all lattices are unstable. For example, the CML system only achieves 50% lattices in chaotic behaviors when $u = 3.8$ and $\varepsilon = 0.2$.

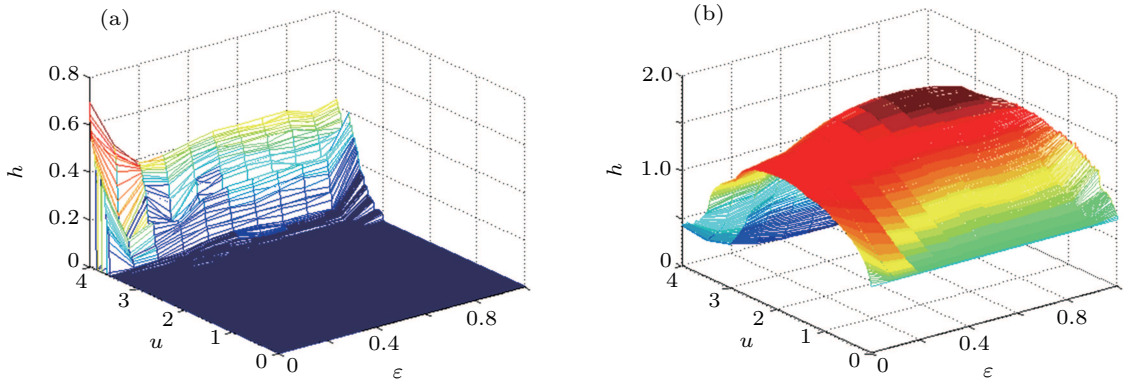


Fig. 2. (color online) Comparison between CML and PCLML in Kolmogorov–Sinai entropy density. (a) CML and (b) PCLML.

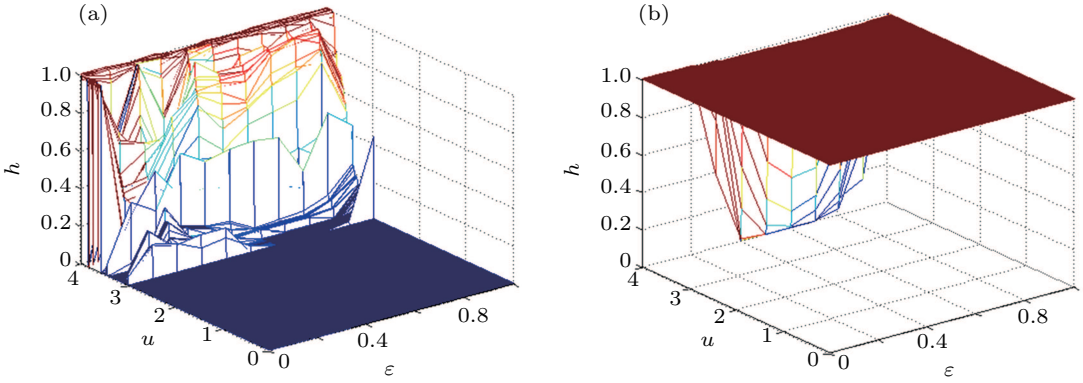


Fig. 3. (color online) Comparison between CML and PCLML in Kolmogorov–Sinai entropy universality. (a) CML and (b) PCLML.

The comparison between the PCLML and the CML systems in Kolmogorov–Sinai entropy indicates that the PCLML system contains more intensive and extensive chaotic behaviors.

3.3. Bifurcations of the PCLML model

It is important to predict an essential aspect of chaotic behavior by considering its bifurcation of the coupled system. In the CML system and proposed PCLML model, the bifurcation diagrams with different u and fixed ε are shown in Fig. 4.

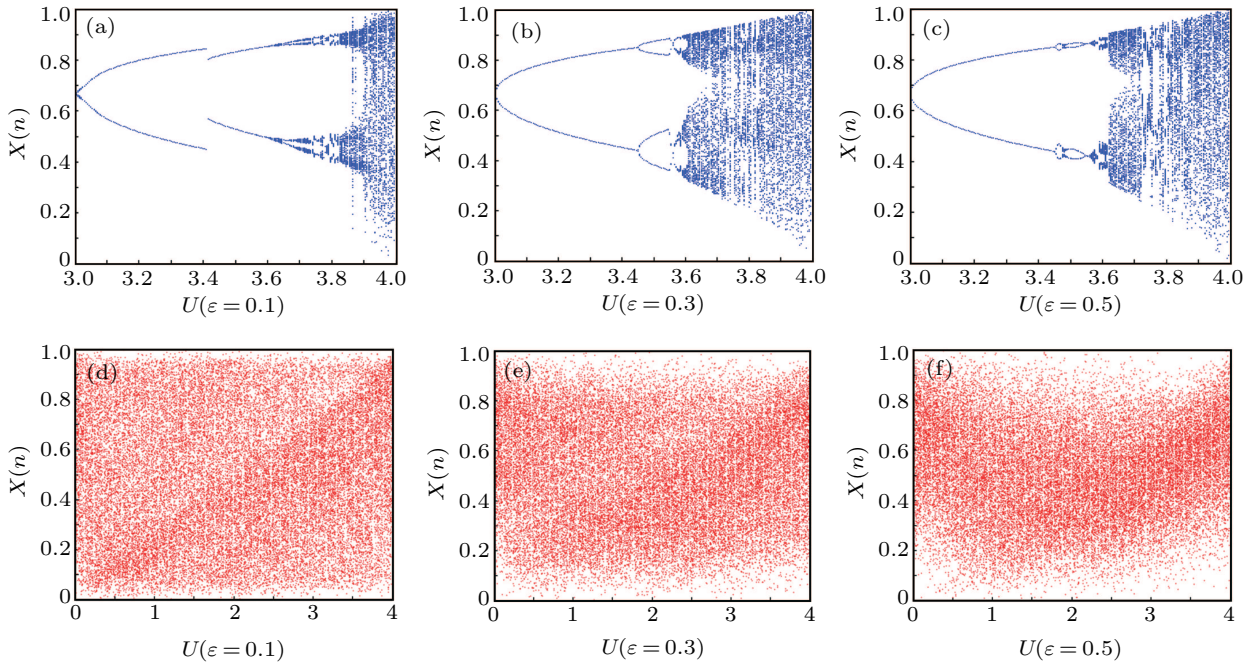


Fig. 4. (color online) The comparison between CML and PCLML in bifurcations. (a) CML ($u = 0.1$), (b) CML ($u = 0.3$), (c) CML ($u = 0.5$) and (d) PCLML ($u = 0.1$), (e) PCLML ($u = 0.3$), (f) PCLML ($u = 0.5$).

Figures 4(a)–4(c) illustrate bifurcation of the CML system where $u \in (3,4)$ with $\varepsilon = 0.1$, $\varepsilon = 0.3$, and $\varepsilon = 0.5$ respectively, which show the same forking of the possible periods of orbits from period-2 to period-4 and period-4 to period-8 with logistic map. Beyond that, there are some periodic windows and blank windows in the bifurcation diagram, which is against its security.

The bifurcation of PCLML model when $u \in (0,4)$ with $\varepsilon = 0.1$, $\varepsilon = 0.3$, and $\varepsilon = 0.5$ is drawn in Figs. 4(d)–4(f), respectively. We cannot find the bifurcation behavior and its trajectory goes through the whole space of (0, 1). At the same time, the bifurcation diagram without periodic windows and blank windows in the proposed PCLML model is a new feature. The explanation of the difference of bifurcation is that the proposed novel 1D LP map has better chaotic characteristics than logistic map and pseudo-random coupling increases the instability of the possible periods of the orbits. Since it has less periodic windows than low dimension chaotic map, the CML system is regarded as a suitable spatiotemporal chaotic system for cryptography. Thus, the proposed model is more suitable for cryptography (for the same reason).

4. The applications of the PCLML and LP systems in image encryption

In this section, using PCLML and LP systems, an image encryption scheme based on self-generating matrix model M and dynamic S-Box methods are presented. The secret keys related to plaintext are considered as the initial values of LP and PCLML systems. Chaotic sequences generated by PCLML map are applied to construct matrix model M and S-Boxes. Before encryption, several random values are added to plain image which can ensure that encrypted cipher images are different. Without loss of generality, we suppose that the number of PCLML lattice i is 100 and the size of the plain image F is $W \times H$. The running environment of the algorithm is 8.00 GB RAM, Intel (R) Core (TM) Intel (R) Xeon (R) CPU @2.67 Hz. The encryption algorithm time complexity is O(m^3). The process of encryption is shown in Fig. 5.

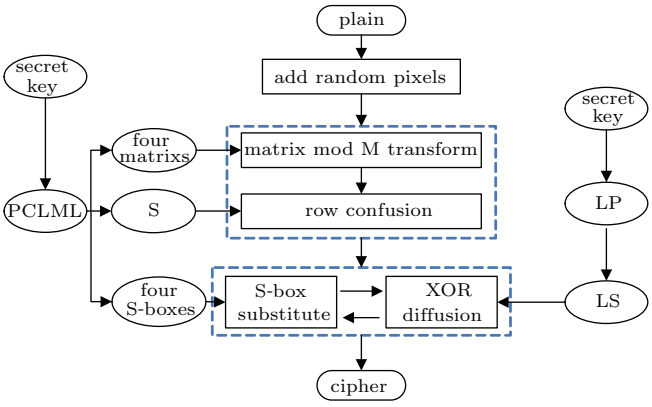


Fig. 5. The process of the encryption algorithm.

4.1. Secret key generation

The key space should be large enough to make brute-force attack infeasible and it should be larger than 2^{100}.[23] To satisfy this requirement, we set the secret key as 256 random bits K and the average value of a plaintext image r. In the real application, r can be represented by 32 bits. Therefore, the total key space is 2^{288}. To resist chosen-plaintext attacks, we combine K and r together to generate the initial values and control parameters of LP and PCLML systems. The generation procedures of initial values are shown in Algorithm 1.

Algorithm 1. The generation procedures of initial values of LP and PCLML system.

Input: the secret 256-bit key K and plain image img

Output: $u_1, u_2, u_3, u_4, x_1, x_2, x_3, \varepsilon$

1: $r = \left(\sum_{i=1}^{W}\sum_{j=1}^{H} img[i][j]\right)/255 \times W \times H$

2: $c_1 = \left(\sum_{i=1}^{32} K[i] \times 2^{i-1}\right)/2^{32}$, $c_2 = \left(\sum_{i=33}^{64} K[i] \times 2^{i-32}\right)/2^{32}$, $c_3 = \left(\sum_{i=65}^{96} K[i] \times 2^{i-64}\right)/2^{32}$, $c_4 = \left(\sum_{i=97}^{128} K[i] \times 2^{i-96}\right)/2^{32}$

$c_5 = \left(\sum_{i=129}^{160} K[i] \times 2^{i-128}\right)/2^{32}$, $c_6 = \left(\sum_{i=161}^{192} K[i] \times 2^{i-160}\right)/2^{32}$, $c_7 = \left(\sum_{i=193}^{224} K[i] \times 2^{i-192}\right)/2^{32}$, $c_8 = \left(\sum_{i=235}^{256} K[i] \times 2^{i-234}\right)/2^{32}$

3: $u_1 = (c_1 + c_2 + c_3 + c_4 - c_5 - c_6 - c_7 - c_8 + r) \bmod 4$, $u_2 = (c_1 + c_3 + c_5 + c_7 - c_2 - c_4 - c_6 - c_8 + r) \bmod 4$;

$u_3 = (c_1 + c_2 + c_4 + c_7 - c_3 - c_5 - c_6 - c_8 + r) \bmod 4$; $u_1 = (c_2 + c_5 + c_6 + c_8 - c_1 - c_3 - c_4 - c_7 + r) \bmod 4$;

$x_1 = (c_1 + c_3 + c_6 + c_8 - c_2 - c_4 - c_5 - c_7 + r) \bmod 1$; $x_2 = (c_1 + c_2 + c_5 + c_6 - c_3 - c_4 - c_7 - c_8 + r) \bmod 1$;

$x_1 = (c_1 + c_4 + c_5 + c_7 - c_2 - c_3 - c_6 - c_8 + r) \bmod 1$; $\varepsilon = (c_3 + c_4 + c_5 + c_6 - c_1 - c_2 - c_7 - c_8 + r) \bmod 1$.

4.2. Adding random pixels

In our algorithm, we add some random values to the plain image before encryption. These random values can influence all the pixels after matrix model M transform and diffusion operations. Since these pixels are generated randomly and are different in each encryption, the generated cipher-images are different even when a plain image is encrypted several times by the same secret key. This step enables the algorithm to strengthen the capability of resisting chosen-plaintext attack.

The number of random pixels depends on the size of the

plain image. When the number of all pixels is less than 16, the algorithm needs to reach the number of total pixels to 16. When the number of all pixels is greater than 16, after adding random pixels, the number of all pixels is L, which needs satisfy the conditions

$$\begin{cases} L \bmod 4 \equiv 0 \\ \left(\dfrac{L}{4}\right) \bmod 3 \equiv 1 \end{cases} \rightarrow (L-4) \bmod 12 \equiv 0. \tag{6}$$

According to Eq. (6), If $W = 256$ and $H = 256$, 12 random pixels should be added to the plain image, and if $W = 255$ and $H = 255$, then seven random pixels should be added to the plain image.

4.2.1. Matrix model M transform and row confusion

Matrix transform operation are often used in image encryption and the representative confusion algorithms are Arnold transform, magic cube transform, Fibonacci transform, and so on.[24] Chen *et al.* employed the 3D cat map to shuffle the positions of image pixels and used chaotic map to confuse the relationship between the cipher-image and the plain-image.[25] Ni *et al.* proposed a novel image encryption algorithm based on bit-level Arnold transform and hyper chaotic maps.[26] The above researches are focused on applying the matrix to change the location but not change the values of the pixels. Hence, attackers can compare the features in a histogram to get the meaningful information in the image. In this paper, we use the self-generated model M 4×4 matrix to multiply the value of pixels to improve the security of algorithm and $M = 256$. To resist the periodicity of matrix, we use four matrices to encrypt images alternately. After matrix transform, we apply the chaotic sequences to confuse the image at the row level. The method of generating model M matrix is shown as Algorithm 2. An example of a matrix and inverse matrix is given by

$$\boldsymbol{M}_1 = \begin{bmatrix} 254 & 47 & 183 & 144 \\ 117 & 180 & 34 & 235 \\ 97 & 76 & 181 & 164 \\ 6 & 197 & 227 & 35 \end{bmatrix} \text{inv},$$

$$\boldsymbol{M}_1 = \begin{bmatrix} 175 & 73 & 232 & 175 \\ 80 & 103 & 255 & 125 \\ 89 & 127 & 217 & 61 \\ 25 & 142 & 14 & 85 \end{bmatrix}.$$

The steps of matrix model M's transform and row confusion are described in Algorithm 3.

Algorithm 2. The method of generating model M matrix.

Input: the chaotic sequence generated by PCLML *MS*

Output: 4×4 model 256 matrix M_1, M_2, M_3, M_4

```
1: Generate the upper triangular matrix Up and the lower triangular matrix Low
For i = 1 to 4
    For j = 1 to 4
      if i = j   // Ensure tempUp, tempLow and 256 are prime numbers each other, if not, k++, look for the next number
          seek :   tempUp = MS(k ++) mod 256;          tempLow = MS(k++) mod 256;
          Up(i, j) = tempUp;          Low(i, j) = tempLow;
      end
      if i > j    Up(i, j) = 0;                Low(i, j) = MS(k ++);   end
      if i < j    Up(i, j) = MS(k ++);         Low(i, j) = 0;   end
    end
end
2: Generate 4×4 model 256 matrix M1, M2, M3, M4
For i = 1 to 4
    For j = 1 to 4
      M(i, j) = 0;
      For k = 1 to 4
          M(i, j) = M(i, j) + Up(i, k) * Low(k, j);      M(i, j) = mod(M(i, j), 256);
      end
    end
end
```

Algorithm 3. The step of matrix model M transform and row confusion.

Input: the plain image P

Output: matrix transform and row confusion result T

1: After adding random pixels, convert the image P into N row, 4 column, $P =$ reshape(P,N, 4).

2: Use u_1, x_1 to iterate LP system to achieve 100 data as the initial values of 100 PCLML lattices, use u_2, x_2 to iterate LP system to generate sequences as the coupling data of the PCLML lattices, and use u_4, ε as control parameters of PCLML to iterate system to get the chaotic sequence S and MS.

3: According to Algorithm 2, using MS, we can get 4 matrixes M_1, M_2, M_3, M_4. Next, do matrix model M transform.

For $i = 1 : 3 : N-3$ // every round, $i = i + 3$;

if i mod 4 = 0 $P(i : i+3,:) = (P(i : i+3,:) \times M_1)$ mod 256 end

if i mod 4 = 1 $P(i : i+3,:) = (P(i : i+3,:) \times M_2)$ mod 256 end

if i mod 4 = 2 $P(i : i+3,:) = (P(i : i+3,:) \times M_3)$ mod 256 end

if i mod 4 = 3 $P(i : i+3,:) = (P(i : i+3,:) \times M_4)$ mod 256 end

end

4: Using sequence S, realize the row confusion, and then we can get the encrypted result T.

For $i = 1$ to N $T = \text{Swap}(P(i,:), P(S(i),:))$ end

4.3. S-Box substitute and XOR diffusion

S-Box structures have high cryptographic features to resist differential cryptanalysis and applying a strong S-Box structure in encryption helps to have a secure effect.[27] By applying the algorithm in Ref. [21], we were able to construct the S-Box dynamically through the nonlinear characteristics of PCLML system. The 256 chaotic values are arranged in ascending order, and thus we can achieve the new order of each value. For example, the index of chaotic data 0.2 is 160, while after ascending sorting, the new index of 0.2 is 20. So in the generated S-Box, 20 and 160 are the corresponding relationships. To further improve the security of encryption, we constructed 4S-Boxes to substitute the pixel's value and alternated with the XOR diffuse operations. The details are shown in Algorithm 4.

Algorithm 4. The details of S-Box substitute and XOR diffusion.

Input: the encryption image T

Output: the final cipher image C

1: Convert the image T into 1 row, M column, T = reshape(T, 1, M).

2: Use PCLML chaotic sequence to generate 4 S-Boxes: S_1, S_2, S_3, S_4, and use u_3, x_3 to iterate LP system to achieve chaotic sequences LS to be applied in process of diffusion.

3: do S-Box substitute and XOR diffusion, and then we can get the cipher image C.

$i = 1$ $T(1) = S_1(T(1))$; $T(1) = \text{XOR}((T(1)), LS(1))$;

For $i = 2$ to imageSumSize

if i mod 4 = 0 $T(i) = S_1(T(i))$; $T(i) = \text{XOR}((T(i)), T(i\text{-}1)), LS(i))$; end

if i mod 4 = 1 $T(i) = S_2(T(i))$; $T(i) = \text{XOR}((T(i)), T(i\text{-}1)), LS(i))$; end

if i mod 4 = 2 $T(i) = S_3(T(i))$; $T(i) = \text{XOR}((T(i)), T(i\text{-}1)), LS(i))$; end

if i mod 4 = 3 $T(i) = S_4(T(i))$; $T(i) = \text{XOR}((T(i)), T(i\text{-}1)), LS(i))$; end

end

4: Reshape the cipher image C into two dimensions and display.

4.4. The process of decryption

The decryption algorithm is the reverse process of encryption algorithm. We can get the decrypted image just by following the reverse steps. We need to achieve inverse matrix and inverse S-Box in decryption. The results of the encryption and decryption are shown in Fig. 6.

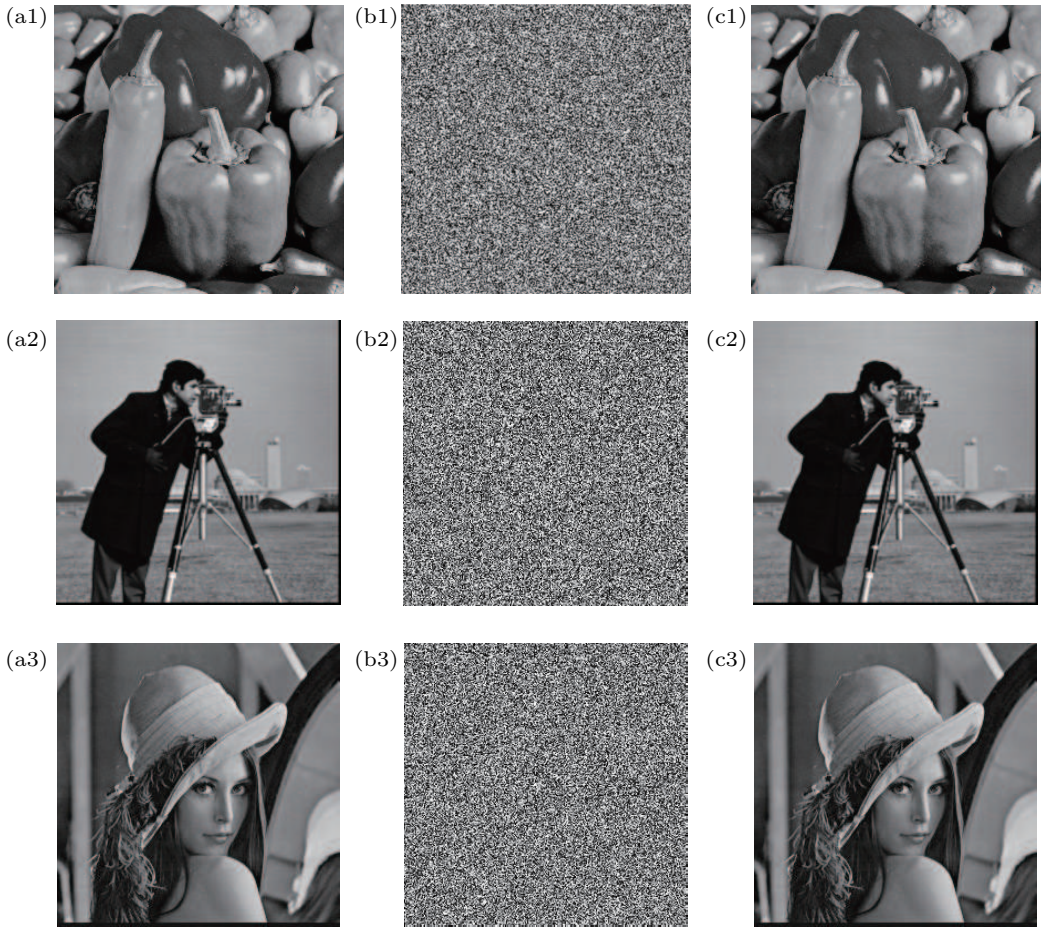


Fig. 6. The encryption/decryption results of the test dataset. (a1) Pepper, (b1) cipher image, (c1) decoding image, (a2) Camera man, (b2) cipher image, (c2) decoding image, (a3) Lena, (b3) cipher image, and (c3) decoding image.

5. Performance and security analysis

In this section, several different kinds of analysis measures are used to demonstrate the security performance of the proposed image cryptosystem. Here, we only show the experimental results of nine images with different size. They are size of 256×256: Lena and Pepper, size of 512×512: Elaine512 and Boat512, and size of 1024×1024: Testpat1k.

5.1. Key space and sensitivity analysis

As mentioned in Section 4.1, the key space of our algorithm reaches 2^{288}, which is large enough to resist brute-force attack. Moreover, the proposed algorithm should also be extremely sensitive for keys to guarantee the security of the cryptosystem. This means that the completely different plain image will be produced when we use different keys to decrypt the cipher-image. Even a tiny change in any of keys will result in a different orbit and values. Suppose that K_2 is a different key derived from the right key K_1 with one bit difference. They are given as

$K_1 =$ "C126EF1D6D859FD39E317C3AA97B89CB02537A9237F078CF2503F84F946A3B8B",
$K_2 =$ "C126EF1D6D859FD39E317C3AA97B89CB02537A9237F078CF2503F84F946A3B8C".

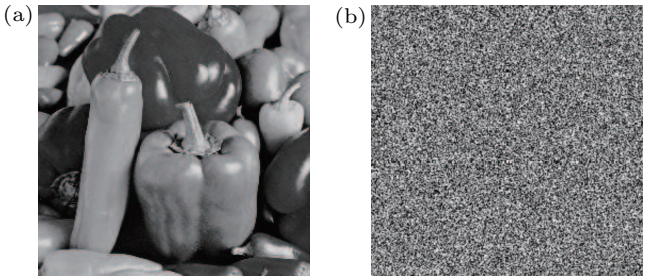


Fig. 7. The results of sensitivity analysis. (a) decrypt using key K_1 and (b) decrypt using key K_2.

The results of using K_1 and K_2 to decrypt a cipher image are displayed in Fig. 7. Figure 7(a) shows the decryption image Pepper with the right key K_1 and figure 7(b) shows the wrong decryption result using K_2. It can be said from these figures that the designed encryption system has perfect sensitivity to the key.

5.2. Information entropy analysis

Information entropy is the most important feature to provide a qualitative standard of the image randomness. The for-

mula for calculating information entropy is described by[27]

$$H(m) = \sum_{i=0}^{2^M-1} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{7}$$

where $p(m_i)$ is the occurrence probability of m_i and M is the total state of information source, which ranges from 0 to 255. The maximum amount of entropy in an image is eight. Hence, an image with a value close to eight is less able for attackers to use to decode cipher images. The entropy values of different original images are listed in Table 1, which demonstrates that all entropies are close to eight.

Table 1. Information entropy of encrypted images.

Image	Lena	Pepper	Elaine512	Boat512	Testpat1k
Entropy	7.9974	7.9973	7.9992	7.9993	7.9998

Meanwhile, the contrasting results with other algorithms in entropy are shown in Table 2. It can be seen from this that our scheme achieves higher information entropy than these existing results. Therefore, our proposed algorithm has better random distributions against entropy attack and information leakage.

Table 2. Comparison in information entropy.

Encryption methods	Entropy
Ref. [23]	7.9972
Ref. [27]	7.9567
Ref. [29]	7.9972
Our scheme	7.9986

5.3. Histogram of the image

Histogram analysis gives a straightforward result to show how uniformly pixels of an image distribute. A good image algorithm should make the histogram of the cipher image as flat as possible. Histograms of plain image and cipher image are plotted in Fig. 8. From Fig. 8(b), it is clear that the encryption cipher image result does not provide any information about gray values distribution, which can resist any statistical attacks.

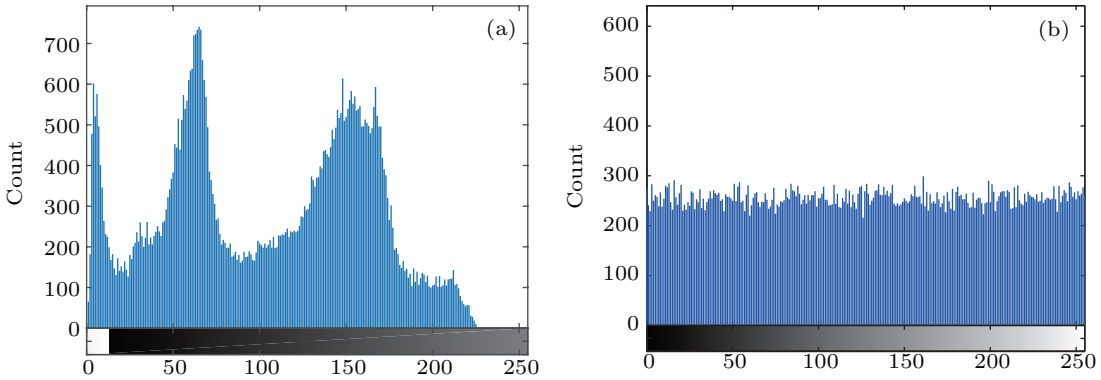


Fig. 8. (color online) Histograms of the Pepper image. (a) Histogram of the plain image and (b) histogram of the cipher image.

5.4. Correlation of adjacent pixels

The adjacent pixels of digital images have strong correlation in horizontal, vertical, and diagonal directions. A secure encryption algorithm should transform the original images into encrypted images with lower or no correlation between adjacent pixels. To analyze this feature, we choose 3000 pairs of adjacent pixels to illustrate the correlation coefficients (CC) r_{xy} of each pair, calculated as[29]

$$\mathrm{cov}(x,y) = E\{(x-E(x))(y-E(y))\}, \tag{8}$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{9}$$

where x and y are the values of two adjacent pixels in the image,

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{10}$$

and

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2. \tag{11}$$

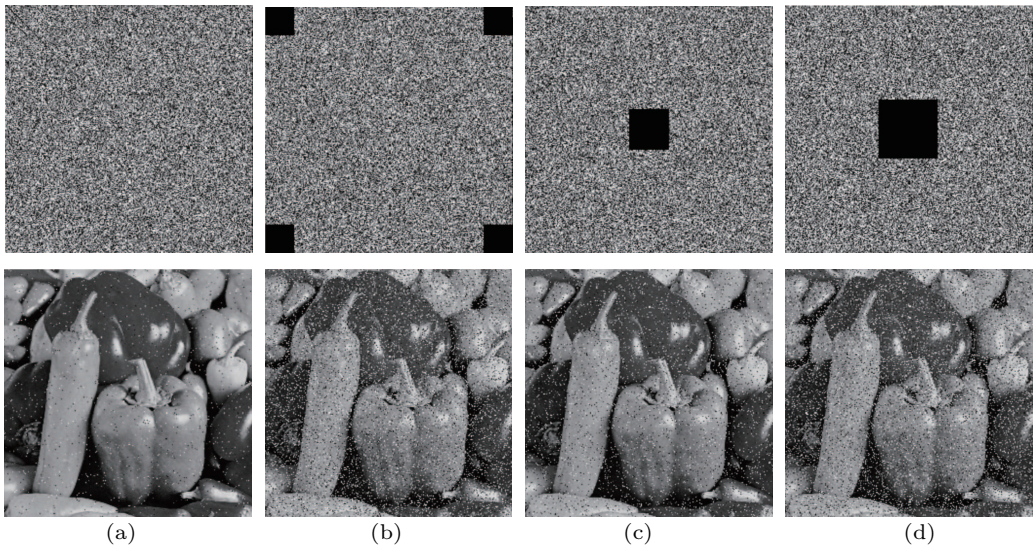
The average values of each group and details are described in Table 3. Furthermore, we also do the contrast experiments with different image encryption schemes. The measured CC of the cipher image is nearly 0, which indicates the effectiveness of the proposed scheme to prevent statistical attacks.

5.5. Robustness to noise and data loss

During the transmission or storage through networks and the physical channel, the image is easily contaminated by noise or has the risk of the data loss.[27,28,30] A good cryptosystem should be robust against data loss or noise jamming. In Fig. 9(a), we randomly changed 2% of the pixel values. Figures 9(b)–9(d) show the decryption results of cipher image in different locations and numbers of data loss. As can be observed, the decryption process can still recover most of the image information, so that it has high robustness to resist noise and data loss attack.

Table 3. The adjacent pixel's CC of plaintext and cipher image in three directions.

Algorithm		Plaintext			Cipher		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Our proposed algorithm	Lena	0.9719	0.9426	0.9199	0.0102	0.0067	0.0052
	Pepper	0.9639	0.9575	0.9331	0.0081	0.0034	0.0041
	Elaine512	0.9729	0.9757	0.9689	0.0038	0.0063	0.0036
	Boat512	0.9717	0.9388	0.9233	0.0056	0.0038	0.0063
	Testpat1k	0.7967	0.7579	0.7001	0.0030	0.0050	0.0018
Our Mean					0.0061	0.0050	0.0042
Ref. [23]					0.0015	0.0032	0.0008
Ref. [25]					0.01183	0.0002	0.0148
Ref. [29]					0.0127	0.0190	0.0012



(a) (b) (c) (d)

Fig. 9. Robustness analysis results of noise and data loss. (a) 2% noise, (b) 5.5% data loss, (c) 2.5% data loss, and (d) 5.5% data loss.

5.6. Differential attack

To resist differential attack, any tiny modification in the plain image should cause a substantial change in the cipher image. Two common quantitative measures are usually used: number of pixels change rate (NPCR) and unified average changing intensity (UACI). They are defined as

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{12}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\%, \tag{13}$$

where E_1 and E_2 are the two cipher images whose corresponding plain images have only one pixel difference under the same key and

$$D(i,j) = \begin{cases} 0, & \text{if} \quad (E_1(i,j) = E_2(i,j)), \\ 1, & \text{if} \quad (E_1(i,j) \neq E_2(i,j)). \end{cases} \tag{14}$$

When they are 8-bit grayscale images, the ideal value of NPCR and UACI are 99.6094% and 33.4635%, respectively.[10,32] NPCRs and UACIs for five simple images are listed in Table 4. Table 5 shows the NPCR and UACI values of different image encryption schemes and our experiment results are comparable with these state-of-the-art algorithms. We have found that the average of NPCR in our proposed scheme is 99.6007% and the average UACI is 33.4300%, which are close to the ideal values. This shows that our proposed cryptosystem is able to effectively resist differential attack.[31,33,34]

Table 4. The NPCR and UACI values.

Image	Lena	Pepper	Elaine512	Boat512	Testpat1k
NPCR/%	99.5804	99.5972	99.6029	99.6219	99.6011
UACI/%	33.3561	33.4296	33.5051	33.3783	33.4810

Table 5. Comparison of different algorithms in resisting differential attacks.

Name	Ref. [23]	Ref. [27]	Ref. [29]	Our proposed
Mean NPCR /%	99.6279	99.6177	99.6510	99.6007
Mean UACI /%	33.4105	33.6694	33.4805	33.4300

6. Conclusion

This paper designs a new spatiotemporal chaos PCLML, which we named pseudo-random coupled map lattices with logistic-PWLCM map under pseudo-random method for spatial coupling connections. The purpose of our proposed LP map is used to replace the logistic map. The results of our

comparisons show that the LP system has larger key space, no blank windows, and more uniform data distribution. The criteria, such as the Kolmogorov–Sinai entropy density and universality, and bifurcation diagram analysis are employed to quantify the complexity of the system's behaviors in the proposed PCLML model.[35,36] In comparison with the CML system, we obtain the new features in PCLML system, such as larger parameter space, better random sequences, and no periodic windows. These features ensure that it is more suitable for encryption. Furthermore, we use PCLML system to encrypt n image by combining some new methods of image preprocessing, such as adding random pixels, matrix model M transform, and dynamic S-Box technology. Several different kinds of analysis measures are used, including key space and sensitivity, information entropy, histogram, and robustness to noise, data loss, and differential attack. Our security analysis and simulation results prove that our new algorithm offers a powerful method against potential attacks and has excellent encryption performance.

References

[1] Zheng Y and Jin J 2015 *Multimed. Tools Appl.* **74** 1
[2] Kanakov O, Laptyeva T and Tsimring L 2016 *Physica D* **318** 116
[3] Khellat F, Ghaderi A and Vasegh N 2011 *Chaos Soliton. Fractals.* **44** 934
[4] Danca M F, Aziz-Alaoui M A and Small M 2015 *Chin. Phys. B* **24** 060507
[5] Guedes A V and Savi M A 2010 *Phys. Scr.* **81** 387
[6] Poria S, Shrimali M D and Sinha S 2008 *Phys. Rev. E* **78** 417
[7] Chen Y, Xiao J and Wu Y 2010 *Phys. Lett. A* **374** 3185
[8] Zhang Y Q and Wang X Y 2013 *Nonlinear Anal. -Model.* **18** 526
[9] Zhang Y Q, Wang X Y and Liu J 2016 *Opt. Laser. Eng.* **82** 95
[10] Hua Z and Zhou Y 2016 *Inform. Sci.* **339** 237
[11] Sam I S, Devaraj P and Bhuvaneswaran R S 2012 *Multimed. Tools Appl.* **56** 315
[12] Xie J, Yang C and Xie Q 2009 *Int. Conf. Netw. Security IEEE* 111
[13] Wu X, Li Y and Kurths J 2015 *PLoS One* **10** 1
[14] Zhen P, Zhao G and Min L 2016 *Multimed. Tools Appl.* **75** 6303
[15] Li X, Zhou C and Xu N 2018 *Int. J. Network Security* **20** 110
[16] Ercan S and Cahit C 2011 *Inform. Sci.* **181** 227
[17] Bechikh R, Hermassi H and Abd A A 2015 *Signal Process. Image* **39** 151
[18] Liu H, Kadir A and Niu Y 2014 *Int. J. Electron. Commun.* **68** 676
[19] Zhang L M, Sun K H, Liu W H and He S B 2017 *Chin. Phys. B* **26** 100504
[20] Hussain I, Shah T and Gondal M A 2013 *Nonlinear Dynam.* **71** 133
[21] Cao X M, Chen H S and Wang S H A 2017 *Comput. Sci.* **44** 107
[22] Zhou Y, Bao L and Chen C P 2014 *Signal Process.* **97** 172
[23] Li Y, Wang C and Chen H 2017 *Opt. Laser. Eng.* **90** 238
[24] Zhang L N 2013 *Sci. Technol. Eng.* **13** 2555
[25] Chen G, Mao Y and Chui C K 2004 *Chaos Soliton. Fract.* **21** 749
[26] Danca F M and Tang W K S 2016 *Chin. Phys. B* **25** 010505
[27] Sun F, Liu S and Li Z 2008 *Chaos Soliton. Fract.* **38** 631
[28] Niyat A Y, Moattar M H and Torshiz M N 2017 *Opt. Laser. Eng.* **90** 225
[29] Liao X F, Lai S Y and Zhou Q 2010 *Signal Process.* **90** 2714
[30] Yu M Y, Sun K H, Liu W H and He S B 2018 *Chaos Soliton. Fract.* **106** 107
[31] Liu W H, Sun K H and He S B 2017 *Nonlinear Dynam.* **89** 2521
[32] Liu W H, Sun K H and Zhu C X 2016 *Opt. Laser. Eng.* **84** 26
[33] Liu W H, Sun K H, He Y and Yu M Y 2017 *Int. J. Bifurcat. Chaos* **27** 1750171
[34] Cao C, Sun K H and Liu W H 2018 *Signal Process.* **143** 122
[35] Liu S and Zhang F 2014 *Nonlinear Dynam.* **76** 1087
[36] Sun F and Liu S T 2009 *Chaos Soliton. Fract.* **41** 2216