Multimedia Tools and Applications (2024) 83:10481–10502
https://doi.org/10.1007/s11042-023-16031-3

A new spatiotemporal chaos model and its application in bit-level image encryption

Xingyuan Wang[1,2] · **Maochang Zhao**[1]

Received: 18 October 2021 / Revised: 24 April 2023 / Accepted: 12 June 2023 /
Published online: 22 June 2023

Abstract
With the development of network technology, multimedia security has attracted extensive attention. Although chaotic system is widely used in this field because of its own characteristics, designing a more secure and efficient chaotic system and encryption algorithm has great application potential. In this paper, a new spatiotemporal chaos model, dynamic coupled perturbation map lattice (DCPML), is proposed. The variable function is introduced to replace the coupling input variable of spatiotemporal chaotic system, and the output of two-dimensional Logistic map is used as dynamic coupling coefficient and disturbance term to improve the pseudo randomness and chaos of the system. Through a series of analysis, it is proved that the model has excellent chaotic characteristics. The system is applied to chaotic encryption, and a new bit-level image encryption algorithm is designed. The algorithm breaks the correlation between pixels through bit-level confusion and diffusion operation. A large number of experiments and security analysis show that the algorithm can resist common attacks and has high security and robustness.

Keywords Multimedia security · DCPML · Image encryption · Bit-level · Security

1 Introduction

With the progress of science and technology and the development of the Internet, emerging technologies such as the Internet of things and big data have gradually entered people's life [3, 41], which has greatly facilitated people's daily life and promoted the development of society. With the increase in data volume, the risk of data leakage increases accordingly. The security of information is the primary problem of cloud computing and big data, and it is also the main problem at present. Therefore, secure communication and multimedia

✉ 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

security have become important research topics in the field of computer science. To ensure the security of multimedia information in communication, scholars have proposed many methods, including multimedia hiding technology, digital media forensics, biometrics, and so on [14]. As the most representative part of multimedia information, the digital image is also a research hotspot in the field of secure communication and multimedia information hiding. Scholars have also proposed many protection strategies, such as image encryption [28, 30] and image watermarking [19]. In recent years, the emergence of chaotic cryptography, which combines chaos theory with cryptography, can better meet the security needs of the image field.

Chaos theory originated in 1960s, which was put forward by Lorenz [18], an American meteorologist, when he studied atmospheric flow. Chaos has many good properties such as pseudo-random and initial sensitivity. Therefore, chaos theory has an important influence in many fields, such as economics, computer science and communication [1, 8, 15]. In 1989, Kaneko [12] proposed the coupled map lattice (CML) model, which is a spatiotemporal chaotic model originated from the field of fluid mechanics. CML has been widely concerned and studied because of its excellent dynamic behavior. Khellat [13] proposed global nonlocal coupled map lattice, Meherzi [22] proposed one-way coupled map lattice, Zhang and Wang [44, 45] proposed Arnold coupled logistic map lattice (ACLML) and mixed linear-nonlinear coupled logistic map lattice (MLNCML). These spatiotemporal chaotic systems improve their chaotic performance to some extent, but there are still some shortcomings. Generating chaotic signals on machines with limited accuracy will lead to the degradation of the dynamic behavior of chaotic characteristics. Several feasible methods are proposed to solve this problem [10, 16, 27, 34], such as using higher accuracy, cascading multiple chaotic systems, etc. Common operations in image encryption [30, 39] include Arnold map, DNA coding, wavelet transform, etc. Wang [29] applied a synchronous update Boolean network to the field of image encryption and designed an image encryption algorithm. Hua [11] proposed a new 2D Logistic-adjusted-Sine map (2D-LASM). Xian [38] proposed the concept of fractal matrix and combined it with image encryption to design an encryption algorithm. Ye [42] proposed a new chaotic circuit with multi-mode resistor and applied it to encryption. However, these algorithms have some disadvantages due to their own limitations, such as the periodicity of Arnold map.

In the era of big data, image encryption is often aimed at not only one image, but multiple images. The characteristics of the spatiotemporal chaotic system just meet this demand, but the traditional CML and other systems have many shortcomings. Therefore, in order to improve the characteristics of the spatiotemporal chaos and the efficiency of image encryption algorithm, a new spatiotemporal chaotic system and encryption algorithm are proposed in this paper. A spatiotemporal chaotic system with dynamic coupling coefficient and coupling term perturbation, dynamic coupling perturbation map lattice (DCPML), is constructed. This operation enhances the pseudo-randomness of chaos to a certain extent and proves the performance of the system through various indexes. On this basis, a bit-level image encryption algorithm is designed. Through simulation and analysis, it is proved that the encryption scheme is feasible and DCPML has good cryptographic and chaotic characteristics. The overall contribution of the proposed work can be summarized as follows:

1) An improved spatiotemporal chaotic system is proposed, in which the coupling term is replaced by the perturbation function to improve the chaotic characteristics.
2) The chaotic characteristics of the proposed system are verified and applied to the field of chaotic encryption to prove the performance of the system.

3) A new bit-level image encryption algorithm is proposed, which is proved to have high security and robustness through simulation and test.
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 the related work. Section 3 introduces the proposed DCPML system and analyzes the proposed system. Section 4 introduces the application of DCPML system in image encryption. Section 5 is the experimental results and safety analysis. Finally, the conclusion is in Section 6.

2 Related work

In recent years, spatiotemporal chaotic system and image encryption have become a research hotspot [6]. Many scholars have also devoted themselves to the research in this direction and published many papers.

Zhang et al. [46] proposed a new two-dimensional nonlinear coupled map lattices and a color image encryption algorithm. The spatiotemporal chaotic system adopts spatial nonlinear coupling to replace the adjacent coupling and reduce the periodic window. However, when the coupling coefficient is in part, the chaotic characteristics will still be low. The encryption algorithm only encrypts the color image, and the object of encryption is also limited.

Wang et al. [34] proposed a nonlinear delayed feedback Logistic chaotic map (NDFL), applied it to DMLNCML, improved it, and obtained the delayed feedback dynamic mixed linear nonlinear coupling map lattice (DFDMLMCML). The spatiotemporal chaotic system has achieved good performance in chaotic characteristics and randomness. The encryption algorithm adopts the mixed encryption algorithm of pixel value, pixel bit, and binary bit. At the same time, the linear nonlinear diffusion operation is introduced to complete the scrambling and diffusion process at one time. However, due to the introduction of delayed feedback and the complex calculation of encryption, the complexity increases, and the efficiency decreases when applied to encryption.

Liu et al. [17] proposed an image encryption algorithm based on DNA dynamic coding and adaptive permutation. A new four-dimensional hyperchaotic system is designed, which has strong pseudo-randomness and a wide range of chaotic parameters. On this basis, an image encryption algorithm is designed, which adopts the methods of DNA dynamic coding, dynamic calculation, and dynamic decoding to make the operation result more unpredictable and improve the sensitivity of the algorithm to plaintext image and key. However, the cost of image encryption algorithm is high in terms of time efficiency, and the robustness of the algorithm needs to be further improved.

Yildirim et al. [43] proposed an optical device and encryption technology using chaotic system. Firstly, the circuit is used to realize the chaotic system, and an operational transmission amplifier (OTA) is designed. Then the encryption algorithm adopts the DNA encoding and decoding operation mode and expands it to greatly increase the encoding and decoding rules and operation rules. Then many security tests are carried out. The numerical test results show that the encryption algorithm can resist common attacks. However, due to the need for DNA encoding, decoding and operation, the encryption complexity is improved.

In addition, in recent years, many excellent papers on image encryption based on chaos have been published successively [7]. In Table 1, we combed the methods and

Table 1 Related work

Reference	Methodology used	Highlights
[9]	2D logistic-sine map Multi-channel orthogonal Gegenbauer moments	Large key space Good encryption effect
[5]	Optical chaotic system DNA coding Block encryption algorithm	Better security Encryption efficiency
[20]	Convolution neural network 5D conservative chaotic system	Dynamic adaptability High security
[35]	2D chaotic system Compressive sensing 3D discrete cosine transform	High encryption efficiency Novel structural design
[36]	3D hyperchaotic system Fisher-Yates scrambling DNA coding operation	Excellent resistance to differential attack
[32]	Improved wavelet optimization method Particle swarm optimization algorithm	Image adaptive encryption Correlation and information entropy are improved

highlights used in some papers. These research results have greatly promoted the efficiency and security in the field of chaos and image encryption, but these algorithms still have some shortcomings, such as Ref. [35] each encryption requires three images, which is partially limited in practical application scenarios; Ref. [36] when converting color images and DNA coding operations, the encryption efficiency of the algorithm is low. Therefore, there are still some problems to be solved in this field.

3 Introduction of DCPML model

3.1 DCPML model

The most classical CML model was proposed by Kaneko [12], and its mathematical expression can be expressed as follows:

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

where x represents the lattice in the chaotic sequence, e represents the coupling coefficient, $f(x)$ represents the Logistic map and μ represents the parameter of Logistic map, and x and e are values between 0 and 1.

In order to overcome the defect that some lattice chaotic state is weak or even not chaotic when the coupling parameters of the spatiotemporal chaotic model are in some ranges, Wang [31] proposed logistic-dynamic coupled logistic map lattice (LDCML). The difference between LDCML model and CML model is that dynamic function $L(e)$ is used instead of coupling coefficient e, where $L(e)=\gamma e(1-e)$, γ represents the parameter of Logistic map.

To enhance the pseudo-randomness of the spatiotemporal chaotic system, the output term of 2D chaotic system is used as the coupling coefficient of spatiotemporal chaos, and the coupling term is perturbed. The definition of DCPML model is as follows:

$$\begin{cases} x_{n+1}(i) = (1-e_n)f(x_n(i)) + \frac{e_n}{2}\left(f\left(\sqrt{u_n \times x_n(i-1)}\right) + f\left(\sqrt{u_n \times x_n(i+1)}\right)\right) \\ f(x) = \mu x(1-x) \\ \begin{cases} e_{n+1} = \sin\left(\pi r(u_n+3)e_n(1-e_n)\right) \\ u_{n+1} = \sin\left(\pi r(e_{n+1}+3)u_n(1-u_n)\right) \end{cases} \end{cases} \tag{2}$$

where e and u are two output terms of the 2D-LASM. The boundary condition of spatiotemporal chaos system is periodic boundary which makes space dimension i belong to [1, L].

Next, by analyzing the Kolmogorov-Sinai entropy, information entropy, and other indicators of CML and DCPML, it can be proved that DCPML has better cryptographic properties than the CML. In order to better demonstrate the advantages of the DCPML model and eliminate the influence of Logistic mapping and two-dimensional chaos, the parts with better chaotic performance are selected in terms of parameter selection., the parameter μ of Logistic map is 3.99, the parameter r of 2D chaotic map is 0.66 and the lattices number $L = 100$.

3.2 Kolmogorov-Sinai entropy analysis

Lyapunov exponent (LE) [25, 26] can be used to estimate the separation of adjacent orbits in phase space, and can be used to measure the dynamic characteristics, so it is one of the characteristics used to identify chaos. The formula is as follows:

$$\lambda = \lim \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dF(x)}{dx} \right|_{x=x_i} \tag{3}$$

where $F(x)$ is the dynamic system and i is the time sequence index.

Kolmogorov-Sinai entropy analysis can effectively show the influence of different parameters on the chaotic behavior of the system. Kolmogorov-Sinai entropy density (KED) h is used to measure the chaos of spatiotemporal chaotic system by normalized positive LE. Kolmogorov-Sinai entropy breadth (KEB) hu is proposed by Zhang to describe the proportion of chaotic lattice in the system. The calculation formulas are as follows:

$$h = \frac{\sum_{i=1}^{L} \lambda_{(i)}^{+}}{L} \tag{4}$$

$$hu = \frac{L^{+}}{L} \tag{5}$$

where L^{+} represents the number of time sequences in which LE is a positive number. The KED and KEB of CML and DCPML are shown in Fig. 1a-d respectively. The X-axis represents the coupling coefficient e. The Y-axis represents the Logistic map coefficient μ. The Z-axis is KSD and KSB. It is obvious that compared with CML system, the chaos performance of DCPML system is obviously better. With the increase of the parameter μ, the chaotic performance of the two spatiotemporal chaotic systems becomes stronger.

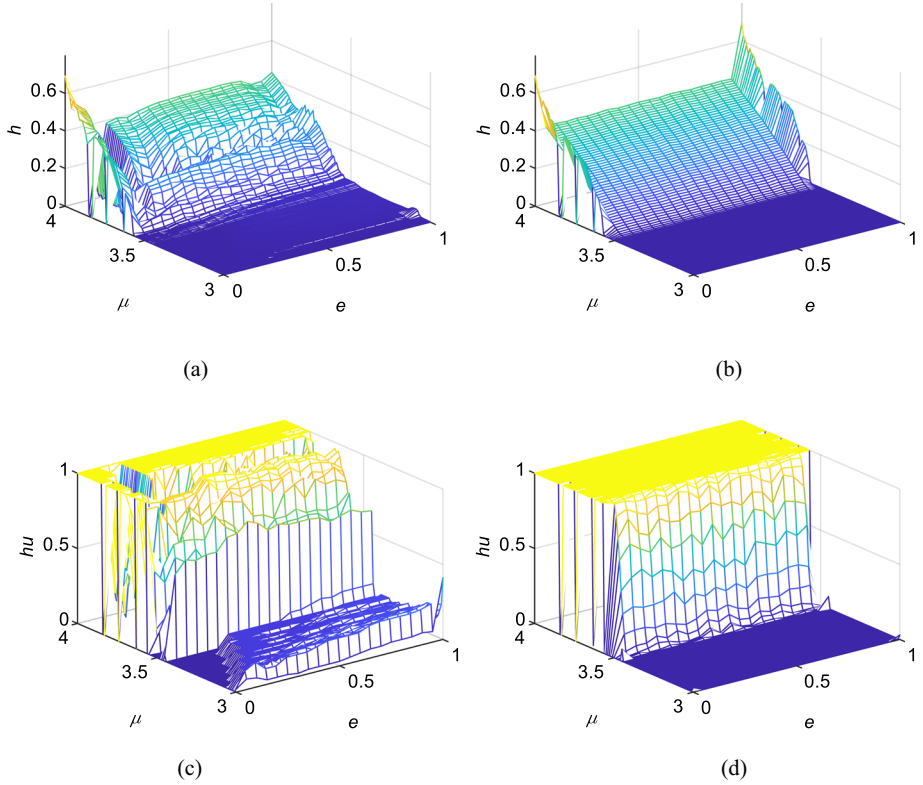

Fig. 1 KS entropy: (**a**) KED of CML; (**b**) KED of DCPML; (**c**) KEB of CML; (**d**) KEB of DCPML

However, in the two intervals of $0.1 < e < 0.2$ and $3.7 < \mu < 3.8$, the chaotic performance of CML system decreases obviously. However, the dynamic coupling coefficient and disturbance function of DCPML system improve these shortcomings, and the chaotic characteristics of DCPML system are obviously improved.

It can be seen in Fig. 2 about 75% of the parameter pairs can make DCPML system satisfy the requirement that all spatial lattices are in chaotic state, while only about 37% of the parameter pairs can make CML system satisfy the requirement. Compared with CML, DCPML has nearly 40% more parameter pairs, which can make the chaotic system completely in chaotic state. It shows that compared with CML system, DCPML system has better chaotic characteristics.

3.3 Bifurcation diagram

Bifurcation diagram is an intuitive representation of a series of period doubling generated by chaotic system under different parameters. Without losing generality, we analyze the bifurcation diagrams of the 20th, 50th and 80th lattices of CML and DCPML respectively. In Fig. 3, the bifurcation diagrams of two spatiotemporal chaotic systems are shown when the initial value of e is 0.6. It can be seen that the period window of DCPML is obviously smaller than that of CML.

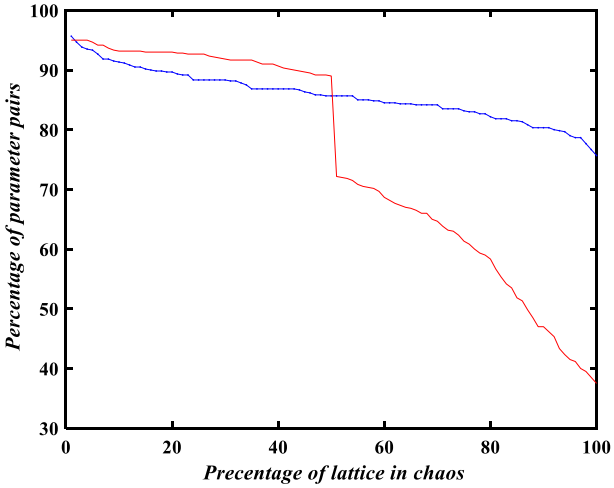

Fig. 2 Percentage of lattices in chaos for different parameter pairs in DCPML (blue) and CML (red)

3.4 Information entropy

In 1949, the concept of information entropy was proposed by Shannon [24], which can describe the randomness of dynamic system and chaotic system. Therefore, the pseudo-random sequence can be evaluated by information entropy. It can be defined as Eq. (6):

$$H(s) = -\sum_{i=1}^{n} P(s_i)\log_2 p(s_i) \tag{6}$$

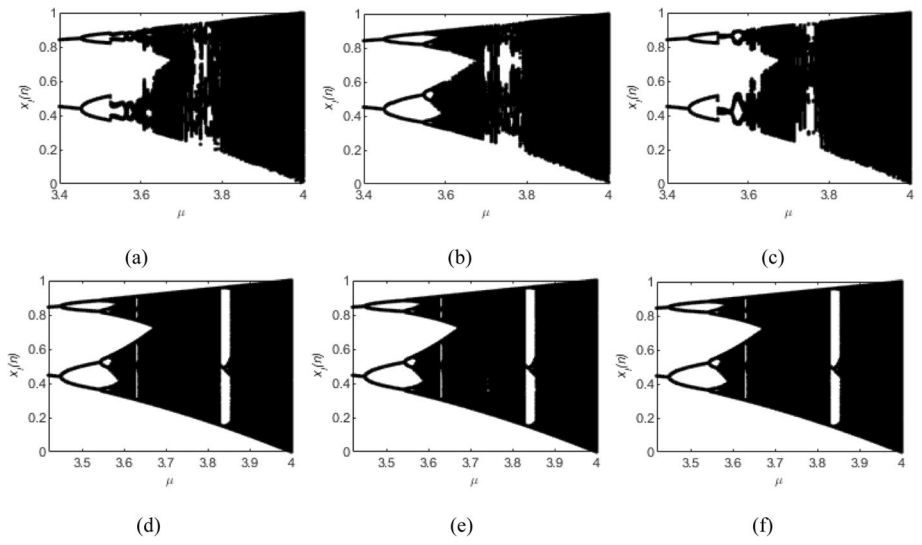

Fig. 3 Bifurcation Diagram: (**a**) 20th lattice of CML; (**b**) 50th lattice of CML; (**c**) 80th lattice of CML; (**d**) 20th lattice of DCPML; (**e**) 50th lattice of DCPML; (**f**) 80th lattice of DCPML

where s is the information source. In this paper, the number of information source states n is 10. Because the value of the sequence is between 0 and 1, the ten states are $s_1 = [0, 0.1)$, $s_2 = [0.1, 0.2)$, ..., $s_{10} = [0.9, 1]$. In addition, $p\ (s_i)$ is the probability of state s_i. Theoretically, the maximum information entropy of each lattice in spatiotemporal chaotic system is $\log_2 10 \approx 3.32$.

As shown in Fig.4a-d, the information entropy of CML and DCPML is compared when $\mu = 3.8$ and $\mu = 3.99$. It can be seen that CML system has obvious defects in these parameter ranges, while DCPML system is almost close to the ideal value in this range.

3.5 Mutual information

Mutual information can represent the independent relationship between two random variables, indicating the strength of the dependence between two variables. It can be defined as Eq. (7). According to the definition of entropy, the expansion result can be obtained, as shown in Eq. (8):

$$I(X, Y) = H(X) - H(X|Y) \tag{7}$$

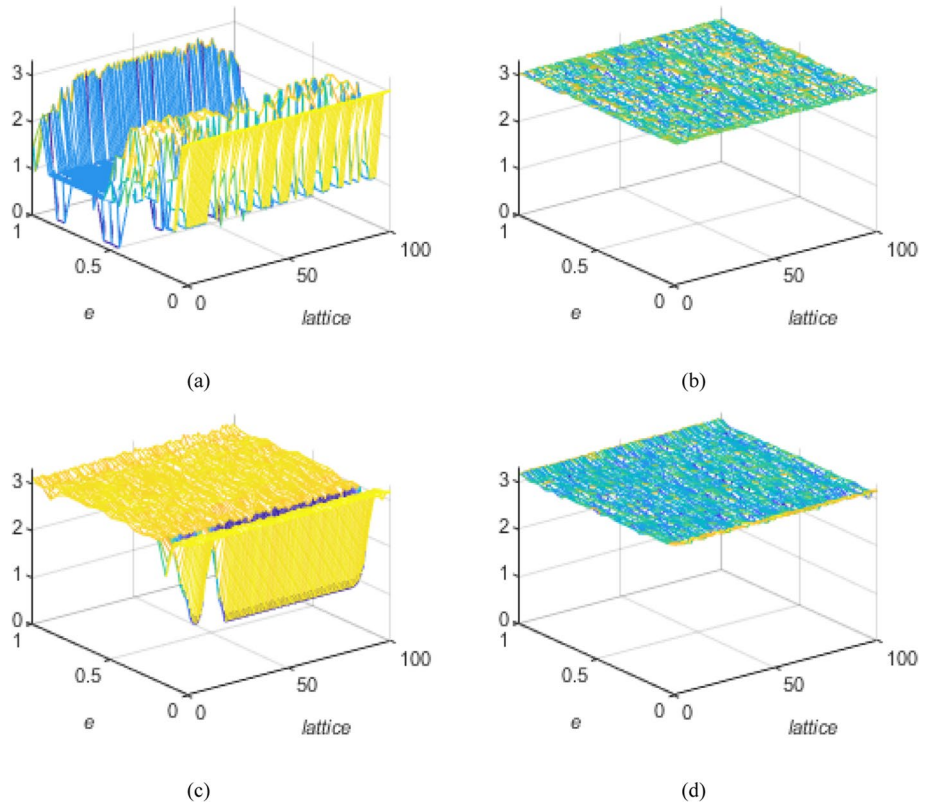

Fig. 4 Information entropy of each lattice: (**a**) The CML system at $\mu = 3.8$; (**b**) The DCPML system at $\mu = 3.8$; (**c**) The CML system at $\mu = 3.99$; (**d**) The DCPML system at $\mu = 3.99$

$$I(X,Y)=\sum_{x,y}p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \tag{8}$$

where $X=\{x_1, x_2, \ldots, x_n\}$, $Y=\{y_1, y_2, \ldots, y_n\}$, represents different time sequences in spatiotemporal chaotic system. $H(X)$ denotes the information entropy of sequence X. In spatiotemporal chaotic system, the mutual information between multiple lattices should be as low as possible to prevent the chaotic sequence of unknown lattice from being recovered based on the chaotic sequence of known lattice. To display the mutual information of the system more intuitively under different parameters, we analyze the system through average mutual information. It can be defined as Eq. (9):

$$Ld=\frac{\sum_{i=1}^{L}\sum_{j=1,j\neq i}^{L}I(x_i,y_j)}{L(L-1)} \tag{9}$$

For the convenience of analysis, let $L=10$. The average mutual information of CML and DCPML is shown in Fig. 5. When the parameters $\mu\in[3.6,4]$ and $e\in[0,1]$, more than half of CML systems have mutual information values higher than 0.5, while DCPML systems almost have mutual information values close to 0 within this parameter range.

3.6 Spatiotemporal behaviors

The traditional CML model of spatiotemporal chaotic system has six spatiotemporal modes: frozen random pattern, complete turbulence pattern, and so on. As can be seen in Fig. 6, when the parameter $\mu\geq 3.7$, DCPML system is in complete turbulence pattern. Compared with CML system, chaos is improved significantly.

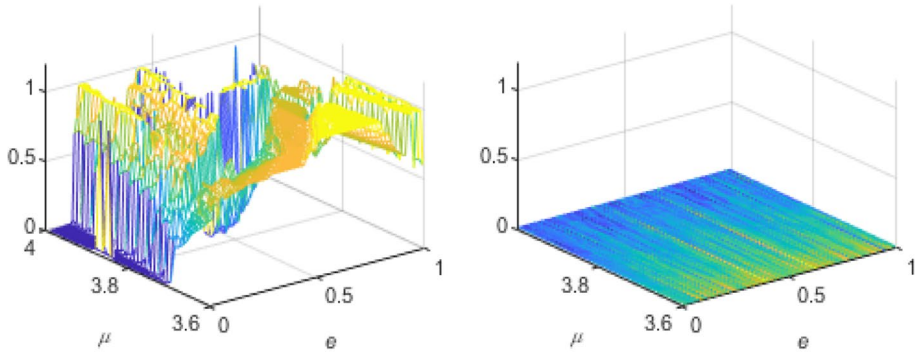

Fig. 5 Average mutual information: (**a**) CML; (**b**) DCPML

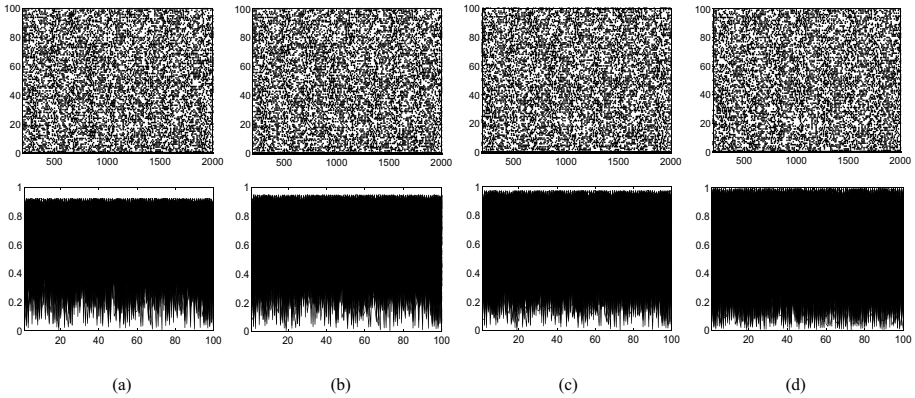

Fig. 6 Space-time diagram and space amplitude diagram of DCPML: (**a**) $\mu = 3.7$; (**b**) $\mu = 3.8$; (**c**) $\mu = 3.9$; (**d**) $\mu = 4$

4 Application in image encryption

The encryption process can be roughly divided into several parts: the generation of secret key and chaotic sequences, bit-level confusion based on DCPML system, and diffusion. After encryption, the original plain image is transformed into a noise like image, so that the information in the plain image can be protected. The brief encryption flow chart is shown in Fig. 7. Without losing generality, this section describes the detailed steps of encrypting an image of size $M \times N$.

4.1 Key and chaotic sequences generation

In order to resist violent attacks more effectively, there are certain requirements for the key, in which the length of the secret key should not be less than 2^{100} [2]. In this paper, the length of the secret key is set to 280-bits. The secret key consists of a random string K of 260-bits length and the average value of plaintext pixels. The initial value of DCPML system is determined by the first 200-bits, and the parameter of DCPML system $\{e, u, \mu\}$ are determined by the rest of the key and the average value of the plain image pixels. The specific process can refer to Algorithm 1. Without losing generality, the random string is taken as K:

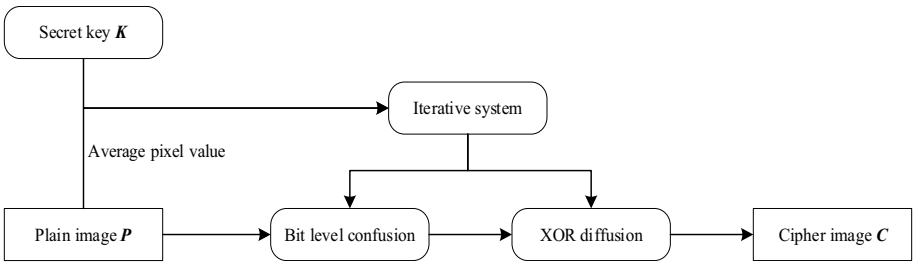

Fig. 7 Encryption flow chart

$$K = 5be9cb317c7c277c5d5b0f1e260f24f840c04f0af628d9617ad5f6b3d733e9cfd$$

According to Algorithm 1, we can get the system parameters $\{e, u, \mu\} = \{0.5489025115966, 0.5882196426391, 3.9947808265686\}$ and the initial value. By iterating DCPML system $2MN$ times, discard the values of the first 500 time to avoid the transient effect, the sequence $S1$, $S2$ and SI used for encryption is obtained.

Input: Average pixel value of plain image $\boldsymbol{Avg}$ and string $\boldsymbol{K}$ with length of 260-bits.
Output: Chaotic sequences $\boldsymbol{S1}$ and $\boldsymbol{S2}$, index sequence $\boldsymbol{SI}$.
1: The key $\boldsymbol{K}$ is divided into 13 parts ($\boldsymbol{K_i}$, $i = 1, 2, \ldots, 13$), each of which is 20 bits;
2: Calculate the initial value $\boldsymbol{Y}$ according to $\boldsymbol{K_1}$ to $\boldsymbol{K_{10}}$, $\boldsymbol{Y_i}$ = bi2de($\boldsymbol{K_i}$)/2^{20}, where bi2de represents binary to decimal;
3: Calculate $\boldsymbol{T}$ according to $\boldsymbol{avg}$, $\boldsymbol{T}$ = bi2de(floor($\boldsymbol{Avg}\times10^8$)), and then intercept the first 20 bits, where floor represents rounding down;
4: $\boldsymbol{e}$ = bi2de(bitxor($\boldsymbol{K_{11}}$, $\boldsymbol{T}$))/2^{20};
5: $\boldsymbol{u}$ = bi2de(bitxor($\boldsymbol{K_{12}}$, $\boldsymbol{T}$))/2^{20};
6: $\boldsymbol{\mu}$ = 3.95 + 0.05×bi2de(bitxor($\boldsymbol{K_{13}}$, $\boldsymbol{T}$))/2^{20};
7: Ten chaotic sequences $\boldsymbol{SC_i}$ ($i = 1, 2, \ldots, 10$) are obtained by iterating the DCPML system according to the calculated parameters $\boldsymbol{Y}$, $\boldsymbol{e}$, $\boldsymbol{u}$ and $\boldsymbol{\mu}$;
8: Sort the sequence $\boldsymbol{SC_2}$ to obtain the index sequence $\boldsymbol{SI}$ of $\boldsymbol{SC_2}$;
9: The sequence $\boldsymbol{S1}$ is calculated according to $\boldsymbol{SC_5}$, $\boldsymbol{S1}$ = floor($\boldsymbol{SC_5}\times2^{14}$) mod 8;
10: The sequence $\boldsymbol{S2}$ is calculated according to $\boldsymbol{SC_8}$, $\boldsymbol{S2}$ = floor($\boldsymbol{SC_8}\times2^{14}$) mod 256;

Algorithm 1 The generation of initial values and sequences

4.2 Bit-level confusion and diffusion

Confusion and diffusion are the two most common operations in image encryption. They can effectively destroy the correlation between image pixels and resist attacks.

Firstly, the image with the size of $M\times N$ is converted into a binary matrix with the size of $MN\times8$, and the bits of each pixel value are scrambled by cyclic shift operation. Then, each row of the matrix performs the cyclic shift operation again according to the value of sequence $S1$, and reorders the rows according to SI. Finally, perform the reverse cyclic shift operation in the first step, and convert the decimal matrix with the size of $M\times N$ to obtain the scrambled image. Algorithm 2 describes the encryption process in more detail, and Fig. 8 shows an example of the confusion process.

The diffusion adopts XOR operation. The generated chaotic sequence $S2$ is used to XOR the scrambled image and change its pixel value. The processes can be defined as:

$$C(i) = \begin{cases} C_2(i) \oplus S2(i), i = 1 \\ \big(\big(C_2(i-1) + C_2(i)\big) \bmod 256\big) \oplus S2(i), i \neq 1 \end{cases} \tag{10}$$

where $\oplus$ represents the XOR operation. After diffusion, the ciphered image C can be obtained.

Input: Plain image $\boldsymbol{P}$, sequences $\boldsymbol{S1}$, $\boldsymbol{S2}$, and $\boldsymbol{SI}$.
Output: Cipher image $\boldsymbol{C}$.
1: Obtain the size M, N of image $\boldsymbol{P}$;
2: The image $\boldsymbol{P}$ is converted into a binary matrix with a size of MN rows and 8 columns;
3: Perform an upward cyclicshift of 8-i times for each column, $\boldsymbol{P}_i$ = circshift_up($\boldsymbol{P}_i$, 8-i), where i represents the index of the column;
4: Create a matrix $\boldsymbol{C}_1$ as large as $\boldsymbol{P}$;
5: Perform a right cyclicshift on each row of $\boldsymbol{P}$, according to $\boldsymbol{S1}$, and put the result in $\boldsymbol{C}_1$;
6: **for** i = 1:MN **do**
7: $\quad \boldsymbol{C}_1(\boldsymbol{SI}(i), :)$ = circshift_right($\boldsymbol{P}_i$, $\boldsymbol{S1}(i)$);
8: **end for**
9: Perform the reverse operation in Step 3, and then convert it to decimal to obtain the scrambled image $\boldsymbol{C}_2$;
10: Diffuse it according to Eq. (10) to obtain the final cipher image $\boldsymbol{C}$;

Algorithm 2 Bit-level confusion and diffusion

5 Simulation results and security analysis

In this algorithm, the main time-consuming parts are chaos iteration, confusion and diffusion. When the encrypted image size is $M \times N$. The time complexity of iterative chaotic system is O($M \times N$). In the confusion stage, the time complexity of cyclic shift and index permutation is O($8M \times N$). In the diffusion phase, the time complexity of bit-level XOR is O($M \times N$). Therefore, the time complexity is O($10M \times N$).

In order to prove the feasibility and security, common security experiments are done on the encryption algorithm, and its security is analyzed and verified. The encryption

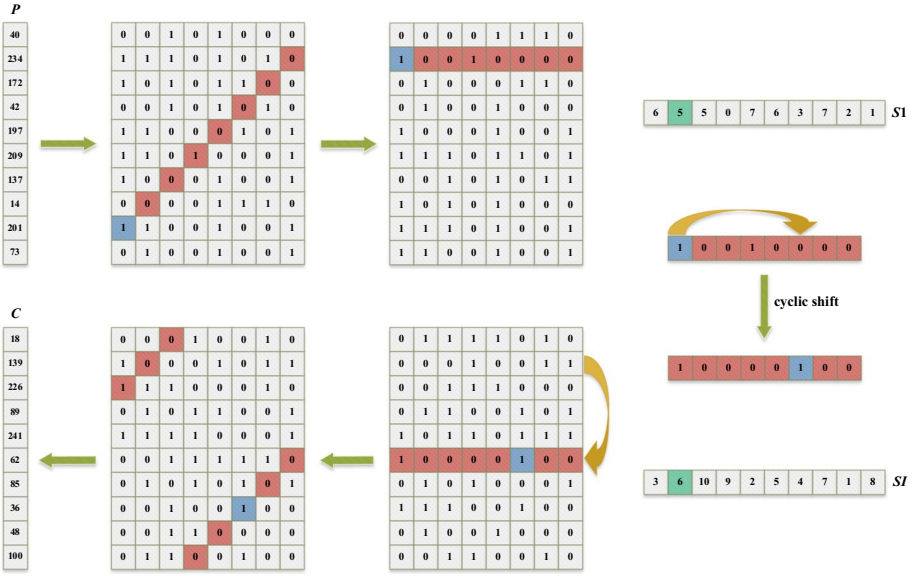

Fig. 8 A example of bit-level confusion

and decryption program are implemented with MATLAB 2020A. The operating system and configuration are Windows 10 and 8 GB RAM.

5.1 Simulation results

In Fig. 9, we give the simulation results of gray image, binary image and color image, and the gray histogram of images. From Fig. 9a and c, we can see that the plain image becomes a noise like image after encryption. By using the correct key to decrypt the cipher image, the original image can be restored to the original image losslessly. Comparing the histogram of plain image and cipher image, we can find that the gray histogram of encrypted image is more uniform, and the attacker cannot obtain effective information from it.

5.2 Secret key analysis

A secure encryption algorithm should not only ensure the size of the secret key space, but also ensure the sensitivity to the secret key. Even if the secret key changes slightly, the image encrypted twice will be greatly different, or the image decrypted with two secret keys will be completely different. Here we select K as the correct key, $K1$ is a key slightly different from K:

$$K = 5be9cb317c7c277c5d5b0f1e260f24f840c04f0af628d9617ad5f6b3d733e9cfd$$
$$K1 = 5be9cb317c7c277c5d5b0f1e260f24f840c04f0af628d9617ad5f6b3d733e9cf6$$

The key sensitivity analysis results are shown in Fig. 10. Among them, Fig. 10b and c are the results of encryption using secret key K and $K1$ respectively, Fig. 10d is the absolute

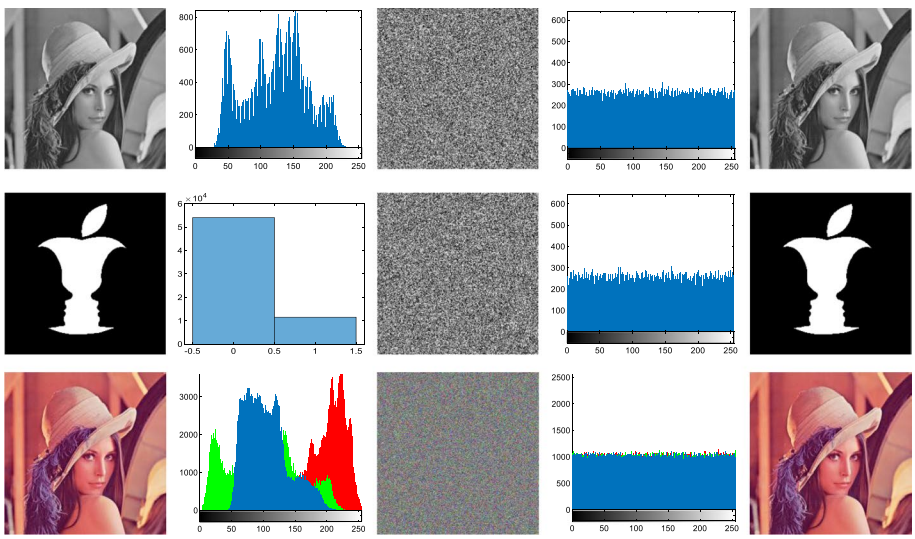

Fig. 9 Simulation results: (**a**) Plain images; (**b**) Histogram of (a); (**c**) Encryption of (a); (**d**) Histogram of (c); (**e**) Decryption of (c)

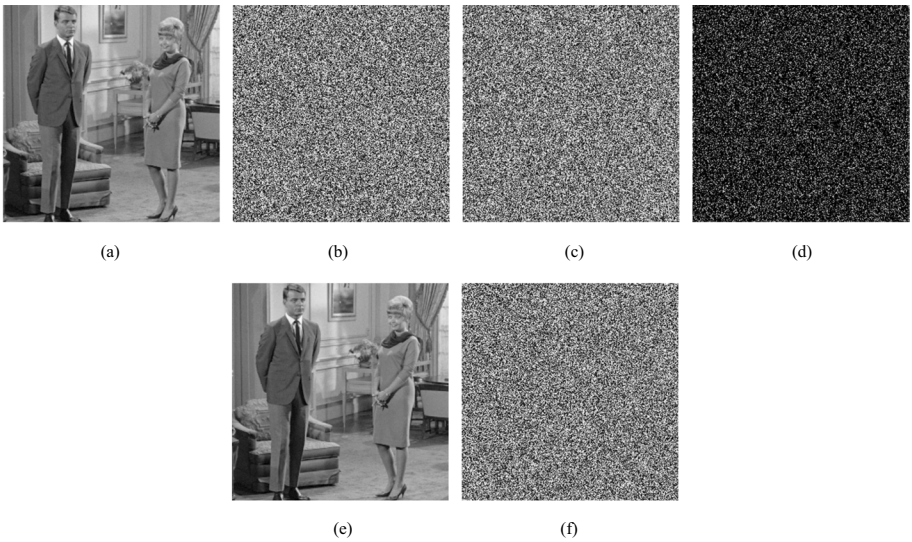

Fig. 10 Key sensitivity analysis: (**a**) Plaintext image; (**b**) Image encrypted with K; (**c**) Image encrypted with $K1$; (**d**) The difference between (b) and (**c**); (**e**) Image decrypted with K; (**f**) Image decrypted with $K1$

value of the difference between the pixel values of the two cipher images encrypted with two secret keys, and Fig. 10e and f are the results of using two keys to decrypt the image encrypted with K, respectively. Even if the key change is very small, the difference between encryption and decryption is very large.

5.3 Statistical analysis

5.3.1 Correlation analysis

In the plain image with visual significance, there is a strong correlation because of the small difference between the pixel values of adjacent pixels, which has a certain security risk. One of the most important tasks in image encryption is to break the correlation to resist the attacker's statistical analysis attack. The calculation formula is as follows:

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

where x and y are the pixel values of two adjacent pixels in the correlation analysis. $E(x)$ and $D(x)$ are defined as follows:

$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \end{cases} \tag{12}$$

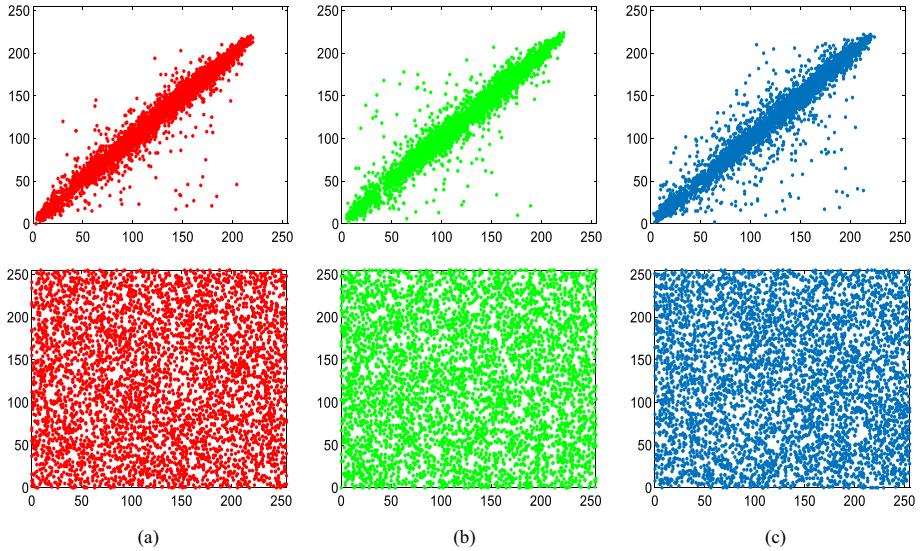

Fig. 11 Correlation coefficients: (**a**) Horizontal correlation of Pepper's plain image and cipher image; (**b**) Vertical correlation of Pepper's plain image and cipher image; (**c**) Diagonal correlation of Pepper's plain image and cipher image

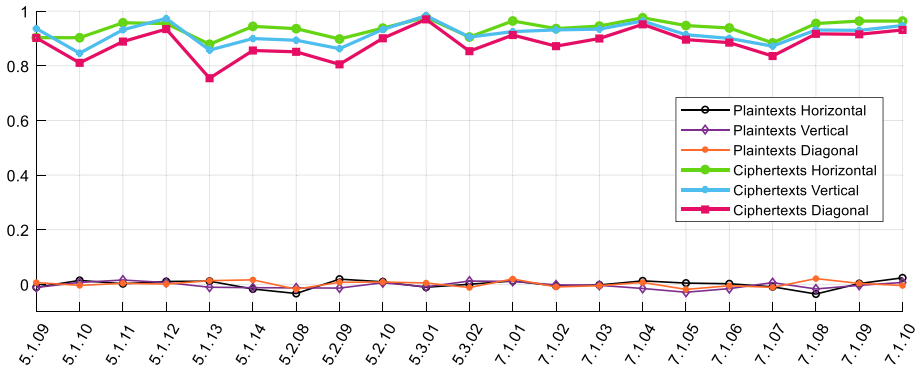

Fig. 12 Correlation coefficients

where N is the total number of randomly selected pixels. In this paper, 5000 pairs of adjacent pixels are randomly selected to verify the ability of the algorithm to break the pixel correlation. The correlation test results of Pepper's plain image and cipher image in three directions are shown in Fig. 11. From the test results, it can be seen that the proposed algorithm can well break this correlation.

Figure 12 shows the correlation coefficients of 21 images from the USC-SIPI miscellaneous image database. It can be seen from Fig. 12, the correlation between adjacent pixels of plain images of these images is between 0.8 and 1, which is very strong, while the correlation between adjacent pixels of encrypted images is between −0.1 and 0.1, which is almost zero. In Table 2, the average correlation is compared with other

Table 2 Compared with other algorithms

Algorithms	Direction		
	Horizontal	Vertical	Diagonal
Ref. [32]	0.0022	−0.0020	0.0018
Ref. [40]	−0.0059	0.0013	0.0003
Ref. [4]	0.0020	−0.0046	0.0029
Ref. [33]	0.0018	−0.0024	0.0033
Proposed	−0.00014	−0.00430	0.00110

algorithms. It can be seen that the proposed algorithm has lower average correlation and stronger resistance to statistical attacks.

5.3.2 Information entropy

The definition of information entropy is as Eq. (6) in Section 3.4. For the signal source with 2^N signals, the ideal value should be N. In this section, information entropy is used to evaluate the disorder and randomness of cipher image pixel values. Table 3 and Table 4 gives the test results and comparison with the other three algorithms. It can be

Table 3 Information entropy

Image	Ref. [4]	Ref. [23]	Proposed
5.1.09	7.9974	7.9975	7.9973
5.1.10	7.9971	7.9973	7.9973
5.1.11	7.9973	7.9977	7.9968
5.1.12	7.9974	7.9976	7.9975
5.1.13	7.9971	7.9974	7.9975
5.1.14	7.9971	7.9977	7.9973
5.2.08	7.9994	7.9994	7.9993
5.2.09	7.9993	7.9994	7.9992
5.2.10	7.9992	–	7.9993
7.1.01	7.9993	7.9994	7.9993
7.1.02	7.9993	7.9993	7.9993
7.1.03	7.9994	7.9993	7.9993
7.1.04	7.9993	7.9994	7.9993
7.1.05	7.9993	7.9994	7.9994
7.1.06	7.9994	7.9994	7.9992
7.1.07	7.9993	7.9994	7.9994
boat.512	7.9993	7.9993	7.9993
gray21.512	7.9994	–	7.9993
ruler.512	7.9993	7.9993	7.9993
5.3.01	7.9998	7.9998	7.9998
5.3.02	7.9998	7.9998	7.9998
7.2.01	7.9998	–	7.9998

Table 4 Information entropy

Ref.	Ref. [4]	Ref. [23]	Ref. [33]	Proposed
Avg.	7.9988	7.9987	7.9986	7.9989

seen that the information entropy of the image encrypted by this algorithm is above 7.99, indicating that the pixel value of the encrypted image has strong randomness.

5.4 Differential attack

Differential attack is to encrypt the plain image with small change, and then analyze the difference between these encrypted images to crack the encryption algorithm. It is a selective plaintext attack. The diffusion operation can amplify the small changes and make the pixels interact with each other, to achieve the complete avalanche effect. The pixel number change rate (NPCR) refers to the degree of difference between two images. The calculation method is the number of pixels with the same position but different pixel values divided by the total number of pixels in two images with the same total number of pixels. Unified average intensity of change (UACI) refers to the sum of the absolute value of the pixel value difference at the corresponding position of two images divided by the product of pixel level and total number of pixels. NPCR and UACI are used to evaluate the differential attack capability of encryption algorithms. They are defined as follows:

$$\boldsymbol{NPCR} = \frac{\sum_{i,j} E(i,j)}{TP} \times 100\% \tag{13}$$

$$\boldsymbol{UACI} = \frac{1}{TP} \sum_{i,j} \frac{\left| C_1(i,j) - C_2\left(i,j\right) \right|}{255} \tag{14}$$

where TP is the number of pixels. C_1 and C_2 are cipher images of the two images. If $C_1(i, j)$ is equal to $C_2(i, j)$, then $E(i, j)$ is equal to 0; otherwise, $E(i, j)$ is equal to 1.

N_α^* and U_α^* are the two critical values [37]. In the NPCR and UACI test, in order to limit the change rate to the image and the change intensity of the pixel value of the encryption algorithm, the value of NPCR must larger than N_α^*, the value of UACI is in the interval $(U_\alpha^{*-}, U_\alpha^{*+})$. They are defined as Eq. (15) and Eq. (16).

$$N_\alpha^* = \frac{L - \Phi^{-1}(\alpha)\sqrt{L/RC}}{L+1} \tag{15}$$

$$\begin{cases} U_\alpha^{*-} = \frac{L+2}{3L+3} - \boldsymbol{\Phi}^{-1}(\alpha/2) \times \sqrt{\frac{(L+2)\left(L^2+2L+3\right)}{18(L+1)^2 \times L \times MN}} \\ U_\alpha^{*+} = \frac{L+2}{3L+3} + \boldsymbol{\Phi}^{-1}(\alpha/2) \times \sqrt{\frac{(L+2)\left(L^2+2L+3\right)}{18(L+1)^2 \times L \times MN}} \end{cases} \tag{16}$$

Table 5 NPCR and UACI

Image	NPCR				UACI			
	Ref. [4]	Ref. [23]	Ref. [21]	Proposed	Ref. [4]	Ref. [23]	Ref. [21]	Proposed
256×256	$N_\alpha^* \geq 99.5693\%$				$U_\alpha^{*-} = 33.2824\%, U_\alpha^{*+} = 33.6447\%$			
5.1.09	99.61	99.62	99.6048	99.6323	33.53	33.46	33.3625	33.4561
5.1.10	99.60	99.61	99.6559	99.6124	33.49	33.45	33.3902	33.5674
5.1.11	99.62	99.64	99.6394	99.6078	33.47	33.46	33.4063	33.4934
5.1.12	99.61	99.62	99.6484	99.6185	33.51	33.44	33.4420	33.4669
5.1.13	99.60	99.61	99.5808	99.5956	33.42	33.42	33.3664	33.4151
5.1.14	99.60	99.61	99.6244	99.6292	33.42	33.47	33.3671	33.4585
512×512	$N_\alpha^* \geq 99.5893\%$				$U_\alpha^{*-} = 33.3730\%, U_\alpha^{*+} = 33.5541\%$			
5.2.08	99.61	99.59	99.6093	99.6193	33.47	33.46	33.3765	33.4772
5.2.09	99.59	99.61	99.6161	99.6178	33.51	33.45	33.4688	33.4369
5.2.10	99.62	–	99.6139	99.6323	33.43	–	33.4527	33.4081
7.1.01	99.60	99.62	99.5923	99.6204	33.54	33.46	33.4610	33.4324
7.1.02	99.60	99.61	99.5999	99.6101	33.49	33.44	33.5514	33.4435
7.1.03	99.62	99.61	99.6127	99.5975	33.40	33.42	33.4992	33.4653
7.1.04	99.61	99.60	99.6044	99.6113	33.48	33.46	33.4768	33.4360
7.1.05	99.62	99.61	99.5915	99.6159	33.45	33.48	33.4172	33.4468
7.1.06	99.62	99.59	99.6230	99.6162	33.48	33.47	33.4495	33.4857
7.1.07	99.62	99.61	99.5938	99.6086	33.53	33.47	33.5062	33.4385
boat.512	99.62	99.60	99.5961	99.6078	33.48	33.45	33.4079	33.4853
gray21.512	99.62	–	99.6052	99.6227	33.55	–	33.4522	33.4007
ruler.512	99.61	99.62	99.6067	99.6216	33.41	33.44	33.4252	33.4343
1024×1024	$N_\alpha^* \geq 99.5994\%$				$U_\alpha^{*-} = 33.4183\%, U_\alpha^{*+} = 33.5088\%$			
5.3.01	99.61	99.61	99.6119	99.6024	33.45	33.45	33.4263	33.4902
5.3.02	99.61	99.61	99.6124	99.6009	33.46	33.47	33.4765	33.4440
7.2.01	99.61	–	99.6079	99.6059	33.48	–	33.4910	33.4598
Mean	99.6104	99.6105	99.6119	99.6139	33.4750	33.4536	33.4449	33.4565
Std	0.00898	0.01129	0.01730	0.01037	0.04273	0.01640	0.05387	0.03579

where $\Phi^{-1}(\cdot)$ is inverse cumulative density function of standard normal distribution N (0, 1). In the NPCR test, the value of NPCR must larger than N_α^*, the value of UACI is in the interval $(U_\alpha^{*-}, U_\alpha^{*+})$.

Table 6 NPCR

Image size	NPCR				
	Ref. [4]	Ref. [23]	Ref. [21]	Ref. [33]	Proposed
256×256	99.6066	99.6183	99.6256	99.6042	99.6159
512×512	99.6123	99.6064	99.6045	99.6034	99.6155
1024×1024	99.6100	99.6100	99.6107	–	99.6030
Mean	99.6104	99.6105	99.6119	99.6038	99.6139
Std	0.00898	0.01129	0.01730	–	0.01037

Table 7 UACI

Image size	UACI				
	Ref. [4]	Ref. [23]	Ref. [21]	Ref. [33]	Proposed
256×256	33.4733	33.4500	33.3890	33.4748	33.4762
512×512	33.4784	33.4546	33.4572	33.4444	33.4454
1024×1024	33.4633	33.4600	33.4646	–	33.4646
Mean	33.4750	33.4536	33.4449	33.4596	33.4565
Std	0.04273	0.01640	0.05387	–	0.03579

In Tables 5, 6 and 7, we list the experimental results of this algorithm on some images in the image database, and list and compare three more advanced algorithms. It can be seen that the average value and standard deviation of this algorithm are better than other algorithms, and it also has a good performance in the passing rate.

5.5 Robustness analysis

In the process of communication, all kinds of interference often lead to the loss of information in the cipher image, destroy the integrity of the transmitted information, and make the receiver unable to obtain the information in the original image. A robust encryption algorithm can ensure that when this happens, the damaged part of the cipher in the process of information transmission has as little impact on decryption as possible. Therefore, robustness is very important for encryption algorithm. The common malicious attacks mainly include clipping attack and noise attack. In this paper, we simulate the resistance to different degrees of clipping attack and salt & pepper noise attack. Image encryption scheme should be able to minimize the impact of data loss on decryption. In Fig. 13, the decryption results of cipher image after 1/16, 1/8, 1/4,

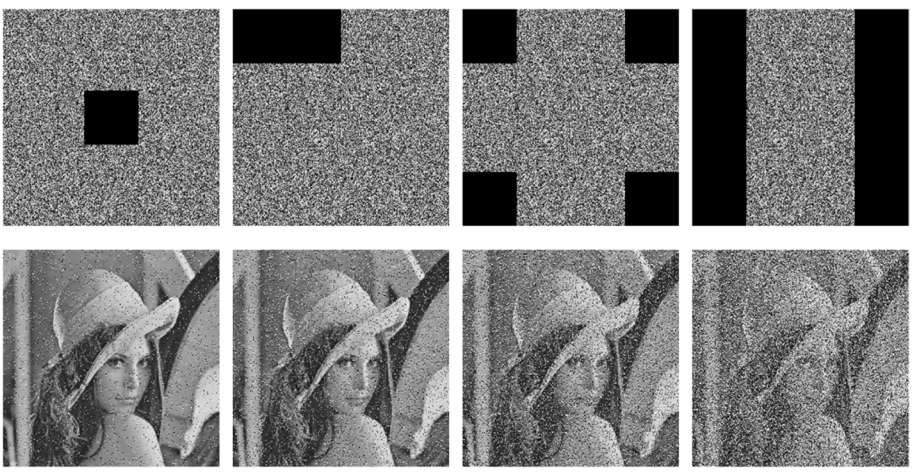

Fig. 13 Clipping attack: (**a**) 1/16-degree clipping; (**b**) 1/8-degree clipping; (**c**) 1/4-degree clipping; (**d**) 1/2-degree clipping

Fig. 14 Noise attack: (**a**) 2% intensity; (**b**) 5% intensity; (**c**) 10% intensity; (**d**) 15% intensity

and 1/2 degree clipping are shown respectively. In Fig. 14, the decryption results of encrypted images under 2%, 5%, 10%, and 15% degree salt & pepper noise are shown. It can be seen that most of the information can still be identified visually after the recovered image.

6 Conclusion

In this paper, a new spatiotemporal chaos model is proposed and applied to the field of image encryption. DCPML model uses perturbation function instead of chaotic coupling term, and adopts dynamic coupling coefficient. Through the analysis of multiple indexes, it is proved that DCPML model has stronger chaotic characteristics and higher information entropy, and reduces the mutual information value between lattices. Then a bit-level image encryption algorithm based on DCPML system is proposed. Due to the excellent chaotic performance of spatiotemporal chaotic model, the encryption algorithm has higher security. Through the analysis of encryption and decryption algorithms, it is proved that the algorithm can resist various common attacks, and has better security and lower computational complexity compared with other encryption algorithms. Although DCPML has improved its performance, the parameter range of its chaotic state is still affected by the parameters of Logistic map. In the future research, we will further study this problem and more efficient encryption 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).

Data availability My manuscript has no associated data.

Declarations

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

References

1. Adeli H, Ghosh-Dastidar S, Dadmehr N (2007) A wavelet-chaos methodology for analysis of EEGs and EEG subbands to detect seizure and epilepsy. IEEE Trans Biomed Engin 54(2):205–211
2. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos 16(8):2129–2151
3. Babiceanu RF, Seker R (2016) Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Comput Ind 81:128–137
4. 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
5. Dong WL, Li QL, Tang YW (2021) Image encryption-then-transmission combining random sub-block scrambling and loop DNA algorithm in an optical chaotic system. Chaos, Solitons Fractals 153:111539
6. Ghosh G, Verma S, Jhanjhi NZ, Talib MN (2020) Secure surveillance system using chaotic image encryption technique. IOP Conf Series: Mater Sci Engin 993(1):012062
7. Ghosh G, Anand D, Verma S, Jhanjhi NZ, Talib MN (2021) A Comparative Review on Non-chaotic and Chaotic Image Encryption Techniques. Intel Comput Innov Data Sci:465–471
8. Heidari-Bateni G, McGillem CD (1994) A chaotic direct-sequence spread-spectrum communication system. IEEE Trans Commun 42(234):1524–1527
9. Hosny KM, Kamal ST, Darwish MM (2022) A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map. Vis Comput. https://doi.org/10.1007/s00371-021-02382-1
10. Hu HP, Xu Y, Zhu ZQ (2008) A method of improving the properties of digital chaotic system. Chaos, Solitons Fractals 38(2):439–446
11. Hua ZY, Zhou YC (2016) Image encryption using 2D Logistic-adjusted-Sine map. Inf Sci 339:237–253
12. Kaneko K (1989) Pattern dynamics in spatiotemporal chaos: Pattern selection, diffusion of defect and pattern competition intermittency. Phys D 34(1–2):1–41
13. 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
14. Li Q, Wang XY, Wang XY, Ma B, Wang CP, Shi YQ (2021) An encrypted coverless information hiding method based on generative models. Inf Sci 553:19–30
15. Liao TL, Tsai SH (2000) Adaptive synchronization of chaotic systems and its application to secure communications. Chaos, Solitons Fractals 11(9):1387–1396
16. Liu LF, Miao SX (2015) A universal method for improving the dynamical degradation of a digital chaotic system. Phys Scr 90(8):085205
17. Liu XL, Tong XJ, Wang Z, Zhang M (2022) A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-12472-4
18. Lorenz EN (1963) Deterministic nonperiodic flow. J Atmos Sci 20(2):130–141
19. 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
20. Man ZL, Li JQ, Di XQ, Sheng YH, Liu ZF (2021) Double image encryption algorithm based on neural network and chaos. Chaos, Solitons Fractals 152:111318
21. Mansouri A, Wang XY (2021) A novel block-based image encryption scheme using a new Sine powered chaotic map generator. Multimed Tools Appl 80:21955–21978
22. Meherzi S, Marcos S, Belghith S (2006) A new spatiotemporal chaotic system with advantageous synchronization and unpredictability features. System:147–150
23. Riyahi M, Rafsanjani MK, Motevalli R (2021) A novel image encryption scheme based on multi-directional diffusion technique and integrated chaotic map. Neural Comput & Applic 33:14311–14326
24. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Techn J 28(4):656–715

25. 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 Circ Syst I: Reg Papers 61(8):2380–2389
26. Shevchenko II (2014) Lyapunov exponents in resonance multiplets. Phys Lett A 378(1–2):34–42
27. Tong XJ (2013) Design of an image encryption scheme based on a multiple chaotic map. Commun Nonlinear Sci Numer Simul 18(7):1725–1733
28. 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
29. Wang XY, Gao S (2020) Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Inf Sci 507:16–36
30. Wang XY, Zhao MC (2021) An image encryption algorithm based on hyperchaotic system and DNA coding. Opt Laser Technol 143:107316
31. Wang XY, Feng L, Wang SB, Zhang C, Zhang YQ (2018) Spatiotemporal chaos in coupled Logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access 6:39705–39724
32. Wang J, Liu WY, Zhang S (2020) Adaptive encryption of digital images based on lifting wavelet optimization. Multimed Tools Appl 79:9363–9386
33. Wang MX, Wang XY, Wang CP, Xia ZQ, Zhao HY, Gao S, Zhou S, Yao NM (2020) Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption. Chaos, Solit Frac 139:110028
34. Wang XY, Chen SN, Zhang YQ (2021) A chaotic image encryption algorithm based on random dynamic mixing. Opt Laser Technol 138:106837
35. Wang XY, Liu C, Jiang DH (2021) A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf Sci 574:505–527
36. Wang XY, Su YN, Liu L, Zhang H, Di SH (2021) Color image encryption algorithm based on Fisher-Yates scrambling and DNA subsequence operation. Vis Comput. https://doi.org/10.1007/s00371-021-02311-2
37. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidiscip, J Sci Technol, J Selec Areas Telecommun 1(2):31–38
38. Xian YJ, Wang XY (2021) Fractal sorting matrix and its application on chaotic image encryption. Inf Sci 547:1154–1169
39. Xian YJ, Wang XY, Teng L (2021) Double parameters fractal sorting matrix and its application in image encryption. IEEE Trans Circuits Syst Vid Technol. https://doi.org/10.1109/TCSVT.2021.3108767
40. 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
41. Xu LD, He W, Li SC (2014) Internet of things in industries: A survey. IEEE Trans Indust Inform 10(4):2233–2243
42. Ye XL, Wang XY, Gao S, Zhao HY, Mou J, Wang ZS, Yang FF (2020) A new chaotic circuit with multiply memristors and its application in image encryption. Nonlin Dynam 99(2):1489–1506
43. Yildirim M (2022) Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. Chaos, Solitons Fractals 155:111631
44. Zhang YQ, Wang XY (2013) Spatiotemporal chaos in Arnold coupled logistic map lattice. Nonlinear Analy-Model Control 18(4):526–541
45. Zhang YQ, Wang XY (2014) Spatiotemporal chaos in mixed linear-nonlinear coupled logistic map lattice. Physica A 402:104–118
46. Zhang YQ, He Y, Li P, Wang XY (2020) A new color image encryption scheme based on 2DNLCML system and genetic operations. Opt Lasers Eng 128:106040