Research Article

A Novel Compressive Image Encryption with an Improved 2D Coupled Map Lattice Model

Zhuo Liu, Yong Wang, Leo Yu Zhang, and Jun Ma

1College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2School of Mathematics and Big Data, Guizhou Education University, Guiyang 550018, China
3School of Information Technology, Deakin University, Victoria 3216, Australia
4Department of Physics, Lanzhou University of Technology, Lanzhou 730050, China

Correspondence should be addressed to Yong Wang; wangyong_cqupt@163.com

Received 28 December 2020; Revised 4 February 2021; Accepted 17 March 2021; Published 10 April 2021

Academic Editor: David Megias

The digital image, as the critical component of information transmission and storage, has been widely used in the fields of big data, cloud and frog computing, Internet of things, and so on. Due to large amounts of private information in the digital image, the image protection is fairly essential, and the designing of the encryption image scheme has become a hot issue in recent years. In this paper, to resolve the shortcoming that the probability density distribution (PDD) of the chaotic sequences generated in the original two-dimensional coupled map lattice (2D CML) model is uneven, we firstly proposed an improved 2D CML model according to adding the offsets for each node after every iteration of the original model, which possesses much better chaotic performance than the original one, and also its chaotic sequences become uniform. Based on the improved 2D CML model, we designed a compressive image encryption scheme. Under the condition of different keys, the uniform chaotic sequences generated by the improved 2D CML model are utilized for compressing, confusing, and diffusing, respectively. Meanwhile, the message authentication code (MAC) is employed for guaranteeing that the encryption image be integration. Finally, theoretical analysis and simulation tests both demonstrate that the proposed image encryption scheme owns outstanding statistical, well encryption performance, and high security. It has great potential for ensuring the digital image security in application.

1. Introduction

In the recent years, the digital image, as an important carrier tool of information transmission and storage, has been popularly used in the fields of big data, cloud and frog computing, Internet of things, and so on [1–5]. The digital image contains personal privacy, commercial, and important military information. Thus, the leaking of this important information leads to some serious consequences [6, 7]. In order to combat illegal access, revision, and other attacks of the digital image, it is considerably essential to design high level of encryption schemes. Moreover, due to the enormous amount of the digital image, compression in the digital image should be also taken into account to improve the efficiency of transmission and storage [8, 9].

There are two views on how to design the encryption image scheme; the first one is to consider the traditional encryption method for the digital image encryption [10], such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Those traditional schemes can guarantee the digital image safety. However, those schemes are not highly efficient and do not consider the inherent characteristics of the digital image, which causes high pixel correlation and redundancy. That probably brings about some potential vulnerability to the safety image. In addition, the traditional image encryption scheme cannot be applied to compress the digital image. On the other hand, to solve the abovementioned security risks, considering the unique characteristics of randomness and initial sensitivity of the chaos, combining some special features of the digital image, it is quite clear that the chaotic sequences generated by the chaotic system are pretty suitable for compression and encryption [11, 12].

The chaotic system, firstly proposed in 1982, has been widely studied by many researchers [13, 14]. In particular,
the higher-dimensional chaotic system, which possesses a much larger Lyapunov exponent (LE) and more complex dynamic performance, is popularly utilized in the digital image encryption recently. The CML model, as one of the classic spatiotemporal models, has been used as key competent to construct the digital image compression and encryption scheme. Compared with the one-dimensional CML (1D CML), the 2D CML model has much more complex chaotic dynamic characteristics, which is promising to the digital image encryption. Based on the 2D Nonadjacent CML model, the digital image encryption scheme was proposed [15], and theoretical analysis and numerical simulation demonstrate that the digital image encryption scheme is effective. He et al. proposed a new image encryption scheme according to the 2D CML model and bit-level permutation [16], which owns more secure and effective performance. A novel image encryption scheme based on the nearest-neighboring CML was proposed [17], and it has higher security level, higher sensitivity, and higher speed. Although the 2D CML model was considered for encryption in the aforementioned schemes [15–17], the application of the 2D CML model in compression is still in the infancy; because of the difficulty in verifying the Restricted Isometry Property (RIP), the existing compressive image schemes mainly focus on the low-complexity chaotic system [18, 19]. The logistic system is utilized to produce the measurement matrix for compression in [18]. A novel encrypted compressive sensing of images based on fractional-order hyperchaotic Chen system and DNA operations is proposed in this paper [19]. The low-complexity chaotic system indicates the low-security image encryption scheme and small key space. To improve the encryption scheme’s security and enlarge the key space, the high-dimensional system such as the 2D CML model should be applied in the CS. Moreover, the key issue is how to verify the independence of the chaotic sequences generated by the 2D CML model. However, few scholars have discussed this problem. Meanwhile, the PDD of the core model in those schemes [15–19] is uneven, and the uneven sequences indicate that they are easier to be attacked, which brings about the security risks to the designing of the digital image encryption scheme.

To remedy the above-mentioned problems, we proposed an improved 2D CML model; compared with the original 2D CML model, it has more uniform PDD. Meanwhile, the chaotic sequences generated by the improved model are independent according to the independent testing. Based on the improved 2D CML model, a novel compressive image encryption scheme is designed. In our scheme, the independent sequences are firstly used for compressing, confusing, and diffusing, respectively.

(i) According to adding different offsets for each node, an improved 2D CML model is presented. The simulation analysis shows that the PDD of the chaotic sequences generated by the improved 2D CML mode is uniform. Meanwhile, the LE expression of the improved model is derived mathematically, which can guide the setting of the parameters to ensure the complex chaotic performance.

(ii) Based on the improved 2D CML model, the proposed image encryption scheme is designed. With different keys, the chaotic sequences generated by the improved model are used for compressing, confusing, and diffusing, respectively.

(iii) In the proposed image encryption scheme, we use the MAC algorithm to ensure the digital image integrity. Finally, theory analysis and simulation tests both prove that the proposed scheme possesses outstanding encryption performance.

The remaining part of this paper is organized as follows. Preliminaries are presented in Section 2, and an improved 2D CML model is proposed in Section 3. In Section 4, the proposed image encryption scheme based on the improved model and MAC algorithm is designed. In Section 5, the performances of the proposed encryption scheme are analysed. Finally, we draw the conclusion in Section 6.

2. Preliminaries

2.1. 2D CML Model. The CML model is firstly proposed by Kaneko in [20], which is a common spatiotemporal chaos model. To enhance the complexity of the CML model, it is extended into the 2D CML one, which is depicted as follows.

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

where \( f(.) \) denotes the local chaotic map and \( i = 1, 2, \ldots, R \) and \( j = 1, 2, \ldots, L \) are the row and column indexes of the nodes, respectively. The periodic boundary conditions are \( x_n^{i+R,j} = x_n^{i,j} \) and \( x_n^{i,j+L} = x_n^{i,j} \).

According to equation (1), we need to iterate \( f \) for five times to calculate the value of \( x_{n+1}^{i,j} \). For improving the computation efficiency of the model, the 2D CML model is simplified as

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

2.2. The Piecewise Logistic Map. Owing to much larger LE and more complex chaotic characteristics, the piecewise logistic map (PLM) was proposed [21], which is defined by
where \( N \) is the segment number of the PLM function, \( \mu \in (0, 4] \) is the control parameter, \( x_m \) is the state value, and \( x_m \in (0, 1) \). Moreover, when \( N = 64 \) and \( \mu = 4 \) in equation (3), the LE value of PLM is 4.574594, which is the maximum LE value, and the PLM function owns the most complex chaotic performance.

2.3. Compressive Sensing. Compressive sensing (CS), as depicted in Figure 1, was proposed by Candes and Donoho in 2006 [22], which is shown by

\[
y = \Phi x, \tag{4}
\]

where \( x \) is the original signal of dimensions \( N \times 1 \), \( \Phi \) is the measurement matrix with dimensions \( M \times N \), \( y \) is the compressed measurement matrix with dimensions \( M \times 1 \), and \( M \ll N \). In equation (4), the original signal \( x \) is mostly not sparse, which is represented as

\[
x = \Psi s. \tag{5}
\]

where \( \Psi \) is the orthogonal basis matrix and \( s \) is the coefficient vector.

According to equations (4) and (5), the CS processing is as follows:

\[
y = \Phi x = \Phi \Psi s = \Theta s, \tag{6}
\]

where \( \Theta \) is the sensing matrix of dimensions \( M \times N \) and \( \Theta \) must satisfy the RIP defined in Definition 2. Due to the reconstruction of the signal, \( x \) can be recovered by calculating \( \Psi s \).

**Definition 2.** Suppose that there exists a constant \( \delta_{xK} \) such that

\[
(1 - \delta_{xK}) x^3_i \leq \Theta \theta^3_i \leq (1 + \delta_{xK}) x^3_i,
\]

holds for all \( x \in \sum K = \{ x : x_0 \leq K \} \).

3. The Improved 2D CML Model

3.1. The Model. In the original 2D CML model, set \( \mu = 4 \) and \( N = 64 \) in the local mapping PLM and \( R = L = 4 \) and \( \varepsilon = 0.1 \) in model; we plot the PPD of sequences generated by the nodes in Figure 2. Clearly, the PPD of sequences is uneven, and the peak areas are covered in the intervals \([0, 0.2]\) and \([0.8, 1.0]\).

From the perspective of cryptography, the uneven PPD of chaotic sequences causes some security breaches for the attackers. To overcome the shortcoming, we add a different offset for each node after each iteration and propose an improved 2D CML model, which is described as

\[
\begin{align*}
\frac{x_{n+1}^{ij}}{x_{n}^{ij}} &= \left(1 - \varepsilon\right) f\left(x_{n}^{ij}ight) + \varepsilon \left[\left(x_{n}^{(i+1)j}ight) + f\left(x_{n}^{ij+1}ight)\right], \\
\frac{x_{n+1}^{ij}}{x_{n}^{ij}} &= \frac{\left(x_{n+1}^{ij} + \left(i - 1\right) \times L + j\right)}{R \times L} \mod 1,
\end{align*}
\]

and, in the proposed 2D CML model, \( y_{n+1}^{ij} \) is the iteration state value of the \( i \)th and \( j \)th nodes at time \( n + 1 \). For each \( y_{n+1}^{ij} \), we add the offset value \( \left(\left(i - 1\right) \times L + j\right) / \left(R \times L\right) \). \( x_{n+1}^{ij} \) is obtained and used for the state value in the next iteration.

According to the above-mentioned 2D CML model, using the same parameter as in the original 2D CML model, the PPD of the sequences generated by the improved model is shown in Figure 3. According to Figure 3, the PPD becomes uniform.

3.2. The Characteristics of the Proposed Model

3.2.1. Lyapunov Exponent. LE is usually used to judge whether a system is chaotic, and a positive LE indicates the system is in chaos. Otherwise, it is not chaotic. Meanwhile, according to the LE formula of the chaotic system, we can set the parameters to make the chaotic system remain in the fully chaotic state. Using the method in [23], the LE formula of the improved 2D CML model is derived as follows.

Firstly, the improved 2D CML model is converted to a one-dimensional CML. Therefore, equation (2) is converted to

\[
x^{(i-1)\times L+j}_{n+1} = \left(1 - \varepsilon\right) f\left(x^{(i-1)\times L+j}_{n}\right) + \varepsilon \left[\left(x^{(i+1)\times L+j}_{n}\right) + f\left(x^{(i+1)\times L+j}_{n}\right)\right],
\]

Figure 1: The procedure of compressive sensing.
In equation (9), the periodic boundary is $x_{n+1} = x_n$, and $x_{n-j} = x_{j+n}$.

We can get the derivatives of $f$ as follows:

$$f'(x_{n+1}) = f'(x_n) = f'(x_{n-j}) = f'(x_{j+n}),$$

(10)

Then, the differential of equation (9) is

$$\delta x_{n+1} = (1 - \varepsilon)\delta x_n + \frac{\varepsilon}{2}\left[ f'(x_n)\delta x_n + f'(x_{n-j})\delta x_{n-j} \right].$$

(11)

Based on equations (10) and (11), we have

$$\delta x_{n+1} = f'(x_n)((1 - \varepsilon)\delta x_n + \frac{\varepsilon}{2}\delta x_{n-j} + \delta x_{n-j+1}).$$

(12)

From equation (13), we can get

$$\delta x_{n+1} = J_n\delta x_n,$$

(13)

where $J_n$ is the Jacobian matrix and $J_n = f'(x_n)G$.

$$G = \begin{pmatrix} A_1 & A_2 & A_3 & \cdots & A_R \\ A_R & A_1 & A_2 & \cdots & A_{R-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ A_2 & A_3 & A_4 & \cdots & A_1 \end{pmatrix}.$$ 

(14)

Moreover, set $K = J_1 \times J_2 \times \cdots \times J_n = G^n \prod_{i=1}^{n} f'(x_n)$, and the eigenvalue of $G$ is $\lambda$ and the eigenvalue of $K$ is $\lambda^n \prod_{i=1}^{n} f'(x_i)$. It is easy to verify the formula of LEs:

$$\text{LEs} = \lim_{n \to \infty} \frac{1}{n} \ln \prod_{i=1}^{n} f'(x_i) + \ln|\lambda|.$$ 

(15)

$G$ is a block circulant matrix; its eigenvalue values are $\lambda = 1 - \varepsilon + (\varepsilon/2)\omega_k + (\varepsilon/2)\phi_1$. Substituting $\lambda$ into equation (15), we have

$$\text{LEs} = \lambda f(\varepsilon) + \frac{3}{2} \varepsilon^2 - 2\varepsilon + \varepsilon(1 - \varepsilon) \left( \frac{\cos \frac{2\pi R}{L} + \cos \frac{2\pi l}{L}}{2} \right) + \frac{\varepsilon^2}{2} \cos \left( \frac{2\pi R}{L} - \frac{2\pi l}{L} \right).$$ 

(16)

According to equation (16), we can get the following significant theoretical results. The MLE is solely decided by the local chaotic map $f$. Consequently, in the proposed 2D CML model, when choosing PLM with $N = 64$ and $\mu = 4$, the LE of the proposed 2D CML model is maximum, and it has the most complex chaotic performance.
3.2.3. Ergodicity. In statistics, ergodicity describes the randomness of statistical results at time and space. In a chaotic system, the iteration values of a system cover the entire interval, and it indicates that the chaotic system is more complex. Here, fix $R = L = 4$, $\varepsilon = 0.1$, and $N = 64$, and change the value of $\mu$ with $\mu = 0.1, 0.5, 1, 2, 3, 4$; we plot the ergodicity of the original 2D CML model and the improved 2D CML model caused by $x_n$ in Figures 6 and 7, respectively. It is clear that the improved model has much better chaotic performance than in the original model, and this is because, in the improved 2D CML model, the values of $x_n$ are covered fully the interval $[0, 1]$ when $\mu = 0.5$ and when $\mu = 2$ in the original one.

4. Construction of the Chaotic-Based Measurement Matrix

4.1. The Independence Testing of Chaotic Sequences. The chaotic sequences utilized for constructing the measurement matrix must satisfy the RIP, and the chaotic sequences are requested to be independently identically distributed. To authenticate that the chaotic sequences generated by the improved 2D CML model are independent, only the independent sequences can be used as the chaotic-based measurement matrix for compressing the digital image. Moreover, the PPD expression of the model cannot be derived at present; it indicates that we only apply
the well-known simulation method to verify the independent; according to the test for independence, we make use of that method to judge whether the chaotic sequences are independent. The step-by-step details of the independence testing method are summarized as follows.

**Step 1.** Let $X$ and $Y$ be two sequences; the variances of $X$ and $Y$ are $D_X$ and $D_Y$, respectively. The covariance of $X$ and $Y$ is $D_{XY}$, and the relation among them is as follows:

$$P_{XY} = \frac{D_{XY}}{\sqrt{D_X \cdot D_Y}}.$$  

**Step 2.** Supposing that $X$ and $Y$ are independent, we use equation (18) to calculate the values of $T$. When $T$ satisfies equation (19), the hypothesis testing is reasonable. Otherwise, it is unreasonable.

$$T = \left( Z_{\alpha/2} + \rho - 2 \right)^{1/2} \times P_{XY},$$

$$-Z_{\alpha/2} < T < Z_{\alpha/2},$$

where $\alpha = 0.05$, $Z_{\alpha/2} = 1.96$, and $\rho$ is the length of the sequence.

**Step 3.** Based on the primary steps, in the improved 2D CML model, select $R = L = 4$, $\varepsilon = 0.1$ and $N = 64, \mu = 4$, the interval of time series $d$ is 40, set different initial values for the two improved 2D CML
models, and iterate those two models for 2,000 times to eliminate the influence of initial value.

Step 4. Perform the two improved 2D CML models, choose the chaotic sequences generated by the node of the 4th row and the 4th column for each iteration, and combine the chaotic sequences with the length 1,000.

Step 5. Repeat the above testing for 100 times and plot the testing results in Figure 8. According to Figure 8, it is clear that the chaotic sequences generated by the above steps are independent.

4.2. The Chaotic-Based Measurement Matrix. The CS plays an important part in the proposed image encryption scheme. According to equation (6), it is essential to design enough complex chaotic-based matrix \( \Phi \). The chaotic sequences have complex chaotic performance and also those sequences are independent by the independence testing. We unitize those chaotic sequences to design the chaotic-based measurement matrix \( \Phi \); the detailed processing is described in Algorithm 1.

5. The Proposed Image Encryption Scheme

Based on the proposed 2D CML model, unitizing the most complexity of the improved model and the high efficiency of the CS to enhance the security and efficiency of the encryption scheme, we design a novel safe image encryption scheme in this section. The key components of the scheme are depicted in Figure 9, and the main flow flat contains the processing of DCT, CS, diffusion, and confusion.

5.1. The Proposed Image Encryption Algorithm. In the proposed image encryption scheme, the processing of the scheme is described in Figure 10, and the detailed steps are elaborated in the following steps.

Step 1. Choose the plain image \( P \) with size \( M \times N \), and separate \( P \) into \( B_1, G_1, \) and \( R_1 \). Then, produce the discrete cosine transform (DCT) basis \( D \) and sparse \( B_1, G_1, \) and \( R_1 \) with equation (20); we have \( B'_1, G'_1, \) and \( R'_1 \) with size \( M \times N \).

\[
\begin{align*}
B'_1 &= DB_1D^T, \\
G'_1 &= DG_1D^T, \\
R'_1 &= DR_1D^T.
\end{align*}
\] (20)

Step 2. Utilize Algorithm 1 to generate the chaotic measurement matrix \( \Phi_1, \Phi_2, \Phi_3 \), respectively. According to equation (21), use the chaotic measurement matrix \( \Phi_1, \Phi_2, \Phi_3 \) to compress \( B'_1, G'_1, \) and \( R'_1 \) and obtain the compressive matrix \( C_1, C_2, C_3 \).

\[
\begin{align*}
C_1 &= \Phi_1B'_1, \\
C_2 &= \Phi_2G'_1, \\
C_3 &= \Phi_3R'_1.
\end{align*}
\] (21)

Step 3. For the compressive matrix \( C_1, C_2, C_3 \), we do the normalization to transform the values of \( C_1, C_2, C_3 \) into the interval \([0, 255]\) by equation (22), respectively. We have the new compressive matrix \( C'_1, C'_2, C'_3 \).

\[
\begin{align*}
C'_1 &= \text{round} \left( \frac{255 \ast (C_1^{\text{max}} - C_1^{\text{min}})}{C_1^{\text{max}} - C_1^{\text{min}}} \right), \\
C'_2 &= \text{round} \left( \frac{255 \ast (C_2^{\text{max}} - C_2^{\text{min}})}{C_2^{\text{max}} - C_2^{\text{min}}} \right), \\
C'_3 &= \text{round} \left( \frac{255 \ast (C_3^{\text{max}} - C_3^{\text{min}})}{C_3^{\text{max}} - C_3^{\text{min}}} \right),
\end{align*}
\] (22)

where \( \text{round} \) is the rounding function and \( C_1^{\text{min}}, C_1^{\text{max}}, C_2^{\text{min}}, C_2^{\text{max}}, C_3^{\text{min}}, \) and \( C_3^{\text{max}} \) are the maximum and minimum of \( C_1, C_2, C_3 \), respectively. \( C'_1 \in C_1, C'_2 \in C_2, \) and \( C'_3 \in C_3 \).

Step 4. Utilize the plain image and generate the MAC value \( C \) by the following equation:

\[
C = \text{Binary} \left( \text{Hash} \left( P_{\text{value}2} \right) \right),
\] (23)

where \( P_{\text{value}2} = \text{average} \left( \text{sum} \left( B_1 \right) + \text{sum} \left( G_1 \right) + \text{sum} \left( R_1 \right) \right) \\
+ \text{average} \left( \text{max} \left( B_1 \right) + \text{max} \left( G_1 \right) + \text{max} \left( R_1 \right) \right) \\
+ \text{average} \left( \text{min} \left( B_1 \right) + \text{min} \left( G_1 \right) + \text{min} \left( R_1 \right) \right),
\] (24)

where \( h(\cdot) \), \( \text{Decimal}(\cdot) \), and \( \text{average}(\cdot) \) are the Hash encryption function, the function of transforming Hexadecimal to Decimal, and the average function, respectively. \( \text{sum}(\cdot) \) is the sum function, \( \text{max}(\cdot) \) is the maximum function, and \( \text{min}(\cdot) \) is the minimum function. \( C \) is partitioned into 8-bit subblocks. Then, each block with binary format is transformed into the
Input: Two sets of initial conditions in the improved 2D CML model
Output: the measurement matrix Φ
Function Main:
Step 1: select PLM as the local map with μ = 4, N = 64, set ε = 0.1 and R = L = 4 in the proposed 2D CML model.
Step 2: under the parameters of step 1, set different initial values for the two improved 2D CML models, iterate the two models for 2000 times to eliminate the influence of initial value.
Step 3: then, run the two improved 2D CML models, choose the chaotic sequences generated by the node of the 4th row and the 4th column for each iteration, and combine the chaotic sequences Z with the length M × N.
Step 4: for each zv ∈ Z, v = 1, 2, . . . , M × N, according to Algorithm 1, transform the chaotic sequences Z and form the new chaotic sequences Wv, wv = 1 − 2zv.
Step 5: finally, arrange the chaotic sequences W by column and construct the measurement matrix ΦM×N as

\[ Φ_{M×N} = \left( \sqrt{2/M} \right) \begin{pmatrix} w_0 & w_M & \cdots & w_{MN-M} \\ w_1 & w_{M+1} & \cdots & w_{MN-M+1} \\ \vdots & \vdots & \vdots & \vdots \\ w_{M-1} & w_{2M-1} & \cdots & w_{MN-1} \end{pmatrix}, \]

where \( \sqrt{2/M} \) is used for normalization.

**Algorithm 1:** The measurement matrix.

---

**Figure 9:** The key components of the proposed image encryption scheme.

**Figure 10:** The proposed image encryption scheme.
integer with decimal format, and the number of all the integers is 32. Then, we do the following:

(i) Apply the 2DWT to \( C_1', C_2', \) and \( C_3'. \) We obtain \( C_{11}', C_{12}', C_{13}', C_{21}', C_{22}', C_{23}', C_{31}', C_{32}', C_{33}', C_1', C_2', C_3'. \)

(ii) Substitute the corresponding Hash values into \( C_1', \) with the first 32 values.

(iii) According to the IDWT, we obtain new \( C_1', C_2', \) and \( C_3'. \)

Step 5. The step includes the two following parts:

(i) Utilize the plain image and the parameter \( \varepsilon_1 \) is generated by the following equation:

\[
\begin{align*}
\epsilon_1 &= \frac{P_{value1}}{256}.
\end{align*}
\]

(ii) In the proposed 2D CML model, set \( \mu = 4, N = 64, \varepsilon = 0.1, \) and \( \varepsilon = \varepsilon_1 + \varepsilon_2 \) and \( R = L = 4, \) and iterate the two models for 2,000 times to eliminate the influence of initial values. Then, generate the chaotic sequences \( H. \) According to equation (26), the sequences \( H \) to diffuse the compressive matrix \( C_1', C_2', C_3' \) and get the diffusion matrix \( C_1'', C_2'', C_3''. \)

\[
\begin{align*}
C_{1''}(t) &= C_1'(t) \oplus H(t) \oplus C_1'(t-1), \\
C_{2''}(t) &= C_2'(t) \oplus H(t) \oplus C_2'(t-1), \\
C_{3''}(t) &= C_3'(t) \oplus H(t) \oplus C_3'(t-1),
\end{align*}
\]

where \( t \in \{1, 2, \ldots, M \times N\}. \)

Step 6. Utilize the sequences \( H \) to change the pixel values of \( C_1'', C_2'', C_3'' \) according to the following operations:

(i) For some points \( C''_{1}(P, Q), C''_{2}(P, Q), \) and \( C''_{3}(P, Q) \) in the \( P \)th row and the \( Q \)th column, compute \( Z = P \times N + Q. \)

(ii) Denote the \( Z^{th} \) element of \( U \) as \( u_Z \) and change the value \( C''_{1}(P, Q) \) as follows:

\[
\begin{align*}
C''_{1}(P, Q) &= C''_{1}(P, Q) \oplus [u_Z \times N \times M \times 10^4], \\
C''_{2}(P, Q) &= C''_{2}(P, Q) \oplus [u_Z \times N \times M \times 10^4], \\
C''_{3}(P, Q) &= C''_{3}(P, Q) \oplus [u_Z \times N \times M \times 10^4].
\end{align*}
\]

(iii) Repeat 1-2 by setting \( P = 0, 1, 2, \ldots, M - 1 \) and \( Q = 0, 1, 2, \ldots, N - 1. \) Finally, output the confused components \( C_1', C_2', \) and \( C_3'. \)

Step 7. For each \( C_1''', C_2''', \) and \( C_3''' \), we do the following operation: get \( B_2(t), G_3(t), \) and \( R_2(t), \) and combine them into the encryption image \( C. \)

5.2 Recovering the Plain Image. According to the proposed image encryption scheme in Section 5.1, we can obtain the encryption image \( C. \) The recovering encryption image is the reverse processing of the proposed scheme, and the specific details are as follows: For the encryption image \( C, \) we use equation (29) to get \( C_1'''(t), C_2'''(t), C_3'''(t). \) Then, utilize the sequences \( H \) to change the pixel values of \( C_1'''(t), C_2'''(t), C_3'''(t) \) and diffuse the sequences \( C_1', C_2', C_3' \) according to equations (30) and (31), respectively. Finally, we can get the plain image \( P \) by equations (32) and (33).

\[
\begin{align*}
B_2(t) &= C_1'''(t) \times (C_2''_{max} - C_2''_{min}) + C_2''_{min}, & \text{where} & \quad P = M - 1, M - 2, M - 3, \ldots, 0 \quad \text{and} \quad Q = N - 1, N - 2, N - 3, \ldots, 0 \quad \text{are chosen.}
\end{align*}
\]
6. Experimental Analysis

To verify that the proposed image encryption scheme in Section 5 is effective, we perform the following experiments and analyse the corresponding statistical results of the plain image and encrypted image; all the experimental results and analyses are to demonstrate that the proposed image encryption scheme is suitable for compressing and encrypting the plain image.

6.1. The Encryption Image. Choose the plain images of Lena (512 × 512), Peppers (512 × 512), Women (256 × 256), and Tree (256 × 256); based on the improved 2D CML model in Section 3 and the proposed image encryption scheme in Section 5, set \( R = L = 4, \varepsilon = 0.1, N = 64, \mu = 4 \) in the improved 2D CML model and the compressive rate is 0.5; we show the encryption image and the recovering image in Figure 11. According to Figure 11, the encryption images are chaos, irregular and hiding the information of the plain image well. Meanwhile, the recovering images are almost the same as the plain images. All abovementioned results prove that the encryption image scheme is practicable and feasible.

6.2. The Statistical Results. The histogram of the plain image reflects the statistics distributed state of the image grayscale value; the more the even statistics are distributed, the less information is exposed. The histograms of the plain image and the encryption image are listed in Figures 12–15. For example, Figures 12(a)–12(c) present the histogram of the plain image of Lena in Red, Green, and Blue, respectively. It can be seen from the histogram that the results of Lena are quite not uniform; the image grayscale values concentrate in the certain interval. Meanwhile, Figures 12(d)–12(f) show the distributed state of the encryption image of Lena in Red, Green, and Blue, respectively. It is clear that the histogram results of the encryption image of Lena are pretty uniform, which means that the encryption scheme can realize hiding the grayscale value information of the plain image. Similarly, Figures 12–15 demonstrate that the encryption image scheme possesses outstanding encryption performance.

In addition, the correlation coefficients of horizontal (H), vertical (V), and diagonal (D) adjacent in the plain image and encryption image are utilized to measure the correlation among those grayscale values. Choose 2,000 pairs of H, V, and D adjacent grayscale, respectively, and plot them in Figures 16–19. According to Figure 16, the results of Lena are shown in Figures 16(a)–16(c), and it can be seen that the grayscale values are concentrated. However, the results of the encryption of Lena are uniform. Moreover, according to equations (34) and (35), we calculate the correlation coefficients of level, vertical, and diagonal adjacent and list them in Table 1. It is clear that the correlation coefficients are all quite close to 0 from Table 1. Thus, there is no relation among the pixel in the encryption image, which suggests that the proposed encryption image scheme holds well encryption characteristic.

\[
\text{cov}(x, y) = E[(x - E(x))(y - E(y))],
\]

\[
r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},
\]

where \( x \) and \( y \) are the adjacent grayscale values, respectively. \( E(x) = (\sum_{i=1}^{P} x_i / P) \), \( D(x) = (\sum_{i=1}^{P} (x_i - E(x))^2 / P) \), and \( P \) is the number of the grayscale pixel pairs.

6.3. Information Entropy Analysis. The information entropy describes the average information in the image; its ideal value can be calculated by equation (36) and the value is 8.0.

\[
H = \sum_{i=0}^{n} p(X_i)\log_{2}(p(X_i)),
\]

where \( X_i \) is the grayscale value of the plain image and \( p(X_i) \) is the rate of the grayscale value \( X_i \).

According to equation (36), we list the information entropy values in Table 2.

6.4. Differential Attack Analysis. Considering the differential attack, the attacker usually adjusts to the plaintext and compares differences with the ciphertexts generated before and after the adjustment to attack. For the differential attacks on the image encryption, the two indicators, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI), are evaluated according to equations (37) and (38), and the corresponding calculation formulas are as follows:

\[
\text{NPCR}(P_1, P_2) = \frac{1}{M \times N} \times \sum_{a=1}^{M} \sum_{b=1}^{N} \text{Sign}(D(a, b)) \times 100\%,
\]

\[
\text{UACI}(P_1, P_2) = \frac{1}{M \times N} \times \left( \sum_{a=1}^{M} \sum_{b=1}^{N} \frac{D(a, b)}{255} \right) \times 100\%,
\]

where \( P_1 \) and \( P_2 \) are two encryption images; then, \( D(i, j) = |P_1(a, b) - P_2(a, b)| \). Sign \( (D(a, b)) \) is as follows:

\[
\text{Sign}(D(a, b)) = \begin{cases} 
1, & P_1(i, j) = P_2(i, j), \\
0, & P_1(i, j) \neq P_2(i, j).
\end{cases}
\]

The results of NPCR and UACI are calculated in Table 3; the ideal values are 0.996094 and 0.334635, respectively. According to Table 3, it can be seen that all the test results are quite close to the ideal values. Therefore, the proposed encryption images scheme has good ability to resist the differential attacks effectively.

6.5. Key Security Analysis

6.5.1. Key Space Analysis. For the image encryption scheme, a larger size of key indicates the larger key space. From the perspective of security, it is infeasible to make brute force when the key space is enough large. The general requirement
Figure 11: The plain image, the encryption image, and the recovering image. (a) The plain image. (b) The encryption image. (c) The recovering image.

Figure 12: The histogram results of Lena and the encryption of Lena. (a) Histogram of Lena in R; (b) histogram of Lena in G; (c) histogram of Lena in B; (d) histogram of the encryption of Lena in R; (e) histogram of the encryption of Lena in G; (f) histogram of the encryption of Lena in B.
value of resisting the attack is $2^{128}$. In the proposed image encryption scheme, the initial values of all 16 nodes are used as the key for two times. According to the IEEE 754 floating-point standard, the precision of the floating number for each node is $10^{15}$, and there are totally $10^{15 \times 32} = 10^{480}$, which is much larger than $2^{128}$. Thus, it is clear that the image encryption scheme can greatly satisfy the need of resisting the brute-force attacks.
Figure 15: The histogram results of Tree and the encryption of Tree. (a) Histogram of Tree in R; (b) histogram of Tree in G; (c) histogram of Tree in B; (d) histogram of the encryption of Tree in R; (e) histogram of the encryption of Tree in G; (f) histogram of the encryption of Tree in B.

Figure 16: Continued.
6.5.2. Key Sensitivity Analysis. The key sensitivity denotes that great changes are caused due to a tiny change of the key. According to the following cases, we do the tests of key sensitivity in the proposed image encryption scheme.

Case 1: keep the original parameter unchanged
Case 2: the parameter \( \varepsilon \) is changed from 0.1 to \( 0.1 + 10^{15} \)

Considering the above cases, under the condition of the different parameters as the key, we use the proposed image encryption scheme to compare the differences of the ciphertext, and the differences of the ciphertext are shown in Table 4. According to Table 4, a tiny change of the key would lead to the huge change of the ciphertext. The differences are all larger than 99.5%, which indicates that the image encryption scheme has well key sensitivity.

6.6. Comparison Analysis. In this section, to further verify that the proposed image encryption scheme has good

![Figure 16: The adjacent results of Lena and the encryption of Lena. (a) Adjacent (H, V, D) results of Lena in R; (b) adjacent (H, V, D) results of Lena in G; (c) adjacent (H, V, D) results of Lena in B; (d) adjacent (H, V, D) results of the encryption of Lena in R; (e) adjacent (H, V, D) results of the encryption of Lena in G; (f) adjacent (H, V, D) results of the encryption of Lena in B.](image-url)
Figure 17: Continued.
Figure 17: The adjacent results of Peppers and the encryption of Peppers. (a) Adjacent (H, V, D) results of Peppers in R; (b) adjacent (H, V, D) results of Peppers in G; (c) adjacent (H, V, D) results of Peppers in B; (d) adjacent (H, V, D) results of the encryption of Peppers in R; (e) adjacent (H, V, D) results of the encryption of Peppers in G; (f) adjacent (H, V, D) results of the encryption of Peppers in B.

Figure 18: Continued.
Figure 18: The adjacent results of Women and the encryption of Women. (a) Adjacent (H, V, D) results of Women in R; (b) adjacent (H, V, D) results of Women in G; (c) adjacent (H, V, D) results of Women in B; (d) adjacent (H, V, D) results of the encryption of Women in R; (e) adjacent (H, V, D) results of the encryption of Women in G; (f) adjacent (H, V, D) results of the encryption of Women in B.

Figure 19: Continued.
encryption characteristic, we compare those schemes with the proposed scheme, and, according to the existing image encryption schemes in [24–30], we present the comparison results for correlation coefficient, NPCR, UACI, and information entropy in Tables 5–7. According to the correlation coefficients results of the proposed scheme and other

Table 1: The correlation coefficient results of the plain image and encrypted image.

<table>
<thead>
<tr>
<th>Image</th>
<th>Lena</th>
<th>Pepper</th>
<th>Women</th>
<th>Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
<td>B</td>
<td>R</td>
</tr>
<tr>
<td>H</td>
<td>0.8871</td>
<td>0.9420</td>
<td>0.9557</td>
<td>0.9560</td>
</tr>
<tr>
<td>V</td>
<td>0.9316</td>
<td>0.9724</td>
<td>0.9840</td>
<td>0.9422</td>
</tr>
<tr>
<td>D</td>
<td>0.8567</td>
<td>0.9317</td>
<td>0.9680</td>
<td>0.9304</td>
</tr>
<tr>
<td>H</td>
<td>0.0016</td>
<td>0.0011</td>
<td>0.0005</td>
<td>0.0019</td>
</tr>
<tr>
<td>V</td>
<td>0.0002</td>
<td>0.0008</td>
<td>0.0005</td>
<td>0.0096</td>
</tr>
<tr>
<td>D</td>
<td>0.0038</td>
<td>0.0038</td>
<td>0.0004</td>
<td>0.0064</td>
</tr>
</tbody>
</table>

Figure 19: The adjacent results of Tree and the encryption of Tree. (a) Adjacent (H, V, D) results of Tree in R; (b) adjacent (H, V, D) results of Tree in G; (c) adjacent (H, V, D) results of Tree in B; (d) adjacent (H, V, D) results of the encryption of Tree in R; (e) adjacent (H, V, D) results of the encryption of Tree in G; (f) adjacent (H, V, D) results of the encryption of Tree in B.
schemes from Table 5, it can be seen that the correlation coefficients results in the proposed scheme are almost 0, which are smaller than the schemes in [25–29]. In Table 6, The NPCR and UACI results of the proposed scheme and other schemes are shown, and the values in the proposed scheme are closer to the ideal values (NPCR = 0.996094, UACI = 0.334635) than the schemes in [25, 27, 29, 30]. Meanwhile, the information entropy results of the proposed scheme and other schemes are listed in Table 7, and the information entropy values of R, G, and B in our scheme are
7.9986, 7.9985, and 7.9985, respectively. Above all, the comparison analysis fully proves that the proposed scheme has outstanding chaotic characteristic.

### 7. Conclusion

In our paper, based on the 2D CML model, to overcome the problem of the uneven PDD in the sequences generated in the original 2D CML model, we add the offset for the model after each iteration. The improved 2D CML model has much better chaotic performance than the original 2D CML model. According to the proposed 2D CML model, we proposed a new compressive image encryption scheme, and we unitized the improved 2D CML model for compression. The analysis and simulation demonstrate that the improved image encryption scheme possesses perfect encryption characteristics and application prospects.

---

**Table 5: The correlation coefficients results of the proposed scheme and other schemes.**

| Image          | Plain image | | | | | | Encrypted image | | | | |
|----------------|-------------|---|---|---|---|---|---|---|---|---|---|---|---|
| Lena in our scheme | 0.8871 | 0.9316 | 0.8567 | 0.0016 | 0.0002 | 0.0038 | |
| Lena in [24]  | 0.8871 | 0.9316 | 0.8567 | 0.0003 | 0.0040 | 0.0013 | |
| Lena in [25]  | 0.8871 | 0.9316 | 0.8567 | 0.0013 | 0.0034 | 0.0072 | |
| Lena in [26]  | 0.8871 | 0.9316 | 0.8567 | -0.0038 | -0.0026 | 0.0017 | |
| Lena in [27]  | 0.8871 | 0.9316 | 0.8567 | -0.0031 | 0.0025 | -0.0001 | |
| Lena in [28]  | 0.8871 | 0.9316 | 0.8567 | 0.0046 | -0.0028 | 0.0014 | |
| Lena in [29]  | 0.8871 | 0.9316 | 0.8567 | 0.0005 | -0.0070 | 0.0006 | |
| Lena in [30]  | 0.8871 | 0.9316 | 0.8567 | -0.0047 | 0.0028 | -0.0043 | |

**Table 6: The NPCR and UACI results of the proposed scheme and other schemes.**

<table>
<thead>
<tr>
<th>Image</th>
<th>NPCR R</th>
<th>NPCR G</th>
<th>NPCR B</th>
<th>UACI R</th>
<th>UACI G</th>
<th>UACI B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena in our scheme</td>
<td>0.9961</td>
<td>0.9963</td>
<td>0.9961</td>
<td>0.3347</td>
<td>0.3345</td>
<td>0.3348</td>
</tr>
<tr>
<td>Lena in [24]</td>
<td>0.9961</td>
<td>0.9961</td>
<td>0.9961</td>
<td>0.3346</td>
<td>0.3346</td>
<td>0.3347</td>
</tr>
<tr>
<td>Lena in [25]</td>
<td>0.9969</td>
<td>0.9969</td>
<td>0.9969</td>
<td>0.3345</td>
<td>0.3346</td>
<td>0.3347</td>
</tr>
<tr>
<td>Lena in [26]</td>
<td>0.9958</td>
<td>0.9958</td>
<td>0.9966</td>
<td>0.3345</td>
<td>0.3346</td>
<td>0.3347</td>
</tr>
<tr>
<td>Lena in [27]</td>
<td>0.9967</td>
<td>0.9969</td>
<td>0.9969</td>
<td>0.3352</td>
<td>0.3353</td>
<td>0.3354</td>
</tr>
<tr>
<td>Lena in [28]</td>
<td>0.9961</td>
<td>0.9961</td>
<td>0.9961</td>
<td>0.3349</td>
<td>0.3349</td>
<td>0.3347</td>
</tr>
<tr>
<td>Lena in [29]</td>
<td>0.9973</td>
<td>0.9968</td>
<td>0.9970</td>
<td>0.3346</td>
<td>0.3345</td>
<td>0.3346</td>
</tr>
<tr>
<td>Lena in [30]</td>
<td>0.9967</td>
<td>0.9964</td>
<td>0.9965</td>
<td>0.3351</td>
<td>0.3350</td>
<td>0.3349</td>
</tr>
</tbody>
</table>

**Table 7: The information entropy results of the proposed scheme and other schemes.**

<table>
<thead>
<tr>
<th>Image</th>
<th>Plain image</th>
<th>Encrypted image</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena in our scheme</td>
<td>6.9684</td>
<td>7.5940</td>
<td>7.2531</td>
<td>7.9985</td>
<td>7.9985</td>
<td>7.9985</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lena in [27]</td>
<td>6.9686</td>
<td>7.5952</td>
<td>7.2531</td>
<td>7.9976</td>
<td>7.9972</td>
<td>7.9972</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lena in [29]</td>
<td>6.9686</td>
<td>7.5952</td>
<td>7.2531</td>
<td>7.9972</td>
<td>7.9973</td>
<td>7.9971</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Data Availability**

The data used to support the findings of this study are available within the article.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This work was supported by grants from the National Natural Science Foundation of China (no. 61572089), the Doctoral Talent Training Project of Chongqing University of Posts and Telecommunications (no. BYJS202003), the Science and Technology Foundation Project of Guizhou Province (QianKeHeJiChu[2020]1Y422), and the Key Project Research Achievements of Guizhou Education University in 2020 (no. 2020ZD006).
References


