Hindawi
Complexity
Volume 2022, Article ID 5193618, 18 pages
https://doi.org/10.1155/2022/5193618

Research Article

Performance of the 2D Coupled Map Lattice Model and Its Application in Image Encryption

Zhuo Liu,[1,2] **Jin Yuan Liu**,[2,3] **Leo Yu Zhang**,[4] **Yong Zhao**,[1] **and Xiao Feng Gong**[5]

[1]*School of Mathematics and Big Data, Guizhou Education University, Guiyang 550018, China*
[2]*College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[3]*School of Intelligent Technology and Engineering, Chongqing University of Science and Technology, Chongqing 401331, China*
[4]*School of Information Technology, Deakin University, Victoria 3216, Australia*
[5]*Guizhou Science and Technology Information Center, Guiyang 550018, China*

Correspondence should be addressed to Leo Yu Zhang; leo.zhang@deakin.edu.au

Received 15 July 2021; Revised 15 February 2022; Accepted 1 April 2022; Published 11 May 2022

Academic Editor: Padmapriya Praveenkumar

The two-dimensional coupled map lattice (2D CML) model has been extensively employed as the basis component for designing various schemes in the cryptography system due to its complicated chaotic dynamic behavior. In this study, we analyze the chaotic characteristics of the 2D CML model, such as the Lyapunov exponent (LE), synchronization stability, bifurcation, and ergodicity. We then show that the chaotic sequences generated by the 2D CML model are random according to the NIST testing. Furthermore, we propose an image encryption scheme based on the 2D CML model and Singular Value Decomposition (SVD). In our scheme, the SVD method is used to reduce the image storage, and the Red, Green, and Blue channels of a color image will be encrypted through confusion and diffusion. The simulation results, as well as the results of the comparison with other schemes, demonstrate that our scheme possesses outstanding statistics, excellent encryption performance, and high security. It has great potential for ensuring the security of digital images in real applications.

1. Introduction

Chaos has become a fresh challenge in the cryptographic systems [1–7], because of its unique characteristics such as the sensitivity to the initial conditions and the unpredictability of trajectory. In subfields like the stream cipher [8], Hash function [9], and multimedia encryption [10], chaotic systems have been widely used as their basic components to construct cryptographic primitives.

The chaotic system commonly contains two categories. The first is a simple chaotic system, such as the Logistic map, the Tent map, and the Sine map. The chaos-based schemes based on a simple chaotic system have the highlight of being significantly more efficient. However, because of their simplistic structure, the chaotic dynamic behaviors are not sufficiently complicated, and some security vulnerabilities, such as being easy to predict and thus get attacked, exist in those schemes [11, 12]. The second is a higher-dimensional chaotic system, which has a significantly greater Lyapunov exponent (LE) and wider bifurcation interval than the simple one, and its chaotic characteristics are more complicated. As a result, the higher-dimensional one is generally regarded as more suitable for constructing the chaos-based schemes [8–10].

In the past decades, many researchers have committed to the chaos-based image encryption schemes with the aim of resisting attacks that make use of high pixel correlation and redundancy of digital images. According to the discrete output signal of Chen's chaotic system, a chaos-based image encryption algorithm has been presented [13]; the simulation results show that the scheme can withstand a brute-force attack. The spatiotemporal chaos was used to construct a new chaos-based encryption [14], which is both efficient and secure. A new color image encryption scheme using the combination of different 1D chaotic maps was introduced [15]; the experimental results demonstrate that the scheme

owns remarkable performance in noise and attacks. The enhanced Sine map was used to propose a unique image encryption approach in which row-by-row and column-by-column concepts were introduced [16], and the strategy is both efficient and effective. The scheme in [17] studied a novel chaos-based image encryption scheme based on the Lorenz chaotic system, and experimental results demonstrate the effectiveness and superiority of the algorithm. By imitating the jigsaw method, a chaos-based image encryption scheme was designed in [18], and the experiment and security analyses show that the scheme is both secure and efficient. A fast-reaching finite time synchronization approach for chaotic systems along with its application to medical image encryption is proposed in [19], which owns good robustness and a fast convergence rate. A new chaotic system with hyperbolic sinusoidal function is designed in [20], and a novel voice encryption algorithm based on the new system is proposed. The chaos-based satellite image encryption system is shown in [21], and it is secure, reliable, robust, and simple to implement.

For all the aforementioned image encryption schemes [13–21], higher-dimensional chaotic systems are employed as their core. However, for most employed chaotic systems, their LE values are either not sufficiently large or derived by simulations. That said, a theoretic analysis of the desirable characteristics for employing those models in cryptographic applications is still missing. Moreover, even if a desired higher-dimensional chaotic system is used, the above schemes fail to justify the usage of additional heuristic procedures to turn the chaotic sequences into random binary streams. Indeed, without addressing these shortcomings, cryptographic primitives based on higher-dimensional chaotic systems are also vulnerable to simple attacks [22].

To address the aforementioned shortcomings and to better balance efficiency and security, the 2D CML model, whose characteristics have been theoretically analyzed in [23], is used as the key component for constructing a novel image encryption scheme. We choose the piecewise Logistic map (PLM) as the local map, since it is more sophisticated than the Logistic map, and we then theoretically investigate the 2D CML system instantiated with PLM. In particular, for this specific system, its properties like LE, synchronization stability, bifurcation, and ergodicity are all thoroughly studied. When the parameters of the system are appropriately chosen, we show that the chaotic sequences can be directly extracted as random binary stream without any further processing, and the extracted stream passes the NIST randomness test suite. Powered by the theoretical studies, using the singular value decomposition (SVD) method, we reduce the storage of the original image, and the block of the combined image in Red, Green, and Blue can improve the running time of the scheme.

In a nutshell, this work makes the following contributions:

(i) When the PLM is used as the local map, the LE of the 2D CML model is proven to be larger, and its bifurcation and ergodicity become much wider. All these indicate that the 2D CML model has complex chaotic behavior, and it can be used as a good candidate to construct image encryption schemes.

(ii) The random binary stream can be extracted directly by using the chaotic sequences generated by the 2D CML model. In particular, we can obtain 32 bits from each node of the model, and the NIST test suite confirms that the extracted binary sequences have good randomness.

(iii) According to the SVD approach, the storage of the original image becomes smaller, the confusion in the block of the combined image in R, G, B can improve the running time of our scheme, and also the diffusion has been performed based on the chaotic sequences produced by the 2D CML model. The simulation experiments show that our scheme has good encryption performance.

The remaining parts of this work are organized as follows. Section 2 shows the preliminary knowledge, and the characteristics of the 2D CML model are analyzed in Section 3. In Section 4, the random binary sequences based on the 2D CML model are generated. Section 5 studies an image encryption scheme based on SVD and 2D CML chaotic sequences. The performance of the proposed image encryption scheme is evaluated in Section 6 and the last section draws the conclusion of this work.

2. Preliminaries

2.1. CML Model. The CML model proposed by Kaneko is a classic form of the spatiotemporal chaos model [24], and it is formulated as

$$x_{n+1}^{s} = (1-\varepsilon) f\left(x_n^s\right) + \frac{\varepsilon}{2}\left[f\left(x_n^{s-1}\right) + f\left(x_n^{s+1}\right)\right], \quad (1)$$

where $f(\cdot)$ denotes the local chaotic map; $s = 1, 2, \ldots, U$, with U being the size of the CML model. The periodic boundary condition of the CML model is $x_n^0 = x_n^{U+1}$.

To improve the complexity of CML, it is later extended into higher-dimensional spaces, for example, the two-dimensional one. In the 2D CML model, the local node is affected by the nearest four nodes simultaneously; that is,

$$x_{n+1}^{s,t} = (1-\varepsilon) f\left(x_n^{s,t}\right) + \frac{\varepsilon}{4}\left[f\left(x_n^{s-1,t}\right) + f\left(x_n^{s+1,t}\right) + f\left(x_n^{s,t+1}\right) + f\left(x_n^{s,t-1}\right)\right], \quad (2)$$

where $s = 1, 2, \ldots, R$ and $t = 1, 2, \ldots, L$ are the row and column indexes of the nodes, respectively. The periodic boundary conditions are $x_n^{R+1,t} = x_n^{0,t}$ and $x_n^{s,L+1} = x_n^{s,0}$. From equation (2), the value of the current node $x_{n+1}^{s,t}$ at the $(n+1)$-timestamp is determined by the local node $f(x_n^{s,t})$, the left node $f(x_n^{s-1,t})$, the right node $f(x_n^{s+1,t})$, the top node $f(x_n^{s,t-1})$, and the bottom node $f(x_n^{s,t+1})$, respectively.

According to [23], the LE values of 2D CML are given by

$$\mathrm{LE}s = \mathrm{LE}_f + \ln\left|1 - \varepsilon + \frac{\varepsilon}{2}\left(\cos\frac{2\pi r}{R} + \cos\frac{2\pi l}{L}\right)\right|, \quad (3)$$

where $r = 1, \ldots, R$, $l = 1, \ldots, L$, and LE_f is the LE value of the employed local chaotic map f $(\cdot)$. When $r = 1$ and $l = 1$, the LEs of 2D CML reach the maximum LE (MLE) LE_f. According to equation (3), we can easily get the following theorem.

Theorem 1. *The MLE of the 2D CML model is independent of the model size, but it is determined by the local chaotic map $f(\cdot)$.*

According to Theorem 1, the local chaotic map has special significance for the 2D CML model and directly decides the MLE value and chaotic characteristics of the model. Consequently, selecting a larger LE in the local map indicates more complexity of the model. As will be discussed later, we use the PLM with $\mu = 4$ and $N = 64$ as the local chaotic map because it has a larger LE.

2.2. The Piecewise Logistic Map. The PLM is the enhanced version of the well-known Logistic map [25], and it possesses much larger LE and more complex chaotic characteristics than the Logistic map. The PLM is defined as

$$x_{m+1} = \mathrm{PLM}(x_m) = \begin{cases} N^2\mu x_m\left(\frac{1}{N} - x_m\right), & 0 < x_m < \frac{1}{N}, \\ 1 - N^2\mu\left(x_m - \frac{1}{N}\right)\left(\frac{2}{N} - x_m\right), & \frac{1}{N} < x_m < \frac{2}{N}, \\ N^2\mu\left(x_m - \frac{1}{N}\right)\left(\frac{i}{N} - x_m\right), & \frac{1}{N} < x_m < \frac{i}{N}, \\ 1 - N^2\mu\left(x_m - \frac{i}{N}\right)\left(\frac{i+1}{N} - x_m\right), & \frac{i}{N} < x_m < \frac{i+1}{N}, \\ \cdots & \cdots \\ N^2\mu\left(x_m - \frac{N-2}{N}\right)\left(\frac{N-1}{N} - x_m\right), & \frac{N-2}{N} < x_m < \frac{N-1}{N}, \\ 1 - N^2\mu\left(x_m - \frac{N-1}{N}\right)(1 - x_m), & \frac{N-1}{N} < x_m < 1, \end{cases} \tag{4}$$

where $x_m \in (0, 1)$ is the state value, $\mu \in (0, 4]$ is the control parameter, and N is the segment number of PLM. When $N = 64$ and $\mu = 4$, its LE value is 4.574594, and hence the MLE of 2D CML is the same.

2.3. The Binary Format. When designing digital image encryption methods based on chaotic systems, the real-valued chaotic orbits need to be converted into binary to obtain pseudorandom sequences (i.e., 0s or 1s). We consider the fixed-point representation of chaotic orbits within the range $[0, 1]$ using Definition 1.

Definition 1. A floating number $D \in [0, 1]$ can be written into the binary format with M bits as follows:

$$D = 0.C^1(x)C^2(x)\cdots C^{M-1}(x)C^M(x), \tag{5}$$

where $C^M(x) \in \{0, 1\}$.

2.4. Singular Value Decomposition. SVD is an effective method for the factorization of an $M \times N\,(M \neq N)$ matrix, and it is commonly used in signal processing and image compression. The general form of SVD is given by

$$\mathbf{A} = \mathbf{U}\Sigma\mathbf{V}^{\mathbf{T}}, \tag{6}$$

where $\mathbf{U}$ and $\mathbf{V}$ are $M \times M$ and $N \times N$ matrices, respectively, and Σ represents the $M \times N$ singular value matrix, whose elements are all 0 except the SVD values on its diagonal.

3. Performance Analyses of the 2D CML Model

As discussed previously, the performance of the 2D CML model is critical for designing chaos-based cryptographic primitives. In the 2D CML model, according to equation (3), its performance is solely determined by the local chaotic map $f(\cdot)$. Therefore, selecting a local map $f(\cdot)$ with a large LE is essential, since it in turn enhances the overall complexity of the 2D CML model. With this consideration, we hereby choose the PLM with $N = 64$ and $\mu = 4$ as the local map.

3.1. The Lyapunov Exponent Analysis. LE is an index used to judge whether a dynamic system is chaotic or not, and a positive LE indicates chaos. Moreover, the larger the value of LE was, the more complex the chaotic system would be. The LE of a chaotic system $x_{n+1} = F(x_n)$ is defined as

$$\mathrm{LE} = \lim_{x \longrightarrow \infty} \frac{1}{n} \ln \left| \prod_{s=0}^{n} F'(x) \right|. \tag{7}$$

Taking the PLM as the local map, we plot the LE values of all 64 nodes $(L = R = 8)$ according to (3) in Figure 1. According to this figure, it can be seen that the LEs lie within the interval $[4, 6]$; all are positive and relatively large (compared to LE of the original Logistic map). This fact demonstrates that the 2D CML model has complex chaotic dynamic behaviors.

Moreover, by taking derivative of equation (3) with respect to ε, we can further have

$$\mathrm{LE}' = \frac{\cos 2\pi r/R + \cos 2\pi l/L - 2}{2 + \varepsilon(\cos 2\pi r/R + \cos 2\pi l/L - 2)}. \tag{8}$$

To select the coupling parameter ε with better chaotic property, we first consider the case where the denominator $2 + \varepsilon(\cos 2\pi r/R + \cos 2\pi l/L - 2)$ of equation (8) is 0. In this case, $r = l = 4$ and $\varepsilon = 0.5$, so $\varepsilon = 0.5$ should be avoided. We then investigate the value of LE' by enumerating all the possibilities of l and r. It turns out that when $\varepsilon \in (0, 0.5)$, $\mathrm{LE}' < 0$ regardless of the choices of l and r, and, depending on specific choices of l and r, LE' can be either positive and negative for $\varepsilon \in (0.5, 1)$. That said, the value of LE monotonically decreases for $\varepsilon \in (0, 0.5)$ and fluctuates for $\varepsilon \in (0.5, 1)$ and smaller ε achieves better chaotic property.

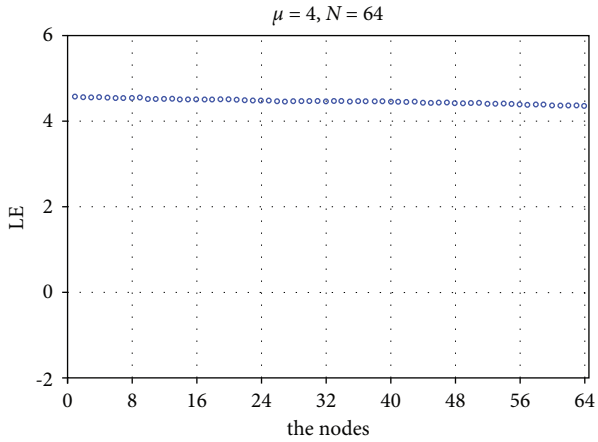

Figure 1: LE of the 8 × 8 2D CML model.

With this consideration and to maintain a certain level of coupling effect, we take the empirical value $\varepsilon = 0.1$ for 2D CML instantiated with PLM in the remainder of this paper.

3.2. The Synchronization Stability Analysis. The stability of periodic orbit and chaos synchronization of the 2D CML model are substantially more complicated [24] compared to its 1D counterpart. However, there is little theoretical study for its configuration. From the standpoint of cryptography applications, the parameter settings should ensure that the 2D CML model runs in a fully developed chaotic state. Thus, we present a theoretical investigation of the synchronization stability for the 2D CML model. Theoretically, for ordered LEs of the 2D CML, the second maximum LE value $\mathrm{LE}_2 > 0$ means that the system is in an asynchronous state, while $\mathrm{LE}_2 < 0$ means that it is synchronous.

To begin with, let $r = R$ and $l = L - 1$; according to equation (3), we can get LE_2 as

$$\mathrm{LE}_2 = \mathrm{LE}_f + \ln\left|1 - \varepsilon + \frac{\varepsilon}{2}\left(\cos 2\pi + \cos\frac{2\pi(L-1)}{L}\right)\right|. \quad (9)$$

Set $\mathrm{LE}_2 = 0$, and the critical value of L is

$$L_c = \left\lfloor \frac{2\pi}{\arccos\left(2e^{-\mathrm{LE}_f} - 2 + \varepsilon\right)/\varepsilon} \right\rfloor. \quad (10)$$

Here, L_c represents the minimum number of nodes that can ensure that the system is in an asynchronous state; that is, $L > L_c$ should be used to make $\mathrm{LE}_2 > 0$.

To verify the above-mentioned analysis, we take the Logistic map,

$$x_{n+1} = 4x_n(1 - x_n), \quad (11)$$

as the local chaotic map and set $R = L = 3$ and $\varepsilon = 0.9$ for the 2D CML model. For this specific 2D CML model, from equation (10), $L_c = 3$.

We randomly initialize the values of the 2D CML, which are denoted as $x_0^{s,t}, s = 1, 2, 3; t = 1, 2, 3$. Then, the 2D CML is iterated 3 times and 100 times and the values are denoted as $x_3^{s,t}$ and $x_{100}^{s,t}$, respectively. We plot $x_0^{s,t}$, $x_3^{s,t}$, and $x_{100}^{s,t}$ in Figure 2. From Figure 2(c), the state values of the nodes in the 2D CML model appear to be synchronized after 100 iterations, which confirms that the 2D CML model is not in a fully developed chaotic pattern. To make $\mathrm{LE}_2 > 0$, we set $L = 4 > L_c = 3$ for the 2D CML and keep all the other parameters unchanged. The simulation results are depicted in Figure 3. It is clear from this figure that no stable synchronous chaos can be observed in the states of the model. Thus, we can conclude that increasing the size of the 2D CML model is an effective way to guarantee that the 2D CML model is not in a synchronous pattern.

3.3. The Bifurcation Analysis. Bifurcation shows the sudden altering of the critical point when changing the parameters in a chaotic system. For the 2D CML model instantiated with the PLM, simulation results indicate that the bifurcations of all 64 nodes are almost the same. Taking the 1^{st} node as an example, we plot its bifurcation diagram in Figure 4. It is clear from this Figure 4 that changing μ significantly influences the bifurcation of the system. When $\mu \in (2, 4)$, the 2D CML model has well-established bifurcation performance. Specifically, the 2D CML model possesses the best bifurcation performance with $\mu = 4$.

3.4. The Ergodicity Analysis. For a chaotic system, ergodicity describes the randomness of statistical results in both time and space. If the states of the system cover a larger interval, the system is more complex. Here, with the parameter settings $\mu = 0.5, 1.0, 1.6, 2, 2.6, 3.0, 3.6$, and 4.0 for the 2D CML instantiated with the PLM, we plot the ergodicity of the model in Figures 5(a)–5(h). As can be seen, the 2D CML model covers the entire interval and has the best chaotic dynamic behavior when $\mu = 4$.

3.5. The Probability Density Distribution. PDD describes the distribution of chaotic state values in the phase space. We plot the PDD of the chaotic sequences generated by all the nodes in Figure 6 for the 2D CML instantiated with the PLM. According to Figure 6, it is clear that PDD of those sequences is uneven, with the peaks appearing in the intervals $[0.0, 0.2]$ and $[0.8, 1.0]$.

4. The Random Chaotic Sequences

According to the above-discussed theoretic analyses and simulation, apparently, when selecting the PLM with $\mu = 4, N = 64$ as the local map and setting $\varepsilon = 0.1$ for 2D CML, the model owns outstanding chaotic dynamic behaviors. Taking the 2D CML model as the key component, we derive random sequences through the following steps:

(i) Step 1: In the 2D CML model, set $R = L = 8$ and $\varepsilon = 0.1$, choose the PLM with $\mu = 4, N = 64$, iterate the model 1,000 times to avoid transition effect, and abandon these first 1,000 states.

(ii) Step 2: Continue to iterate the 2D CML model. For each iteration, a floating number $B \in (0, 1)$ is derived from each node, and there are totally 64

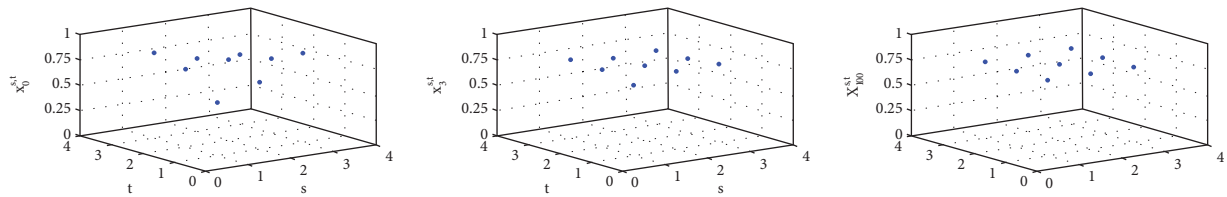

Figure 2: The values of the 3×3 2D CML model with the Logistic map: (a) $x_0^{s,t}$, (b) $x_3^{s,t}$, and (c) $x_{100}^{s,t}$.

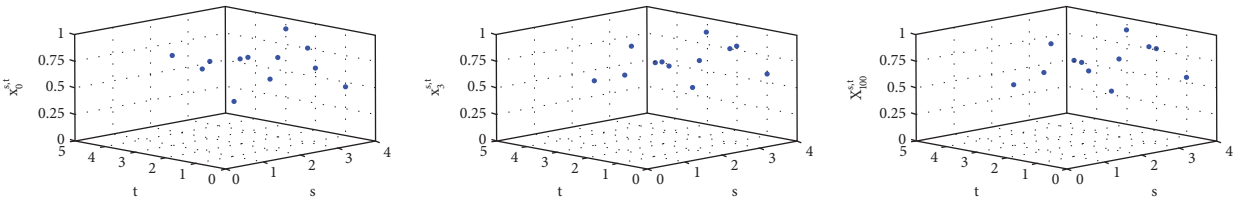

Figure 3: The values of the 3×4 2D CML model with the Logistic map: (a) $x_0^{s,t}$, (b) $x_3^{s,t}$, and (c) $x_{100}^{s,t}$.

floating numbers. Transform B into 64 binary bits according to Definition 1; that is,

$$B = 0.w_1 w_2 \cdots w_{63} w_{64}. \tag{12}$$

(iii) Step 3: The least significant 32 bits are the required binary bits; that is,

$$B' = w_{32} w_{33} \cdots w_{63} w_{64}. \tag{13}$$

For a single iteration of the 8×8 2D CML model, all those 64 nodes can directly generate $32 \times 64 = 2048$ bits. To further analyze the randomness of the binary stream, we use the NIST test suite and the key sensitivity analysis to demonstrate that the binary stream derived using the method above owns excellent randomness and key sensitivity performance.

4.1. Testing Results Analysis. The statistical test package launched by NIST is currently the most authoritative tool for testing the pseudorandom sequences, and it contains 15 subtests. For each test, there exists a p_{value} for measuring whether the sequences can pass the random testing successfully. If $p_{\text{value}} \geq \alpha$, it indicates pass. Otherwise, the sequences fail that test. We randomly initialize the 2D CML model according to the method in Section 4 and run the method 488, 888 times to have 1, 000 M bits. Set $\alpha = 0.01$ and split the 1, 000 M bits to 1, 000 groups of 1 M bit; the NIST test is then performed on these 1, 000 groups and the results are listed in Table 1. According to Table 1, it is clear that all the p_{value} are greater than 0.01, and the minimum pass rate and the maximum pass rate are 0.9841 and 0.9952, respectively. The testing results of p_{value} and pass rate show that the chaotic sequences produced by the 2D CML model possess good randomness.

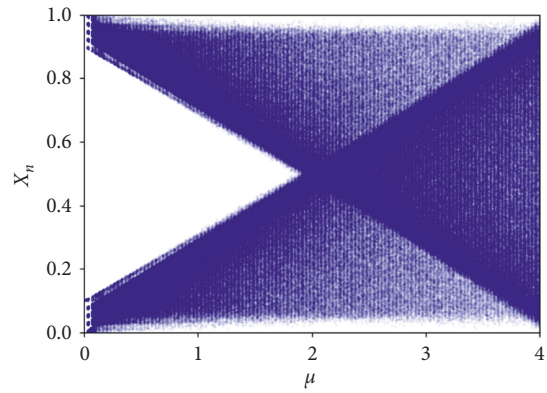

Figure 4: Bifurcation of the 1^{st} 1st node with the change in μ in the 8×8 2D CML model instantiated with PLM.

4.2. Sensitivity Analysis. Sensitivity means that a tiny change of the parameters will lead to huge changes in the output chaotic sequences. We set the parameters of the 2D CML model as the two following proximal cases:

Case I: $\varepsilon = 0.1$, $\mu = 4$, and $x_0 = 0.49903121525011673$;

Case II: $\varepsilon = 0.1$, $\mu = 4$, and $x_0 = 0.49903121625011673$; their outputted pseudorandom binary streams are collected, respectively. To verify the sensitivity, the steams are then used to mask the digital Lena image. The two versions of the masked image and their difference are shown in Figure 7.

Looking into the details of the difference image, the different rate of the encrypted images with Case I and Case II is 99.60%, and the histograms of the two masked images are almost uniform, as shown in Figures 7(f) and 7(g). Hence, the pseudorandom sequences derived from the method discussed in Section 4 own pretty good sensitivity.

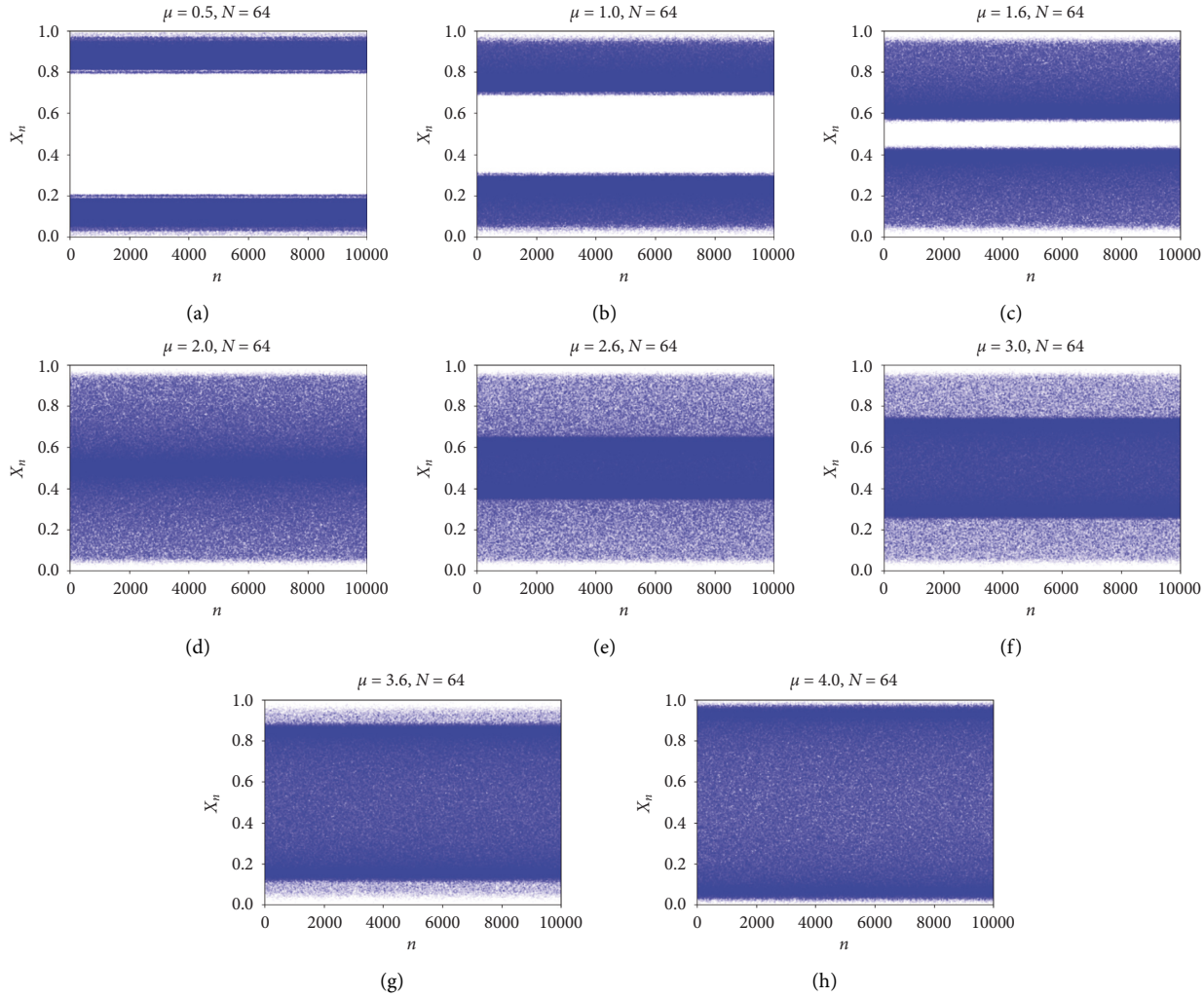

Figure 5: Ergodicity of the 8×8 2D CML model with different μ.

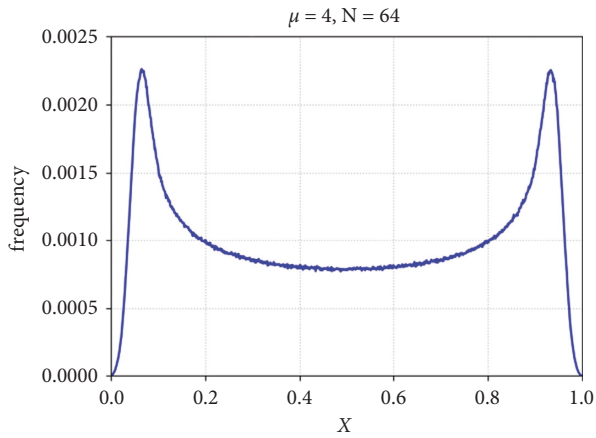

Figure 6: PDD of the 8×8 2D CML model.

5. The Proposed Encryption Scheme

Section 4 demonstrates that the chaotic sequences generated by the 2D CML model are random and they also own good sensitivity against the parameters. This section takes advantage of the chaotic sequences generated by the 2D CML model to design a digital image encryption scheme as an application. As depicted by Figure 8, the proposed image encryption scheme consists of three core components: SVD, confusion, and diffusion. The purpose of using SVD is to reduce storage and improve efficiency. For confusion, the cross-plane permutation in R, G, and B channels has been employed to comprehensively shuffle the pixel positions in the three-color planes via a single operation. The diffusion is performed based on the random chaotic sequences.

5.1. The Encryption Algorithm. The proposed image encryption algorithm, depicted by Figure 9, is elaborated as the four following steps, and also its pseudocode is presented as algorithm 1.

5.2. The Decryption Algorithm. The decryption is basically the inverse of the encryption process. In detail, the encrypted image **C** can be decrypted into the original image **P** according to the following steps. The pseudocode is shown in Algorithm 2.

Table 1: The test results of NIST 800-22.

No.	Test index	Pass number/failure number	Pass rate	P_{value}	Results
1	FT	992/08	0.9920	0.440975	Success
2	FBT	991/09	0.9910	0.233162	Success
3	CST (forward)	989/11	0.9890	0.397688	Success
	CST (reverse)	989/11	0.9890	0.408275	Success
4	RT	995/05	0.9950	0.217857	Success
5	LROBT	989/11	0.9890	0.682823	Success
6	BMRT	993/07	0.9930	0.755819	Success
7	DFTT	992/08	0.9920	0.560545	Success
8	NTMT*	990/10	0.9899	0.525430	Success
9	OTMT	992/08	0.9920	0.448424	Success
10	MUST	985/15	0.9850	0.149495	Success
11	AET	987/13	0.9870	0.883171	Success
		RET (the sample size = 629)			
	(1)	623/06	0.9905	0.744751	Success
	(2)	620/09	0.9857	0.980003	Success
	(3)	619/10	0.9841	0.705598	Success
12	(4)	626/03	0.9952	0.731821	Success
	(5)	625/04	0.9936	0.548839	Success
	(6)	621/08	0.9873	0.526040	Success
	(7)	622/07	0.9889	0.462960	Success
	(8)	622/07	0.9889	0.830070	Success
		REVT (the sample size = 629)			
	(1)	626/03	0.9952	0.692344	Success
	(2)	625/04	0.9936	0.261610	Success
	(3)	625/04	0.9936	0.418149	Success
	(4)	623/06	0.9905	0.290356	Success
	(5)	622/07	0.9889	0.089615	Success
	(6)	621/08	0.9873	0.854868	Success
	(7)	621/08	0.9873	0.882929	Success
	(8)	624/05	0.9921	0.299642	Success
13	(9)	621/08	0.9873	0.251135	Success
	(10)	621/08	0.9873	0.095926	Success
	(11)	624/05	0.9921	0.906025	Success
	(12)	624/05	0.9921	0.131195	Success
	(13)	626/03	0.9952	0.435787	Success
	(14)	623/06	0.9905	0.018417	Success
	(15)	620/09	0.9857	0.516370	Success
	(16)	621/08	0.9873	0.077315	Success
	(17)	620/09	0.9857	0.722038	Success
	(18)	621/08	0.9873	0.194881	Success
14	ST1	994/06	0.9940	0.397688	Success
	ST2	989/11	0.9890	0.344048	Success
15	LCT	990/10	0.9900	0.166260	Success

6. Experimental Analysis

To further analyze the characteristics of the proposed encryption algorithm, the following simulations are performed.

6.1. The Encryption and Decryption Image. For the plain Lena (512×512) and Chocolate (256×256) images, use SVD to decompose the images with the rate $p = 0.3$; the results are shown in Figures 10(b) and 10(d), respectively. From visual inspection, these two images are almost the same as the plain counterparts, shown in Figures 10(a) and 10(c).

Figures 10(e)–10(h) further depict the confusion result from equation (14). Moreover, the encrypted images and the recovered images are shown in Figures 10(i)–10(l). According to Figures 10(i)–10(l), the encrypted images are noisy, and the decrypted images in Figures 10(j) and 10(l) are the same as the original Lena and Chocolate images in Figures 10(a) and 10(d).

6.2. The Statistics Results. The histogram reflects the distribution of the image's pixel value; the more uniform the histogram of the encrypted image is, the better the scheme is. We plot the histogram results of the original images (Lena and Chocolate) and the encrypted images in Figures 11 and 12, respectively. According to Figures 11(a)–11(c), the histogram results of the original image are highly uneven. However, the histograms of the encrypted images in R, G,

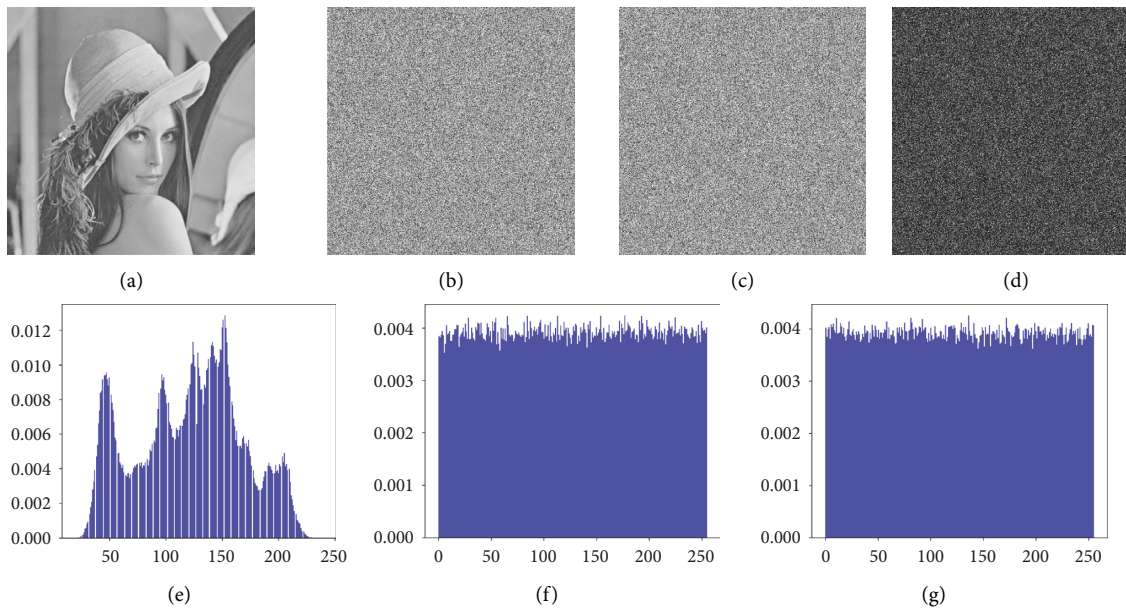

Figure 7: The results of Lena image and the encrypted Lena image. (a) The plain Lena image; (b) the encrypted image with case (i); (c) the encrypted image with case II; (d) the different image with case I and case II; (e) histogram of the plain Lena image; (f) histogram of the encrypted image with case (i); (g) histogram of the encrypted image with case II.

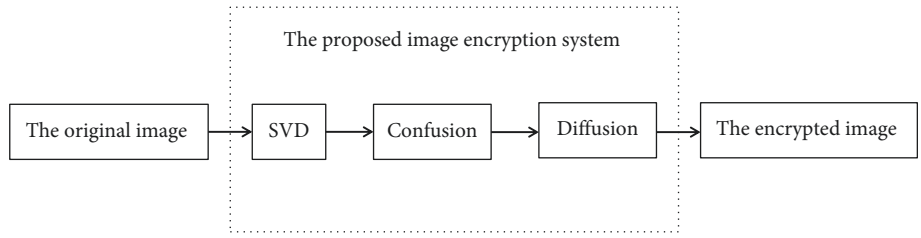

Figure 8: The core parts of our proposed image encryption scheme.

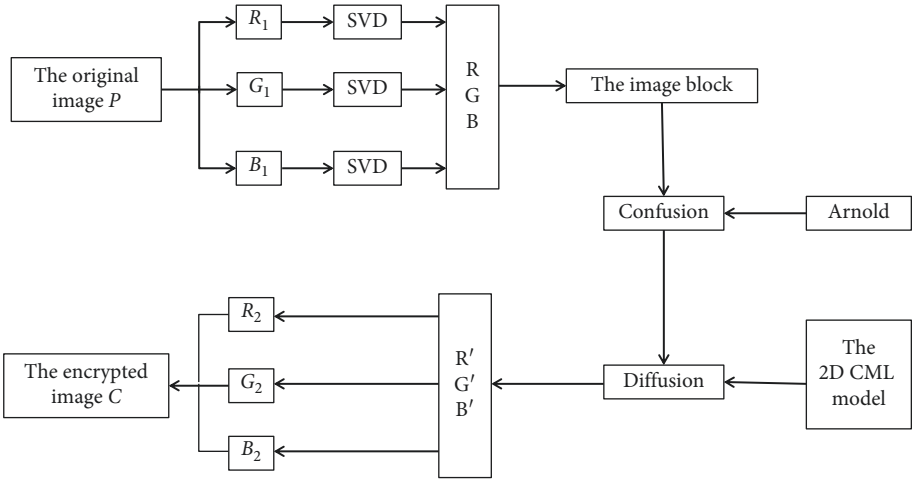

Figure 9: The proposed image encryption scheme.

and B channels are uniform in Figures 11(d)–11(f), and the histogram results of the Chocolate image are similar to those of the Lena image.

According to the approach depicted in [26], the uniformity of histogram can be assessed via the χ^2 test. In this test, the significance value is set as 0.05; if the resultant $P-\text{value} < 0.05$, the decision is 1 (rejecting the hypothesis); if the resultant $P-\text{value} > 0.05$, the decision is 0 (accepting the hypothesis). The values of the χ^2 test for the histogram results of the Lena image and the Chocolate image shown in

Input: The original image $\mathbf{P}$ with size $N \times N$
Output: The cipher image $\mathbf{C}$
(1) Use SVD to decompose $\mathbf{P}$ and get the inverse-transformed image
(2) Divide the inverse-transformed image into $\mathbf{R}_1$, $\mathbf{G}_1$ and $\mathbf{B}_1$ to get the new matrix $\mathbf{P}'$
(3) Divide $\mathbf{P}'$ into small blocks with size 3×1
(4) **while** time $\leq$ count1 **do**
(5) $$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \% N$$
(6) **end**
(7)
(8) **while** time $\leq$ count2 **do**
(9) $\mathbf{P}'''(t) = \mathbf{P}''(t) \oplus \mathbf{H}(t) \oplus \mathbf{P}'''(t-1)$,
(10) **end**
(11) Divide the sequence $\mathbf{P}'''$ into three 2D matrices $\mathbf{R}_2$, $\mathbf{G}_2$, $\mathbf{B}_2$ with size $N \times N$ to form the R, G, B channel of the cipher image $\mathbf{C}$;

(i) Step 1: For an original image $\mathbf{P}$ with size $N \times N$, use SVD to decompose $\mathbf{P}$ and keep $p = 0.3$ of the singular values. Then, separate the inverse-transformed image into $\mathbf{R}_1$, $\mathbf{G}_1$, and $\mathbf{B}_1$ according to its color channels. Stack the three matrices $\mathbf{R}_1$, $\mathbf{G}_1$, and $\mathbf{B}_1$ to get a new matrix $\mathbf{P}'$ with size $3N \times N$.
(ii) Step 2: Divide matrix $\mathbf{P}'$ into small blocks with size 3×1, and in total there will be $N \times N$ blocks. Use the following equation:
$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (N),$$
with $a = 3$ and $b = 4$ to confuse the $N \times N$ blocks of matrix $\mathbf{P}'$ for a few times (count1). The resultant block-shuffled matrix is denoted as $\mathbf{P}''$.
(iii) Step 3: Stack $\mathbf{P}''$ row by row to get a sequence of length $3N \times N$ and generate a chaotic sequence $\mathbf{H}$ of length $3N \times N$ with the method in Section 4, and then diffuse $\mathbf{P}''$ for some times (count2) by the following equation:
$\mathbf{P}'''(t) = \mathbf{P}''(t) \oplus \mathbf{H}(t) \oplus \mathbf{P}'''(t-1)$,
where $t \in 1, 2, \ldots 3N \times N$ and $\mathbf{P}'''(0) = 69$.
(iv) Step 4: Divide sequence $\mathbf{P}'''$ into three 2D matrices $\mathbf{R}_2$, $\mathbf{G}_2$, and $\mathbf{B}_2$ with size $N \times N$ to form the R, G, and B channel of the cipher image $\mathbf{C}$.

Algorithm 1: The proposed image encryption algorithm.

Input: The cipher image $\mathbf{C}$
Output: The original image $\mathbf{P}$ with size $N \times N$
(1) The encrypted image $\mathbf{C}$ with size $N \times N$ is
(2) divided $\mathbf{C}$ into $\mathbf{R}_2$, $\mathbf{G}_2$, $\mathbf{B}_2$; Combine those three components and reshape it to a sequence $\mathbf{P}'''$ of length $3N \times N$;
(3) **while** time $\leq$ count1 **do**
(4) $$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \% N$$
(5) **end**
(6) **while** time $\leq$ count2 **do**
(7) $\mathbf{P}'(t) = \mathbf{P}''(t) \oplus \mathbf{H}(t) \oplus \mathbf{P}'(t-1)$
(8) **end**
(9) Recover the original image $\mathbf{P}$ from $\mathbf{P}'$ according to SVD.

(i) Step 1: The encrypted image $\mathbf{C}$ with size $N \times N$ is divided $\mathbf{C}$into $\mathbf{R}_2$, $\mathbf{G}_2$, and $\mathbf{B}_2$; then combine those three components and reshape it to a sequence $\mathbf{P}'''$ of length $3N \times N$.
(ii) Step 2: $\mathbf{P}'''$ is then reshaped to a matrix with size $3N \times N$, and it will be further divided into blocks of size 3×1. All $N \times N$ blocks of $\mathbf{P}'''$ will be shuffled by using the following equation for the same number of times used for encryption:
$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod (N),$$
where $a = 3, b = 4$. The result is denoted as $\mathbf{P}''$.
(iii) Step 3: Use the chaotic sequences $\mathbf{H}$ to diffuse sequence $\mathbf{P}''$ to get $\mathbf{P}'$; that is,$\mathbf{P}'(t) = \mathbf{P}''(t) \oplus \mathbf{H}(t) \oplus \mathbf{P}'(t-1)$,
where $t \in 1, 2, \ldots, 3N \times N$.
(iv) Step 4: Recover the original image $\mathbf{P}$ from $\mathbf{P}'$ according to SVD.

Algorithm 2: The image decryption algorithm.

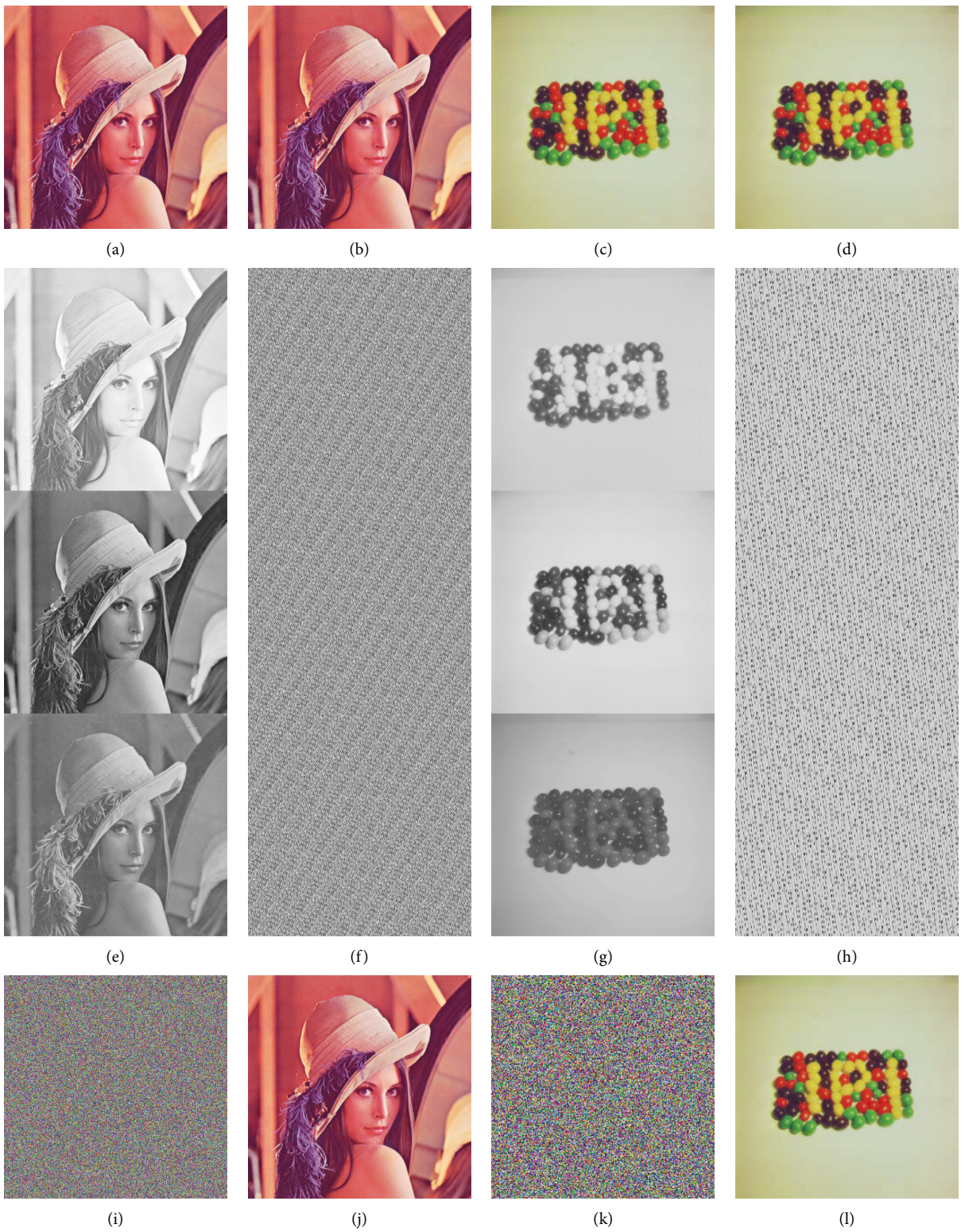

Figure 10: The original image and the SVD image.

Figures 11 and 12 are listed in Table 2. It can be seen from this table that all those P values (i.e., 0.9005, 0.7919, 0.6577, 0.5449, 0.2246, and 0.2069) are greater than the significance value 0.05 for both the encrypted Lena and Chocolate images, thus validating the uniformity of the histograms. So, it is evident that the redundancy of plain images is completely concealed, which confirms the failure of statistical attack.

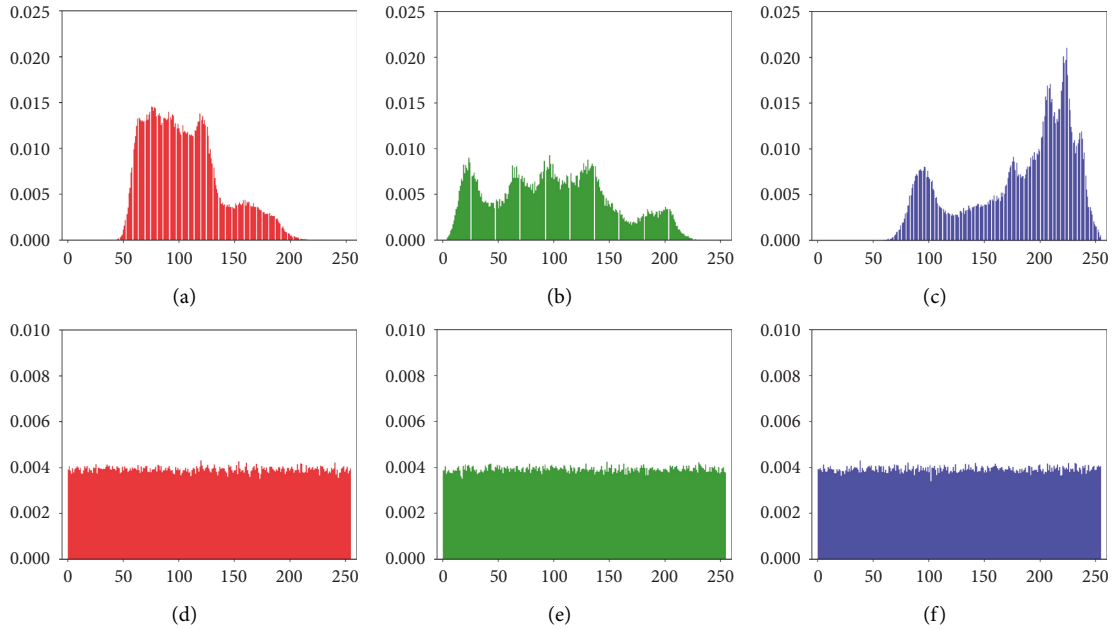

Figure 11: The histogram of the Lena image and the encrypted Lena image. (a) Histogram of the Lena image in R; (b) histogram of the Lena image in G; (c) histogram of the Lena image in B; (d) histogram of the encrypted Lena image in R; (e) histogram of the encrypted Lena image in G; (f) histogram of the encrypted Lena image in B.

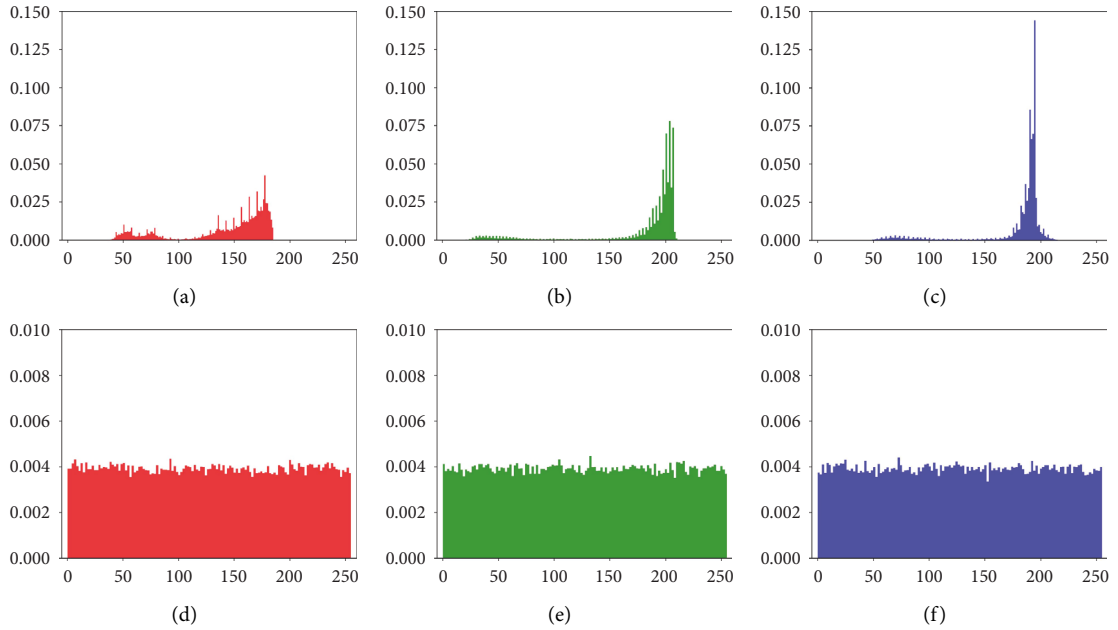

Figure 12: The histogram results of Chocolate image and the encrypted Chocolate image. (a) Histogram of the Chocolate image in R; (b) histogram of the Chocolate image in G; (c) histogram of the Chocolate image in B; (d) histogram of the encrypted Chocolate image in R; (e) histogram of the encrypted Chocolate image in G; (f) histogram of the encrypted Chocolate image in B.

The correlation coefficient is commonly used to measure the independence of horizontal (H), vertical (V), and diagonal (D) adjacent pixels. It is defined by

$$\operatorname{cov}(x, y) = E\{(x - E(x))(y - E(y))\}, \tag{14}$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{15}$$

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

We use 2,000 pairs for each of the H, V, and D directions and present the correlation values in Figures 13 and 14. According to Figures 13(a)–13(i), the correlation coefficients in the H, V, and D directions of R, G, and B channels are concentrated. However, the correlation coefficients of the

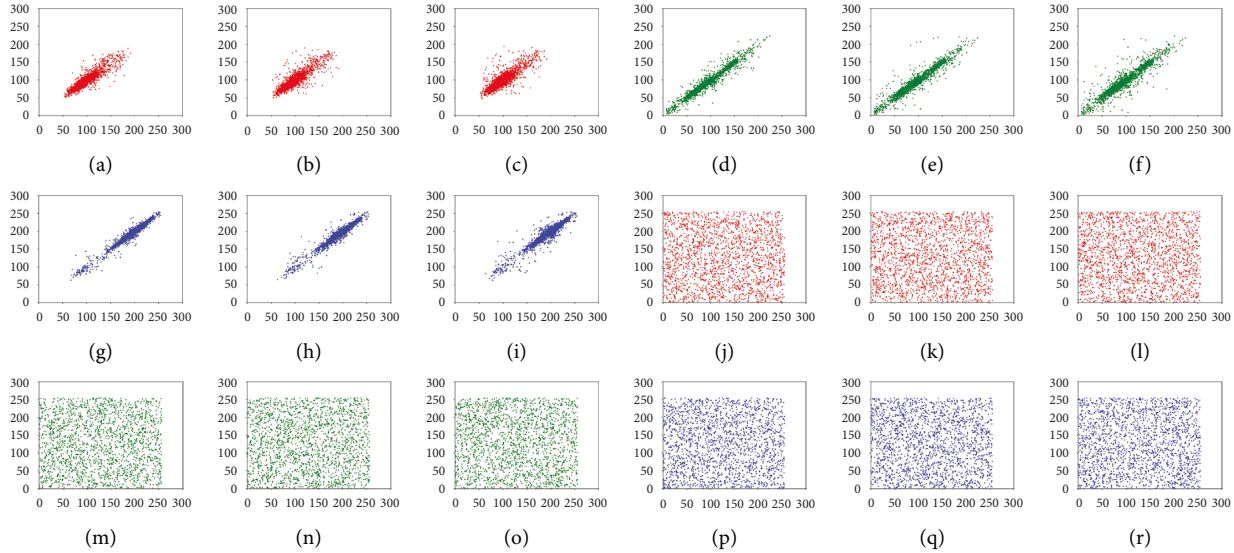

FIGURE 13: The correlation results of the Lena image and the encrypted Lena image. (a) (H, V, D) correlation of the Lena image in R; (b) (H, V, D) correlation of the Lena image in G; (c) (H, V, D) correlation of the Lena image in B; (d) (H, V, D) correlation of the encrypted Lena image in R; (e) (H, V, D) correlation of the encrypted Lena image in G; (f) (H, V, D) correlation of the encrypted Lena image in B.

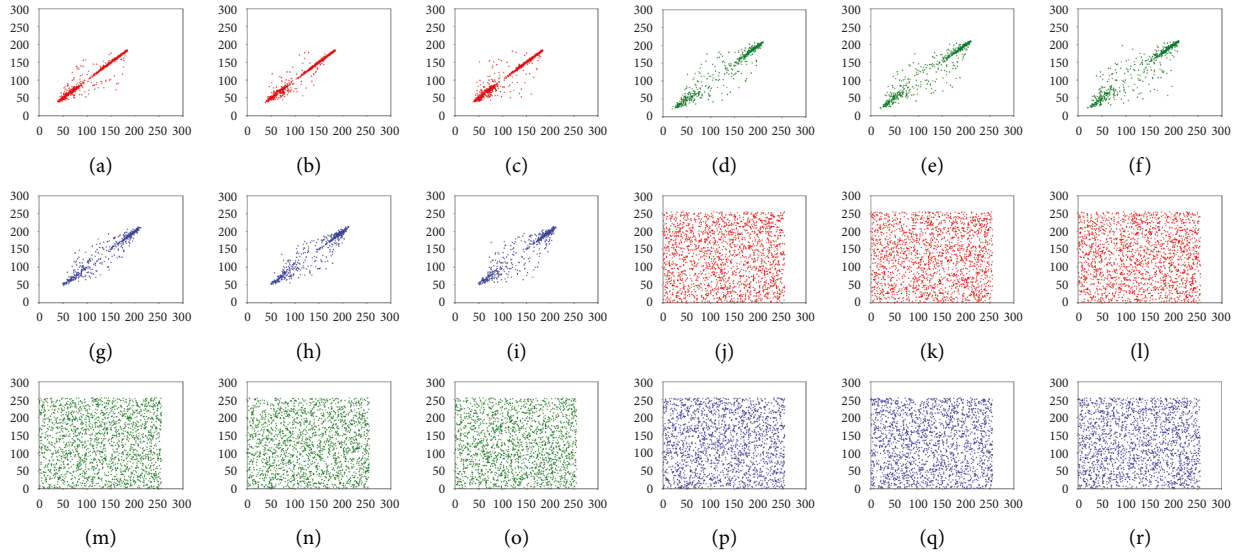

FIGURE 14: The correlation results of the Chocolate image and the encrypted Chocolate image. (a) (H, V, D) correlation of the Chocolate image in R; (b) (H, V, D) correlation of the Chocolate image in G; (c) (H, V, D) correlation of the Chocolate image in B; (d) (H, V, D) correlation of the encrypted Chocolate image in R; (e) (H,V, D) correlation of the encrypted Chocolate image in G; (f) (H, V, D) correlation of the encrypted Chocolate image in B.

encrypted image become uniform, as shown in Figures 13(j)–13(r). Furthermore, we calculate the correlation coefficients of 2, 000 pairs of adjacent pixels in the H, V, and D directions according to equations (18) and (19). The correlation coefficient results are listed in Table 3. It can be seen from this table that the correlation coefficients are all close to 0, which indicates that the pixels of the encrypted image are almost independent of each other.

6.3. Shannon Entropy Analysis. The Shannon entropy reflects the average information contained in an image. It is defined as

$$IE = \sum_{I=0}^{n} p(X_I)\log_2^{p(X_I)}, \tag{16}$$

where X_I is the grayscale value of the image and $p(X_I)$ is the rate of the grayscale value X_I. In the encrypted image, the ideal entropy of a grayscale pixel is 8.0. The global Shannon entropy values of the original image and the encrypted image are calculated via equation (20) and listed in Table 4. According to this table, the values of global Shannon entropy of the encrypted images are quite near 8.0.

To overcome the weaknesses of the global Shannon entropy, such as inaccuracy, inconsistency, and low

Table 2: Histogram uniformity assessment based on the chi-square test.

Image	Histogram of the encrypted Lena image			Histogram of the encrypted Chocolate image		
	R	G	B	R	G	B
P values	0.2246	0.6577	0.2069	0.9005	0.7919	0.5449
Decision (H = 0 or 1)	0; accepted	0; accepted	0; accepted	0; accepted	0; accepted	0; accepted

Table 3: The correlation coefficients of the original image and the encrypted image.

Image	Channel	Original image			Encrypted image		
		H	V	D	H	V	D
Lena	R	0.8946	0.9247	0.8636	−0.0061	0.0042	−0.0007
	G	0.9562	0.9714	0.9307	−0.0040	−0.0003	−0.0045
	B	0.9727	0.9826	0.9515	−0.0018	−0.0013	−0.0032
Chocolate	R	0.9889	0.9851	0.9794	−0.0029	0.0095	−0.0022
	G	0.9768	0.9823	0.9647	0.0021	−0.0077	−0.0008
	B	0.9713	0.9780	0.9573	0.0024	−0.0049	0.0047

efficiency, we use the local Shannon entropy proposed in [27] to measure the encrypted image. For this purpose, we select some nonoverlapping image blocks in the encrypted image and compute the local Shannon entropy value of each block and further calculate the mean of those Shannon entropy values via the following equation:

$$H_{k,T_B}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{17}$$

where k is the number of the randomly selected nonoverlapping image blocks, its minimum number is 30, and T_B is the block size of the nonoverlapping image block.

In our testing, the parameter k is set as 40. Moreover, the block size T_B is 4096 (64×64). The local Shannon entropy values of the encrypted Lena and Chocolate images are presented in Table 5. As can be seen from the table, the mean values of the encrypted Lena image's local Shannon entropy in RGB channel are 7.997297, 7.997129, and 7.997207, respectively, and those of the encrypted Chocolate image's local Shannon entropy are 7.973989, 7.973779, and 7.975590. Both are close to the ideal value of 7.984977322 for 8-bit grayscale images with $64 \times 64 \times 3$ in [26, 28]. To summarize, both global and local Shannon entropy values are very close to the ideal value, which demonstrates the high randomness of the encrypted images.

Table 4: Global Shannon entropy of the original image and the encrypted image.

Image	Channel	Original image	Encrypted image
Lena	R	6.9684	7.9992
	G	7.5940	7.9999
	B	7.2531	7.9992
Chocolate	R	6.5464	7.9975
	G	5.6947	7.9974
	B	5.2626	7.9972

Table 5: Local Shannon entropy of the encrypted image.

Image	Channel	Local Shannon entropy
Lena	R	7.997297
	G	7.997129
	B	7.997207
Chocolate	R	7.973989
	G	7.973779
	B	7.975590

6.4. Differential Attack Analysis. The differential attack is an attack method in which the attacker slightly modifies the plaintext and compares the difference of the ciphertexts generated before and after the modification. The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are two important indicators to judge whether the encryption scheme can resist the differential attack. Those two indexes are defined as

$$\begin{aligned} \mathrm{NPCR}(P_1, P_2) &= \frac{1}{M \times N} \sum_{a=1}^{M} \sum_{b=1}^{N} \mathrm{Sign}(\mathrm{D}(a,b)), \\ \mathrm{UACI}(P_1, P_2) &= \frac{1}{M \times N} \left(\sum_{a=1}^{M} \sum_{b=1}^{N} \frac{D(a,b)}{255} \right), \end{aligned} \tag{18}$$

Table 6: Theoretical NPCR critical values for different image size.

Size	Theoretical NPCR critical values		
	$\alpha = 0.05$	$\alpha = 0.01$	$\alpha = 0.001$
512×512	$N^*_{0.05} = 0.995893$	$N^*_{0.01} = 0.995810$	$N^*_{0.001} = 0.995717$
256×256	$N^*_{0.05} = 0.995693$	$N^*_{0.01} = 0.995527$	$N^*_{0.001} = 0.995341$

Table 7: Theoretical UACI critical values for different image size.

Size	Theoretical UACI critical values		
	$\alpha = 0.05$	$\alpha = 0.01$	$\alpha = 0.001$
512×512	$u^{*-}_{0.05} = 0.333730$ $u^{*+}_{0.05} = 0.335541$	$u^{*-}_{0.01} = 0.333445$ $u^{*+}_{0.01} = 0.335826$	$u^{*-}_{0.001} = 0.333115$ $u^{*+}_{0.001} = 0.336156$
256×256	$u^{*-}_{0.05} = 0.332824$ $u^{*+}_{0.05} = 0.336447$	$u^{*-}_{0.01} = 0.332255$ $u^{*+}_{0.01} = 0.337016$	$u^{*-}_{0.001} = 0.331594$ $u^{*+}_{0.001} = 0.337677$

Table 8: The NPCR and UACI values of the encrypted image.

Image	Channel	Chang bit	NPCR	UACI
Lena	R	First pixel	0.9960	0.3347
		Last pixel	0.9960	0.3341
	G	First pixel	0.9959	0.3342
		Last pixel	0.9961	0.3351
	B	First pixel	0.9961	0.3347
		Last pixel	0.9960	0.3347
Chocolate	R	First pixel	0.9962	0.3347
		Last pixel	0.9959	0.3348
	G	First pixel	0.9961	0.3346
		Last pixel	0.9959	0.3346
	B	First pixel	0.9959	0.3343
		Last pixel	0.9962	0.3342

where P_1 and P_2 are two encrypted images, $\mathrm{D}(i, j) = |P_1(a, b) - P_2(a, b)|$, and

$$\mathrm{Sign}(\mathrm{D}(a, b)) = \begin{cases} 1, & P_1(a, b) = P_2(a, b), \\ 0, & \text{else.} \end{cases} \tag{19}$$

According to the method in [29], the theoretical NPCR critical values for different sizes with respect to the significance levels $\alpha = 0.05$, $\alpha = 0.01$, and $\alpha = 0.001$ are shown in Table 6; $N^*_{0.05}$, $N^*_{0.01}$, and $N^*_{0.001}$ are the critical values of NPCR to reject the null hypothesis regarding the associated α-level of significance. If the NPCR test values are above N^*_α, and they are random-like with the significance level α. As for theoretical UACI critical values listed in Table 7, when the UACI test values for the encrypted image lie in the interval $[u^{*-}_\alpha, u^{*+}_\alpha]$, the encrypted image passes the UACI test successfully.

We generate the cipher images by modifying the first pixel and last pixel of the same plain image. The resultant NPCR and UACI values are listed in Table 8. It is clear from this table that all the NPCR and UACI values meet the criteria for accepting the null hypothesis with respect to the significance levels (i.e., $\alpha = 0.05$, $\alpha = 0.01$, and $\alpha = 0.001$). In other words, the encrypted images pass the NPCR and UACI tests successfully, and our scheme is resistant to differential attacks.

Table 9: The differences of the encrypted image with Case 1 and Case 2.

Image	Channel	Case 1-Case 2
Lena	R	99.6166%
	G	99.6143%
	B	99.6253%
Chocolate	R	99.6170%
	G	99.5910%
	B	99.6200%

6.5. Key Security Analysis

6.5.1. Key Space Analysis. The larger key space indicates a better security of the encryption algorithm. As for today's computation power, the key space over 2^{128} is secured and infeasible, which can resist the brute-force attacks effectively. In our scheme, the keys are the initial values of 64 nodes of the 2D CML model. It is well known that the floating-point arithmetic defined by IEEE 754 has a precision of 10^{-15}. Therefore, each node has the 10^{15} possibilities; the key space of all 64 nodes is then

$$10^{15} \times \cdots \times 10^{15} = 10^{960}. \tag{20}$$

Clearly, 10^{960} is much larger than 2^{128}. Thus, the key space of our scheme is large enough to resist the brute-force attacks.

6.5.2. Key Sensitivity Analysis. Key sensitivity means a tiny change of the secret key causing huge changes of the encrypted results. To verify the key sensitivity of our scheme, we use two proximal secret keys as Case 1 and Case 2 to test our design:

Case 1: Keep the original initial conditions unchanged

Case 2: The initial condition of one node is changed by a magnitude of 0.00001 and all others remain unchanged

We then list the differences of the two cipher images in Table 9. From this table, the rate of different pixels between two cipher images is larger than 99.59%. It indicates that the proposed scheme possesses good key sensitivity.

Table 10: The correlation coefficient results of our scheme and others.

Image	Original image			Encrypted image		
	H	V	D	H	V	D
Lena in ours	0.8946	0.9247	0.8636	−0.0061	0.0042	−0.0007
Lena in [30]	0.8946	0.9247	0.8636	0.0016	0.0002	0.0038
Lena in [31]	0.8946	0.9247	0.8636	0.0003	0.0040	0.0013
Lena in [32]	0.8946	0.9247	0.8636	0.0013	0.0034	0.0072
Lena in [33]	0.8946	0.9247	0.8636	−0.0031	0.0025	−0.0001
Lena in [34]	0.8946	0.9247	0.8636	0.0046	−0.0028	0.0014
Lena in [35]	0.8946	0.9247	0.8636	0.0005	−0.0070	0.0006
Lena in [36]	0.8946	0.9247	0.8636	−0.0047	0.0028	−0.0043
Lena in [37]	0.9902	0.9908	0.9794	0.0013	0.0047	0.0020

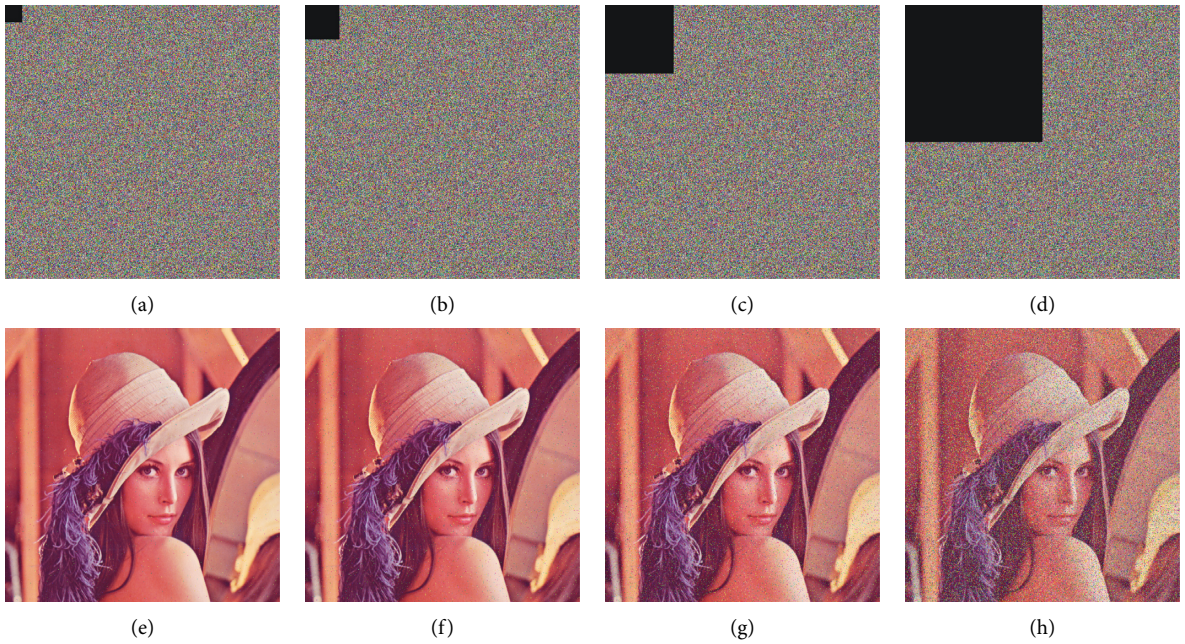

Figure 15: Occlusion attack analysis results of the cipher Lena image. ((a)–(d)) The cipher Lena image with 1/256, 1/64, 1/16, and 1/4 occlusion; ((e)–(h)) decryption results for the images above.

6.6. Comparison Analysis. To further assess the performance of the proposed scheme, quite a few recent studies [30–38] in the same literature are included for comparison. The comparison results of correlation coefficient, NPCR, UACI, and information entropy are listed in Tables 10–12.

Table 10 shows the correlation coefficient values; we can obverse that the correlation coefficient values are quite smaller, almost equal to 0. Meanwhile, Table 11 presents the NPCR and UACI values of our scheme and other schemes; the values of our scheme are closer to the ideal values (NPCR = 0.996094 and UACI = 0.334636) than those of the schemes in [32, 33, 35–37]. Finally, Table 12 describes the information entropy results of our scheme and other schemes; the information entropy results of the R, G, and B channel in our scheme are 7.9992, 7.9999, and 7.9992, respectively, and the average value is 7.999433, which means that they are almost near the ideal value of 8.0. In conclusion, the proposed method performs at least similar to, if not always better than, the others.

6.7. Resistance to Occlusion Attacks. When transmitting the encrypted images, network congestion or malicious destruction may lead to data loss. Occlusion attack is commonly unitized to measure the capacity of recovering the original image from the encrypted image with data loss.

Figures 15(a)–15(d) and Figures 16(a)–16(d) show different encrypted versions of the Lena and Chocolate images with 1/256, 1/64, 1/16, and 1/4 occlusion, respectively, and Figures 15(e)–15(h) and Figures 16(e)–16(h) show the corresponding recovered images of the different occluded cipher images. It is clear that the recovered images are still recognizable even when 25% of the encrypted data are lost.

6.8. Runtime Analysis. The runtime of an encryption scheme is an important factor in practical applications. We implement our scheme with C language on a personal computer equipped with Intel(R) Core(TM) i7-10710U CPU @ 1.10 GHz, 1.61 GHz. The runtimes of our scheme and the literature schemes are given in Table 13. As can be

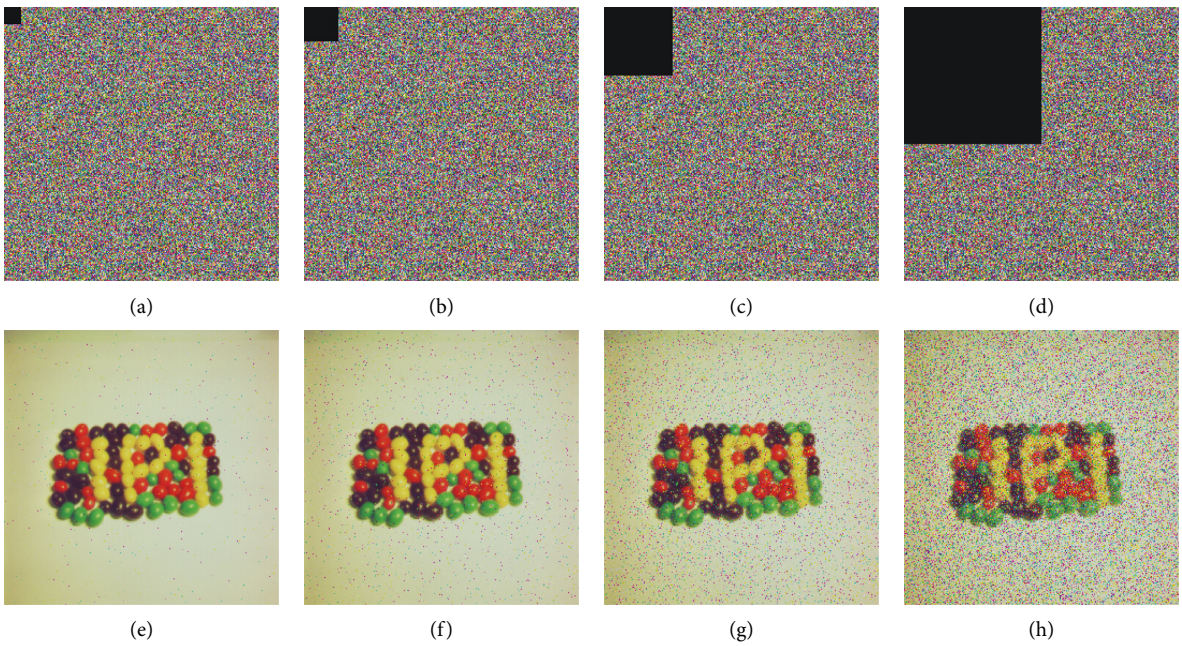

Figure 16: Occlusion attack analysis results of the cipher Chocolate image. ((a)–(d)) The cipher Chocolate image with 1/256, 1/64, 1/16, and 1/4 occlusion; ((e)–(h)) decryption results for the images above.

Table 11: The NPCR and UACI results of our scheme and others.

Image	NPCR				UACI			
	R	G	B	Average	R	G	B	Average
Lena in ours	0.9960	0.9959	0.9961	0.996000	0.3347	0.3342	0.3346	0.334500
Lena in [30]	0.9961	0.9963	0.9961	0.996167	0.3347	0.3345	0.3348	0.334667
Lena in [31]	0.9961	0.9961	0.9961	0.996100	0.3346	0.3346	0.3347	0.334633
Lena in [32]	0.9969	0.9969	0.9969	0.996900	0.3333	0.3333	0.3333	0.333300
Lena in [33]	0.9967	0.9969	0.9969	0.996833	0.3352	0.3353	0.3354	0.335300
Lena in [34]	0.9961	0.9961	0.9961	0.996100	0.3349	0.3349	0.3347	0.334833
Lena in [35]	0.9973	0.9968	0.9970	0.997033	0.3346	0.3345	0.3346	0.334567
Lena in [36]	0.9967	0.9964	0.9965	0.996533	0.3351	0.3350	0.3349	0.335000
Lena in [37]	0.9964	0.9965	0.9964	0.996433	0.3343	0.3347	0.3348	0.334600
Lena in [38]	0.9962	0.9961	0.9962	0.996167	0.3342	0.3343	0.3346	0.334367

Table 12: The information entropy results of our scheme and others.

Image	Encrypted image			Average
	R	G	B	
Lena in ours	7.9992	7.9999	7.9992	7.999433
Lena in [30]	7.9985	7.9985	7.9986	7.998533
Lena in [31]	7.9994	7.9994	7.9993	7.999366
Lena in [32]	7.9997	7.9997	7.9996	7.999666
Lena in [33]	7.9976	7.9972	7.9972	7.997333
Lena in [34]	7.9994	7.9993	7.9992	7.999300
Lena in [35]	7.9972	7.9973	7.9971	7.997200
Lena in [36]	7.9973	7.9965	7.9969	7.996900
Lena in [37]	7.9994	7.9993	7.9994	7.999366
Lena in [38]	7.9917	7.9912	7.9917	7.991533

seen from the table, the encryption times of the Lena and Chocolate images in our scheme for the R channel are 0.369s and 0.097s, respectively, which indicates that it is more efficient than the schemes in [39–44] but inferior to the scheme in [39]. This is because the scheme in [39] has a paralleled architecture and we take the task of designing a paralleled implementation of our design as the future work.

Table 13: Encryption runtime of our scheme and others.

Image	Encrypted Lena image Time (s)	Encrypted Chocolate image Time (s)
Ours	0.369	0.097
[39]	0.079	0.020
[40]	1.260	0.460
[41]	2.290	0.710
[42]	1.590	0.350
[43]	15.140	4.540
[44]	11.420	3.480

7. Conclusion

In this paper, according to theoretical analyses in LE and synchronization stability of the 2D CML model and also the simulation analyses in bifurcation, ergodicity, and PDD, we thoroughly demonstrate that the 2D CML model has good chaotic properties. Moreover, binary sequences can be directly and effectively generated by the 2D CML model, and passing the NIST test suite confirms that the generated sequences possess desired properties for encryption. Relying on this observation, we put forward an image encryption algorithm through confusion and diffusion. Further simulation analyses show that the proposed image encryption scheme possesses good encryption characteristics.

For future work, the study of the characteristics of the higher-dimensional CML system and its applications will be considered.

Data Availability

All data used during the study appear in the submitted article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work described in this paper was supported by Grants from the National Natural Science Foundation of China (no. 61572089), the Science and Technology Foundation Project of Guizhou Province (QianKeHeJiChu[2020]1Y422, QianKeHeJiChu-ZK[2022]YiBan329, QianKeHeJiChu [2019]1425, and QianKeHeJiChu-ZK[2022]YiBan331), the key project research achievements of Guizhou Education University in 2020 (2020ZD006, 2020ZD008), and Guizhou Education Department Youth Science and Technology Talent Growth Project (QianJiaoHe-KY-Zi[2021]239).

References

[1] M. A. Midoun, X. Wang, and M. Z. Talhaoui, "A sensitive dynamic mutual encryption system based on a new 1D chaotic map," *Optics and Lasers in Engineering*, vol. 139, Article ID 106485, 2021.

[2] C. E. C. Souza, D. P. B. Chaves, and C. Pimentel, "One-dimensional pseudo-chaotic sequences based on the discrete arnold's cat map over $\mathbb{Z}_3m$," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 1, pp. 491–495, 2021.

[3] S. Kumari and R. Chugh, "A novel four-step feedback procedure for rapid control of chaotic behavior of the logistic map and unstable traffic on the road," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 30, no. 12, Article ID 123115, 2020.

[4] R. A. Elmanfaloty and E. Abou-Bakr, "An image encryption scheme using a 1D chaotic double section skew tent map," *Complexity*, vol. 2020, Article ID 7647421, 18 pages, 2020.

[5] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, Article ID 107563, 2020.

[6] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, "Privacy preserving high-order Bi-lanczos in cloud-fog computing for industrial applications," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[7] G. Ye, C. Pan, Y. Dong, K. Jiao, and X. Huang, "A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, 2021.

[8] Z. Liu, Y. Wang, Y. Zhao, and L. Y. Zhang, "A stream cipher algorithm based on 2D coupled map lattice and partitioned cellular automata," *Nonlinear Dynamics*, vol. 101, no. 2, pp. 1383–1396, 2020.

[9] J. S. Teh, M. Alawida, and J. J. Ho, "Unkeyed hash function based on chaotic sponge construction and fixed-point arithmetic," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 713–729, 2020.

[10] A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," *Information Sciences*, vol. 550, pp. 252–267, 2021.

[11] R. Logeshwari and L. Rama Parvathy, "Generating logistic chaotic sequence using geometric pattern to decompose and recombine the pixel values," *Multimedia Tools and Applications*, vol. 79, no. 31-32, Article ID 22375, 2020.

[12] L. Wang and H. Cheng, "Pseudo-random number generator based on logistic chaotic system," *Entropy*, vol. 21, no. 10, p. 960, 2019.

[13] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[14] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.

[15] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[16] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Information Sciences*, vol. 520, pp. 46–62, 2020.

[17] S. Xiao, Z. Yu, and Y. Deng, "Design and analysis of a novel chaos-based image encryption algorithm via switch control mechanism," *Security and Communication Networks*, vol. 2020, Article ID 7913061, 12 pages, 2020.

[18] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, Article ID 8824915, 18 pages, 2021.

[19] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, Article ID 25911, 2021.

[20] S. Mobayen, C. Volos, Ü. Çavuşoğlu, and S. Kaçar, "A simple chaotic flow with hyperbolic sinusoidal function and its application to voice encryption," *Symmetry*, vol. 12, no. 2047, pp. 2047–2118, 2020.

[21] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems," *IEEE Access*, vol. 9, Article ID 21332, 2021.

[22] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, 2018.

[23] Y. Wang, Z. Liu, L. Y. Zhang, F. Pareschi, G. Setti, and G. Chen, "From chaos to pseudorandomness: a case study on the 2-D coupled map lattice," *IEEE Transactions on Cybernetics*, pp. 1–11, 2021.

[24] K. Kaneko, "Pattern dynamics in spatiotemporal chaos: pattern selection, diffusion of defect and pattern competition intermittency," *Physica D: Nonlinear Phenomena*, vol. 34, no. 1-2, 1989.

[25] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.

[26] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[27] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[28] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics & Laser Technology*, vol. 114, pp. 224–239, 2019.

[29] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[30] Z. Liu, Y. Wang, and L. Y. Zhang, "A novel compressive image encryption with an improved 2D coupled map lattice model," *Security and Communication Networks*, vol. 6, pp. 1–21, 2021.

[31] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, p. 535, 2018.

[32] X.-J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu, and J. Ma, "A fast encryption algorithm of color image based on four-dimensional chaotic system," *Journal of Visual Communication and Image Representation*, vol. 33, pp. 219–234, 2015.

[33] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607–629, 2017.

[34] S. Cai, L. Huang, X. Chen, and X. Xiong, "A symmetric plaintext-related color image encryption system based on bit permutation," *Entropy*, vol. 20, no. 4, p. 282, 2018.

[35] X. Wu, B. Zhu, and Y. Hu, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[36] A. U. Rehman and X. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2, DNA and SHA-2," *Multimedia Tools and Applications*, vol. 78, no. 2, pp. 2105–2133, 2019.

[37] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

[38] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Optics and Lasers in Engineering*, vol. 128, no. 3, Article ID 106040, 2020.

[39] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, Article ID 103056, 2021.

[40] X. Chai, Z. Gan, and M. Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," *Multimedia Tools and Applications*, vol. 76, no. 14, Article ID 15561, 2017.

[41] Z. Eslami and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," *Optics Communications*, vol. 286, pp. 51–55, 2013.

[42] X. Huang, "Image encryption algorithm using chaotic Chebyshev generator," *Nonlinear Dynamics*, vol. 67, no. 4, pp. 2411–2417, 2012.

[43] X. Wang and D. Xu, "A novel image encryption scheme based on Brownian motion and PWLCM chaotic system," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 345–353, 2014.

[44] Y. Zhou, W. Cao, and C. L. Philip Chen, "Image encryption using binary bitplane," *Signal Processing*, vol. 100, pp. 197–207, 2014.