


Research Article

A Color Image Encryption Scheme Based on a Novel 3D Chaotic Mapping

Chunyuan Liu^{1,2} and Qun Ding¹ 

¹Electronic Engineering College, Heilongjiang University, Harbin 150080, China

²Computer and Information Engineering College, Heilongjiang University of Science and Technology, Harbin 150027, China

Correspondence should be addressed to Qun Ding; qunding@aliyun.com

Received 17 May 2020; Revised 16 October 2020; Accepted 7 December 2020; Published 23 December 2020

Academic Editor: Cornelio Posadas-Castillo

Copyright © 2020 Chunyuan Liu and Qun Ding. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Low-dimensional chaotic mappings are simple functions that have low computation cost and are easy to realize, but applying them in a cryptographic algorithm will lead to security vulnerabilities. To overcome this shortcoming, this paper proposes the coupled chaotic system, which coupled the piecewise and Henon mapping. Simulation results indicate that the novel mapping has better complexity and initial sensitivity and larger key space compared with the original mapping. Then, a new color image encryption algorithm is proposed based on the new chaotic mapping. The algorithm has two processes: diffusion and confusion. In this scheme, the key is more than 2^{216} , and SSIM and PSNR are 0.009675 and 8.6767, respectively. The secret key is applied in the shuffling and diffusion. Security analysis indicates that the proposed scheme can resist cryptanalytic attacks. It has superior performance and has high security.

1. Introduction

Chaos has always been a very active research topic in the field of nonlinear science. There are many common characteristics of digital chaotic system and cryptography, such as sensitivity and being aperiodic and pseudorandom. These characteristics promote the application of digital chaotic system in cryptographic algorithm design. Image encryption is one of the main means of information protection. An image will have some characteristics such as high correlation, large data size, and high data dimension, which should be considered additional, when it is encrypted. Because of the low efficiency of real-time processing, traditional encryption algorithms are not suitable for digital images such as DES, 3DES, and AES [1]. Therefore, many image encryption schemes based on different fields have been proposed in recent years such as cellular automata [2, 3], wavelet transform [4, 5], compressing sensing [6], selective encryption [7], DNA coding [8, 9], and chaos [10–14].

Because of the large key space, strong dynamic characteristics, complex attractor, and strong ergodicity of high-

dimensional chaotic system, it is more secure than low dimension. The high computational cost of high-dimensional chaotic system makes it occupy more hardware and software resources, which is difficult to implement. By contrast, the low-dimensional chaotic system is a simple function, which is easier to implement. Due to the computation precision of software and hardware, the chaotic complexity in real-numbered chaos is often affected by dynamic degradation (collapsing effect) [14, 15]. With the study going on, low-dimensional chaotic maps have been performed perfectly on its characteristics [16, 17]. In particular, some algorithms based on low-dimensional chaotic maps have been widely studied and cracked [18–20]. Therefore, when a low-dimensional chaotic mapping is applied in cryptography, it is necessary to enhance all of its chaotic characteristics.

Aiming at the degradation of digital chaotic property caused by innate structural defects, many algorithms such as [21, 22], pseudorandom perturbation [23], switching systems [24, 25], and combination systems based on modular operation [26–29] have been proposed to overcome this.

However, due to the uncertain parameters, it still includes partial periodic regions which do not maintain long stable synchronization. Each of the existing approaches has its own limitations and drawbacks [30].

Many image encryption algorithms have been proposed based on Shannon's theory about shuffling and diffusion [5, 12, 31, 32]. Shuffling can rearrange pixels by some rules [33] and diffusion can substitute pixels by a series generated by a chaotic map. The inherent features of a chaotic map can be suitable for the two security notions.

Generally, most of algorithms come with the common limitations. Firstly, the key is independent of the original image; that is, if the key is unchanged, the different original images that need to be encrypted will use the same key [34–36]. Secondly, the encryption scheme based on low-dimensional chaotic maps is not suitable for practical use because of its small key space, short period, and low complexity [14–17]. At last, the ciphertext is only related to the key and has no relationship with the plaintext and middle ciphertext, which cannot resist the plaintext attack and the ciphertext attack.

In this paper, we propose a novel color image encryption algorithm based on an efficient chaotic system coupling two low-dimensional chaotic maps. Firstly, the new chaotic system utilizes combination method to formulate a 3D chaotic map. It not only retains the complexity of its underlying maps but also enlarges the dimensions from 2D to 3D. Also, it enlarges the key space. Thus, the chaotic map can depict highly chaotic behavior for all parameters. Secondly, the initial key is derived from plaintext, and different images have different initial key, which improves the security of the algorithm. Finally, the formula of this algorithm is related not only to the key and plaintext but also to the intermediate ciphertext, which increases the complexity among plaintext, ciphertext, and key.

The other sections of this paper are organized as follows: Section 2 represents the proposed chaotic system and introduces the new 3D chaotic map and then proves its chaotic properties. In Section 3, a detailed explanation of the proposed encryption algorithm is provided. Some analysis of its security and performance is carried out in Section 4 and the conclusion is given in Section 5.

2. 3D Piecewise-Henon Map

With the continuous improvement of computing speed and performance of modern computers, nonlinear systems have developed greatly. However, because of the computational accuracy of computer software and hardware limiting, the complexity of chaotic mapping in real number field will gradually decline. In addition, the orbit of the low-dimensional chaotic map will degenerate (collapse effect) in some periods. Therefore, low-dimensional chaotic systems are rarely used alone [37, 38]. In particular, Henon and logistic mappings are quite different in theory when they are used alone [39, 40]. Therefore, we combine the characteristics of Henon mapping and the piecewise mapping to construct a new chaotic mapping with larger dimension and better

chaotic characteristics, 3D piecewise-Henon mapping (3D-PHM).

3D-PHM is as follows:

$$T(x_n, y_n, z_n) = \begin{cases} x_{n+1} = \psi_{c_1}(x_n) + \Lambda_{c_2}(y_n, z_n) \bmod 1, \\ y_{n+1} = \psi_{c_1}(y_n) + \Lambda_{c_2}(z_n, x_n) \bmod 1, \\ z_{n+1} = \psi_{c_1}(z_n) + \Lambda_{c_2}(x_n, y_n) \bmod 1, \end{cases} \quad (1)$$

where c_1 and c_2 are real control parameters; $\psi_{c_1}(x)$ is a piecewise function; that is,

$$\begin{aligned} \psi_{c_1}(x) &= |1 - c_1 x|, \\ \Lambda_{c_2}(x, y) &= y + 1 - c_2 x^2, \end{aligned} \quad (2)$$

is the Henon mapping.

The initial values x_0 , y_0 , and z_0 are selected in the interval $[0, 1]$. From 3D-PHM, three state values are obtained by each integer k , which are denoted as x_k , y_k , and z_k . The range of the value is confined in $[0, 1]^3$. Because of its good simplicity, ergodicity, and sensitivity to initial conditions, the system has good cryptographic performance.

2.1. Graphical Analysis. The control parameters c_1 and c_2 in 3D-PHM are very important. We drew a contour map of the approximate entropy of the system with different values, which is shown in Figure 1; c_1 and c_2 are varied from 0 to 15, and the step = 0.01. In Figure 1(a), the complexity of the system is good in most of the regions, and, with the increase of parameters c_1 and c_2 , the approximate entropy is high, except for some regions (Figure 1(b) is the enlargement of part (a); the low value position can be seen). Therefore, when studying the characteristics of 3D-PHM, we will set the control parameters of the system (formula (1)) as $c_1 = c_2 = c$.

Lyapunov exponent is an important parameter of chaotic systems. When one of Lyapunov exponents is positive, the system will be a chaotic system. Provided that there are two or more positive Lyapunov exponents, the system is a hyperchaotic system. Eigenvalue method is used to calculate Lyapunov exponent of 3D-PHM, which is (0.3055, 0.3158, 0.1529), when $(x_0, y_0, z_0) = (0.1, 0.2, 0.3)$, and $c_1 = c_2 = c = 15$. The Jacobian of equation (1) is as follows:

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_n} & \frac{\partial f_1}{\partial y_n} & \frac{\partial f_1}{\partial z_n} \\ \frac{\partial f_2}{\partial x_n} & \frac{\partial f_2}{\partial y_n} & \frac{\partial f_2}{\partial z_n} \\ \frac{\partial f_3}{\partial x_n} & \frac{\partial f_3}{\partial y_n} & \frac{\partial f_3}{\partial z_n} \end{bmatrix}. \quad (3)$$

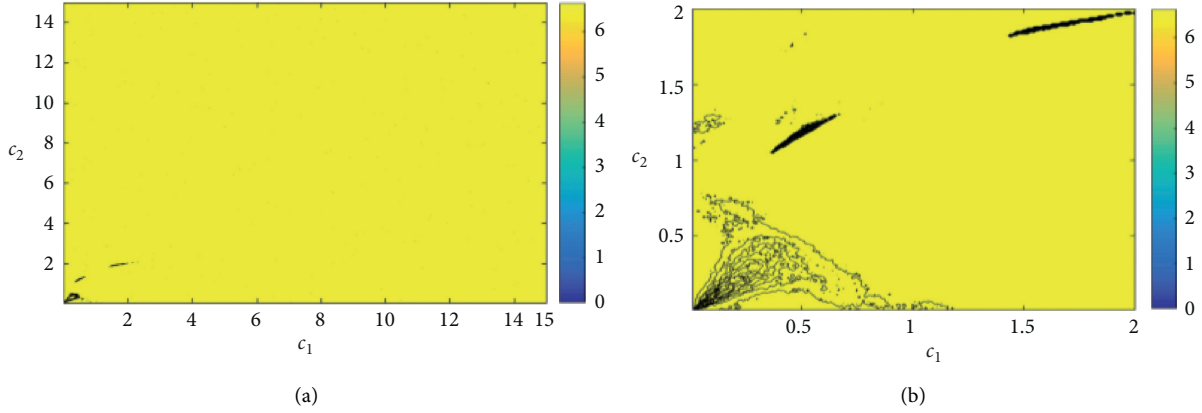


FIGURE 1: The approximate entropy of the control parameters of c_1 and c_2 . (a) $(c_1, c_2) \in [0, 15] \times [0, 15]$; (b) an enlargement of (a).

The initial point is (x_0, y_0, z_0) , and the other iteration points obtained from the iterative equation are $(x_0, y_0, z_0), (x_1, y_1, z_1), \dots, (x_n, y_n, z_n)$, respectively. The first $(n-1)$ Jacobian matrices are $J_0 = J(x_0, y_0, z_0)$,

$J_1 = J(x_1, y_1, z_1)$, and $J_{n-1} = J(x_{n-1}, y_{n-1}, z_{n-1})$, respectively. When the increment is small enough, its evolution satisfies the linear differential equation:

$$\begin{bmatrix} \partial x_n \\ \partial y_n \\ \partial z_n \end{bmatrix} = J_{n-1} \begin{bmatrix} \partial x_{n-1} \\ \partial y_{n-1} \\ \partial z_{n-1} \end{bmatrix} = J_{n-1} J_{n-2} \begin{bmatrix} \partial x_{n-2} \\ \partial y_{n-2} \\ \partial z_{n-2} \end{bmatrix} = \dots = J_{n-1} J_{n-2} \dots J_0 \begin{bmatrix} \partial x_0 \\ \partial y_0 \\ \partial z_0 \end{bmatrix}, \quad (4)$$

where $J = J_{n-1} J_{n-2} \dots J_0$. Let the three eigenvalues of matrix J be $\lambda_1, \lambda_2, \lambda_3$, respectively.

$$\begin{cases} \text{LE}_1 = \frac{1}{n} \ln |\lambda_1|, \\ \text{LE}_2 = \frac{1}{n} \ln |\lambda_2|, \\ \text{LE}_3 = \frac{1}{n} \ln |\lambda_3|. \end{cases} \quad (5)$$

Figure 2 shows the chaotic attractor of A , which has no obvious uneven distribution in the region. It has a very good ergodicity when $c = 15$.

2.2. Comparative Analysis of Permutation Entropy of Henon, 3D-Henon, and 3D-PHM Maps. The complexity of a chaotic system indicates the uncertainty of a mapping, which can be measured by entropy. For a symbol sequence, the higher its entropy is, the higher its complexity is; otherwise, the lower its complexity is.

Permutation entropy (PE) is the algorithm of complexity for measuring time series, which was proposed by Christoph Bandt and Pompe in 2002. The permutation entropy is defined as follows [34]:

$$H(e) = - \sum_{i=1}^k P_k \ln P_k, \quad (6)$$

where e is the embedded dimension of the reconstructed sequence and P_k is the probability of the occurrence of each symbol. In theory, when $P_k = 1/e!$, $H(e)$ reaches the maximum $\ln(e!)$, but, in practice, $H(e) \leq \ln(N - e + 1)$. In general, $H(e)$ will be standardized by $\ln(N - e + 1)$; that is,

$$0 \leq h(e) = \frac{H(e)}{\ln(N - e + 1)} \leq 1. \quad (7)$$

Obviously, the complexity of the series can be reflected by $h(e)$. The smaller $h(e)$ is, the stronger regularity of the chaotic series is. On the contrary, the larger $h(e)$ is, the higher complexity of the chaotic sequence is and the greater the complexity of the chaotic sequence is. The comparisons of PE among Henon mapping, 3D-Henon, and 3D-PHM are shown in Figure 3. As is shown, PE of 3D-PHM is higher than those of 3D-Henon mapping and Henon mapping. Henon mapping is the least complex. PE of 3D-PHM is significantly higher than that of Henon mapping. That means the complexity of Henon mapping is increased significantly.

2.3. Sensitive to Initial Conditions. The initial condition sensitiveness is another important characteristic of chaotic systems. Figure 4 illustrates the sensitivity of 3D-PHM to small changes in initial conditions. For two very close initial values (x_0, y_0, z_0) and $(\tilde{x}_0, \tilde{y}_0, \tilde{z}_0) = (x_0 + \delta, y_0 + \delta, z_0 + \delta)$, where $\delta \approx 10^{-16}$, 3D-PHM can produce two completely different sequences and the gaps between their trajectories

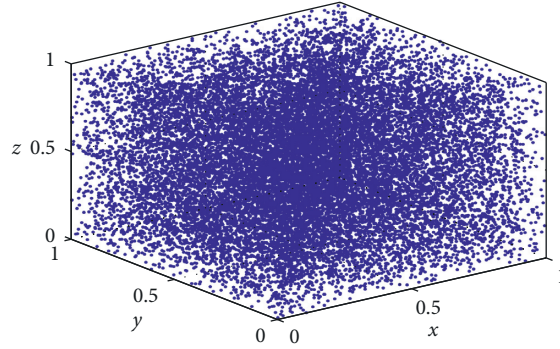
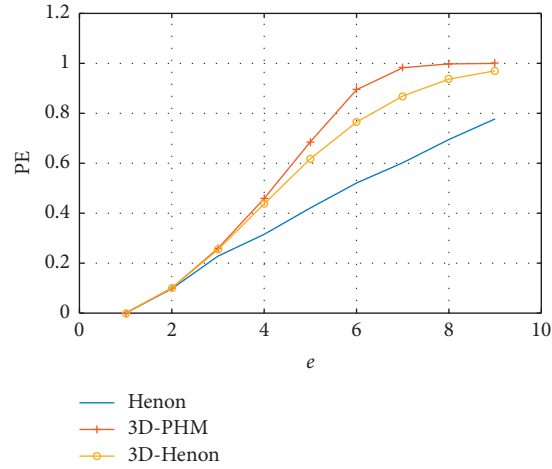


FIGURE 2: The chaotic attractor of 3D-PHM.

FIGURE 3: The comparison of PE between Henon mapping, 3D-PHM, and 3D-Henon mapping (e is the embedded dimension).

$\{(x_n, y_n, z_n)\}_{n=0,1,\dots}$ and $\{(\tilde{x}_n, \tilde{y}_n, \tilde{z}_n)\}_{n=0,1,2,\dots}$ increase considerably.

2.4. The NIST Statistical Test. For all 15 tests in the NIST suite, the significance level was set to 1%. If P -value > 0.01 , the binary sequence is accepted to be random with a confidence of 99%; otherwise, it is considered as nonrandom. To perform this battery of tests, we have generated up to 10^6 points $\{(x_i, y_i, z_i); i > n_t\}$ by 3D-PHM. We convert these sequences into binary form and NIST tests were performed on them. The test results are shown in Table 1 and all the tests were successful. It is shown that 3D-PHM has a strong

randomness and can resist many statistical attacks. Hence, the tested binary sequences generated by 3D-PLM are random with respect to all the 15 tests of NIST suite.

2.5. Approximate Probability Density. Probability distribution function is a tool to measure whether a dynamic system is a uniform distribution [41]. In order to measure the probability density of the system, we divide the three-dimensional attractor A into a group of small cubes in $B = [0, 1]^3$, and the number of cubes is n^3 , which is defined by

$$\begin{aligned}
 r_i &= \frac{i}{n}, g_j = \frac{j}{n}, b_k = \frac{k}{n}, \quad i, j, k = 0, 1, \dots, n-1, \\
 B_{i,j,k} &= [r_i, r_{i+1}] \times [g_j, g_{j+1}] \times [b_k, b_{k+1}], \quad i, j, k = 0, 1, \dots, n-2, \\
 B_{n-1,j,k} &= [r_{n-1}, 1] \times [g_j, g_{j+1}] \times [b_k, b_{k+1}], \quad i, j, k = 0, 1, \dots, n-2, \\
 B_{i,n-1,k} &= [r_i, r_{i+1}] \times [g_{n-1}, 1] \times [b_k, b_{k+1}], \quad i, j, k = 0, 1, \dots, n-2, \text{ and} \\
 B_{i,j,n-1} &= [r_i, r_{i+1}] \times [g_j, g_{j+1}] \times [b_{n-1}, 1], \quad i, j, k = 0, 1, \dots, n-2.
 \end{aligned} \tag{8}$$

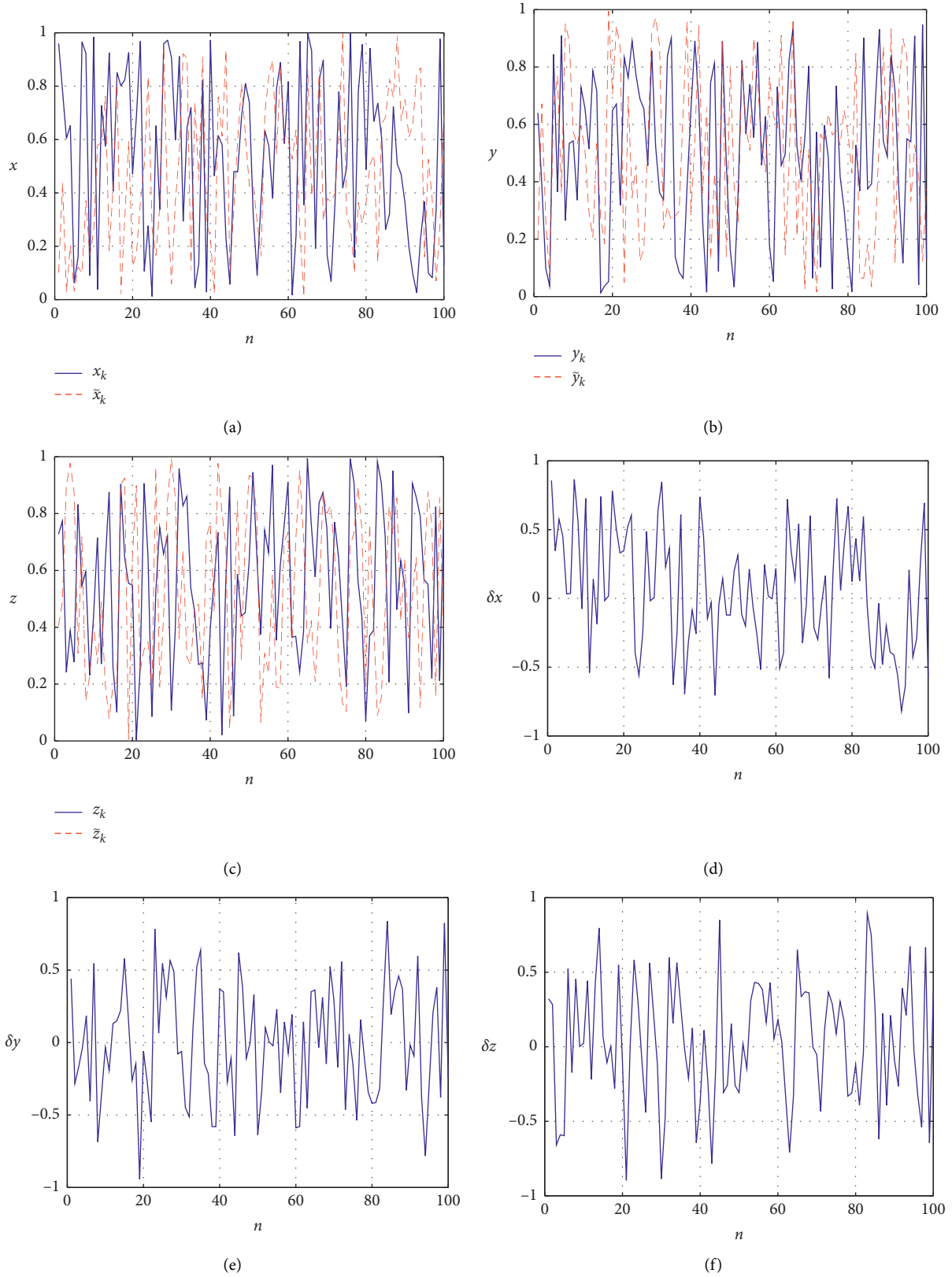


FIGURE 4: Initial value sensitivity for 100 iterations when $c = 15$, $(x_0, y_0, z_0) = (0.103, 0.241, 0.318)$, $(\tilde{x}_0, \tilde{y}_0, \tilde{z}_0) = (x_0 + \delta, y_0 + \delta, z_0 + \delta)$, and $\delta \approx 10^{-16}$. (a) Plot of $\{x_n\}_{n=0}^{n=100}$ and $\{\tilde{x}_n\}_{n=0}^{n=100}$ versus n ; (b) plot of $\{y_n\}_{n=0}^{n=100}$ and $\{\tilde{y}_n\}_{n=0}^{n=100}$ versus n ; (c) plot of $\{z_n\}_{n=0}^{n=100}$ and $\{\tilde{z}_n\}_{n=0}^{n=100}$ versus n ; (d) plot of $\{x_n - \tilde{x}_n\}_{n=0}^{n=100}$ versus n ; (e) plot of $\{y_n - \tilde{y}_n\}_{n=0}^{n=100}$ versus n ; (f) plot of $\{z_n - \tilde{z}_n\}_{n=0}^{n=100}$ versus n .

TABLE 1: The NIST test results of each component generated by 3D-PHM.

No.	Test name	P value			Result
		x	y	z	
1	Frequency	0.554320	0.326810	0.458760	Success
2	Block frequency	0.834570	0.577802	0.435602	Success
3	Runs	0.547600	0.197506	0.231586	Success
4	Longest run	0.801265	0.792351	0.786422	Success
5	Rank	0.972745	0.267811	0.336589	Success
6	FFT	0.035687	0.948721	0.456874	Success
7	Nonoverlapping template	0.235874	0.478512	0.587456	Success
8	Overlapping template	0.497832	0.089451	0.785421	Success
9	Universal	0.935647	0.058974	0.057894	Success
10	Linear complexity	0.798145	0.278945	0.924578	Success
11	Serial	0.754612	0.845971	0.348755	Success
12	Approximate entropy	0.616784	0.089451	0.365874	Success
13	Cumulative sums	0.168745	0.944513	0.638745	Success
14	Random excursions	0.654123	0.087945	0.654716	Success
15	Random excursions variant	0.565209	0.058799	0.565209	Success

Let n_t be the number of iterations in transition regime, large enough, and after $n_t + \hat{n}$ iterations of 3D-PHM, the proportion of the box $\{B_{i,j,k}\}_{0 \leq i,j,k \leq n-1}$ reached by the orbit $C_{\hat{n}}(x_0, y_0, z_0) = \{T^{n_t+i}(x_0, y_0, z_0); i = 1, \dots, \hat{n}\}$ is calculated by

$$\%P_{\hat{n}} = \left[\frac{1}{n^3} \sum_{0 \leq i,j,k \leq n-1} \chi_{B_{i,j,k}}(C_{\hat{n}}(x_0, y_0, z_0)) \right] \times 100\%, \quad (9)$$

where χ_E is a special function about the set E' which is defined as follows:

$$\chi_E(E') = \begin{cases} 1, & \text{if } E \cap E' \neq \emptyset, \\ 0, & \text{if } E \cap E' = \emptyset. \end{cases} \quad (10)$$

In addition, in order to get the number of times the trajectory $C_{\hat{n}}(x_0, y_0, z_0)$ passes through a particular cube $B_{i,j,k}$, we need to calculate the relative times of trajectory $C_{\hat{n}}(x_0, y_0, z_0)$ accessing this box relative to \hat{n} . Given that \hat{n} is large enough, the approximate probability density function $P_{\hat{n}}(x, y, z) = P_{\hat{n}}(B_{i,j,k})$ under all conditions $0 \leq i, j, k \leq n-1$ and all $(x, y, z) \in B_{i,j,k}$ and then

$$P_{\hat{n}}(B_{i,j,k}) = \frac{1}{\hat{n}} \sum_{s=1}^{\hat{n}} \chi_{B_{i,j,k}}(T^{n_t+s}(x_0, y_0, z_0)). \quad (11)$$

In order to define the 3D-PHM system to random, it will be further required that the variables defined above and the invariant measure mathematicians called must be independent of the starting point (x_0, y_0, z_0) . Moreover, when the track $C_{\hat{n}}(x_0, y_0, z_0)$ is evenly distributed throughout the space, in that way, for all $0 \leq i, j, k \leq n-1$, the following formula holds right:

$$\mu(B_{i,j,k}) = \lim_{\hat{n} \rightarrow \infty} P_{\hat{n}}(B_{i,j,k}) = \frac{1}{n^3}, \quad (12)$$

where $\mu(B_{i,j,k})$ represents the natural Lebesgue metric of $B_{i,j,k}$ [42].

For computing the approximate density function of 3D-PHM, cube B is divided into $n^3 = 100^3$ boxes. When $n_t = 10^4$

and $n_t + \hat{n}$ iterates with mapping (1), $\hat{n} = s \times n^3$, where $s = 1, \dots, 30$. The control parameter and the initial values are fixed at $c = 15$ and $(x_0, y_0, z_0) = (0.1, 0.2, 0.3)$. In Figure 5(a), the trajectory $C_{\hat{n}}(x_0, y_0, z_0)$ will visit more than 99% cubes $B_{i,j,k}$, when \hat{n} exceeds $5 \times n^3$. The calculation using mean square error (MSE) is carried out to measure the difference between the values of $P_{\hat{n}}(B_{i,j,k})$ and $\mu(B_{i,j,k})$. This metric is as follows:

$$\text{MSE} \left(P_{\hat{n}} - \frac{1}{n^3} \right) = \frac{1}{n^3} \left\| P_{\hat{n}} - \frac{1}{n^3} \right\|^2, \quad (13)$$

where $\|\cdot\|$ denotes the Euclidian norm. Obviously, in Figure 5(b), MSE values decrease to zero with the number of iterations \hat{n} increasing, which means the point of the trajectory $C_{\hat{n}}(x_0, y_0, z_0)$ is distributed uniformly in the phase space.

The histogram of the approximate density function $P_{\hat{n}}$ is displayed in Figure 6(b). It shows a standard normalized distribution perfectly. The series, which is generated by 3D-PHM, is distributed uniformly in the phase space without any concentration in Figure 6(a). It implies strong chaoticity and ergodicity.

3. The Color Image Encryption Algorithm

To thwart a powerful attack based on statistical analysis, Shannon suggests using confusion and diffusion for encryption [43]. Generally, the security of image encryption technology is defined by shuffling and diffusion. Shuffling is a method to change the positions of pixels in an image. Shuffling can make it difficult to predict the initial positions of an encrypted pixel.

The diffusion operation can be implemented by a chaotic map; it can change the behavior of the whole chaotic system through a small change of the chaotic map. The two implementations can be applied to all kinds of pictures.

Our proposed scheme also has two major steps.

First, the plain image is destroyed by shuffling with 3D-PHM. The second step is to diffuse the shuffled image, which

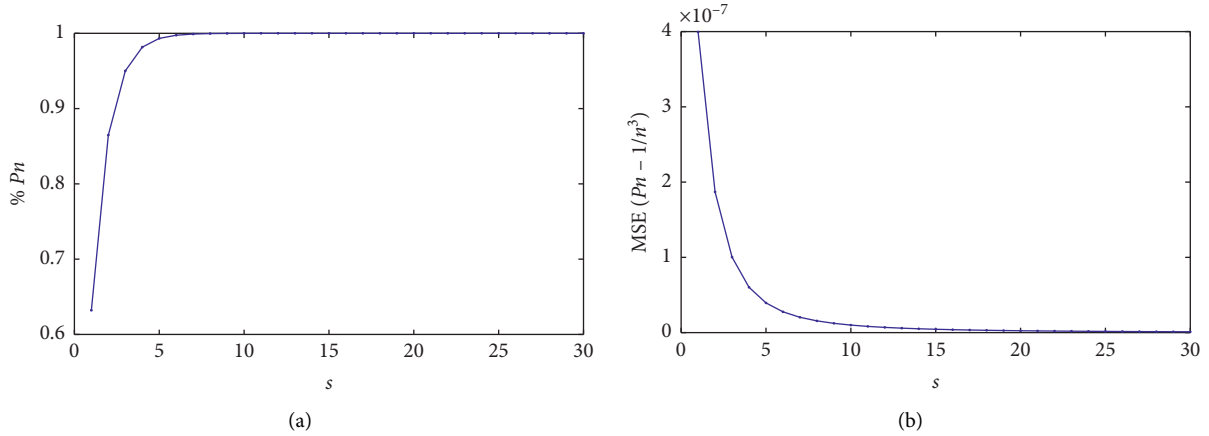


FIGURE 5: The results of P_n and MSE, where $n = 100$, $\hat{n} = s \times n^3$, and $s = 1, 2, \dots, 30$. (a) The proportion of P_n ; (b) the mean square error $\text{MSE}(P_n - 1/n^3)$.

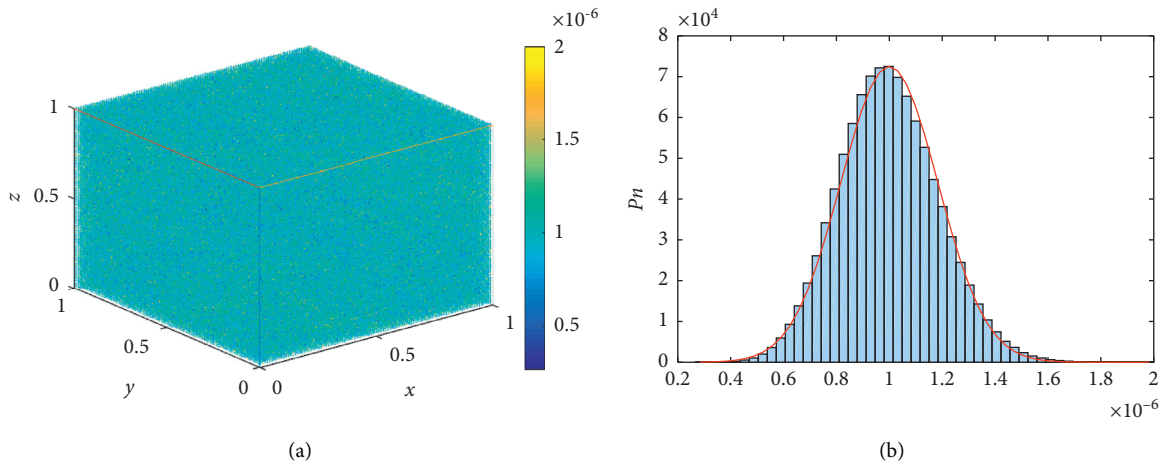


FIGURE 6: (a) The approximate density function P_n of 3D-PHM. (b) The histogram of the density, where $n = 100$ and $\hat{n} = 30 \times n^3$.

is to reach a high complexity. The block diagram of the proposed scheme is shown in Figure 7. The details of the proposed encrypting algorithm are outlined as follows:

- (1) *Primary Stages.* Convert the image with the size of $m \times n \times 3$ into three monochromatic images, where the size is $m \times n$, namely, P_R , P_G , and P_B , and then each matrix is converted into a vector ($1 \times mn$), represented by I_R , I_G , and I_B .
- (2) *Generate the Initial Conditions.* Let the control parameter at $c = 15$ and n_0 be large enough and choose an initial pixel $(\hat{x}_0, \hat{y}_0, \hat{z}_0) \in A$ and calculate the sum of all pixels in every component of the plain image. The formula is as follows:

$$\begin{aligned} \sum_R &= \sum_{i=1}^{mn} I_R(i), \quad \sum_G = \sum_{i=1}^{mn} I_G(i), \\ \sum_B &= \sum_{i=1}^{mn} I_B(i). \end{aligned} \quad (14)$$

K represents the initial values of the scheme and the formula is as follows:

$$K \equiv (x_0, y_0, z_0) = (\hat{x}_0, \hat{y}_0, \hat{z}_0) + \left(10^{-8+d} \times \sum_R, 10^{-8+d} \times \sum_G, 10^{-8+d} \times \sum_B \right). \quad (15)$$

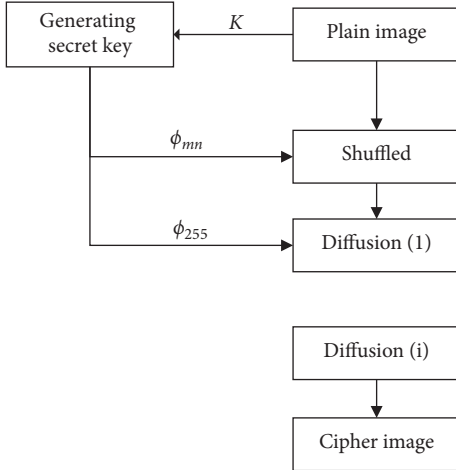


FIGURE 7: The block diagram of encryption algorithm.

- (3) *Generate the Key to Shuffling.* Formula (1) of 3D-PPHM and the initial condition K are used to generate three real-valued sequences with the length of $1 \times mn$, namely, M'_R , M'_G , and M'_B , where $M'_R(i) \in [a_{\min} = 0, a_{\max} = 1]$, $M'_G(i) \in [a_{\min} = 0, a_{\max} = 1]$, and $M'_B(i) \in [a_{\min} = 0, a_{\max} = 1]$, $i = 1, \dots, mn$. The interval $[a_{\min}, a_{\max}]$ is divided into $d + 1$ subintervals on average, and the length of each interval is $h = \lfloor a_{\max} - a_{\min} \rfloor / d + 1$. What function ϕ_d does is to map the value of interval $[a_{\min}, a_{\max}]$ to the set of integers $\{0, 1, \dots, d\}$.

$$\phi_d: [a_{\min}, a_{\max}] \longrightarrow \{0, 1, \dots, d\},$$

$$\phi_d(x) = \begin{cases} \lfloor \frac{x - a_{\min}}{h} \rfloor & \text{if } a_{\min} \leq x < a_{\max}, \\ d, & \text{if } x = a_{\max}, \end{cases} \quad (16)$$

where $d = mn - 1$, and get the integer key sequence $K_R(i)$, $K_G(i)$, and $K_B(i)$; obviously $\{K_R(i), K_G(i), K_B(i)\} \in [0, mn - 1]$.

- (4) *Shuffle Images.* Use Algorithm 1 to generate the shuffled vectors S_R , S_G , and S_B corresponding to the three monochromatic components of the initial plain images I_R , I_G , and I_B .

For example, provide that $K_R(1) = 345$, $I(1) = 255$, and then $S_R(345 + 1) = I(1) = 255$. So generate three shuffled images S_R , S_G and S_B .

- (5) *Generate the Chaotic Mask Sequence.* Use formula (17) to obtain the integer chaotic masks, M_R , M_G and M_B , respectively, where $d = 255$. The formula is as follows:

$$\begin{cases} M_R(i) = \phi_d(M'_R(i)) \\ M_G(i) = \phi_d(M'_G(i)), \quad i = 1, 2, \dots, mn. \\ M_B(i) = \phi_d(M'_B(i)) \end{cases} \quad (17)$$

- (6) *Diffusion of the Cipher Image.* Formulas (18)–(20) are used to obtain three encrypted image integer matrices C_R , C_G , and C_B . For example, for the red component, the pixel sequence of the scrambled image is $\{S_R(i) | tin = q1, 2h, \dots, x, 7mCn\}$, the chaotic mask series is $\{M_R(i) | it = n1, 2q, h \dots, xm7n\}$, and the ciphertext is $\{C_R(i) | tin = q1, 2h, \dots, x, 7mCn\}$. Here, the round n encryption scheme is introduced as follows:

$$\begin{cases} C_R^{(1)}(0) = \text{mod}(D_R(0) + M_R(1), 256), \\ C_R^{(1)}(i) = \text{mod}(S_R(i) + M_R(i + 1), 256) \oplus C_R^{(1)}(i - 1), \\ C_R^{(2)}(i) = \text{mod}(C_R^{(1)}(i) + M_R(i + 1), 256) \oplus C_R^{(2)}(i - 1), \\ \vdots \\ C_R^{(n)}(i) = \text{mod}(C_R^{(n-1)}(i) + M_R(i + 1), 256) \oplus C_R^{(n)}(i - 1), \end{cases} \quad i = 1, 2, \dots, mn, \quad (18)$$

$$\begin{cases} C_G^{(1)}(0) = \text{mod}(D_G(0) + M_G(1), 256), \\ C_G^{(1)}(i) = \text{mod}(S_G(i) + M_G(i + 1), 256) \oplus C_G^{(1)}(i - 1), \\ C_G^{(2)}(i) = \text{mod}(C_G^{(1)}(i) + M_G(i + 1), 256) \oplus C_G^{(2)}(i - 1), \\ \vdots \\ C_G^{(n)}(i) = \text{mod}(C_G^{(n-1)}(i) + M_G(i + 1), 256) \oplus C_G^{(n)}(i - 1), \end{cases} \quad i = 1, 2, \dots, mn, \quad (19)$$


```

Input: the integers  $m$  and  $n$ , and the vectors  $I_R, I_G$  and  $I_B$ 
Output: the shuffled images vectors  $S_R, S_G$  and  $S_B$ 
while  $k_R \leq mn$ 
     $S_R \leftarrow -1, S_G \leftarrow -1, S_B \leftarrow -1$ 
end
     $k_R \leftarrow 1, i \leftarrow 1$ 
    while  $k_R \leq mn$ 
        if  $(S_R(K_R(k_R) + 1) = -1)$ 
             $S_R(K_R(k_R) + 1) \leftarrow I_R(k_R);$ 
        else
             $S_R(K_R(k_R) + 1 + i) \leftarrow I_R(k_R);$ 
        end
         $k_R \leftarrow k_R + 1; i \leftarrow i + 1;$ 
    end

```

ALGORITHM 1: Shuffle images (the red component is selected as research sample).

$$\begin{cases} C_B^{(1)}(0) = \text{mod}(D_B(0) + M_B(1), 256), \\ C_B^{(1)}(i) = \text{mod}(S_B(i) + M_B(i+1), 256) \oplus C_B^{(1)}(i-1), \\ C_B^{(2)}(i) = \text{mod}(C_B^{(1)}(i) + M_B(i+1), 256) \oplus C_B^{(2)}(i-1), & i = 1, 2, \dots, mn, \\ \vdots \\ C_B^{(n)}(i) = \text{mod}(C_B^{(n-1)}(i) + M_B(i+1), 256) \oplus C_B^{(n)}(i-1), \end{cases} \quad (20)$$

where $\{D_R(0), D_G(0), D_B(0)\} \in [0, 255]$ are the parameters introduced when encrypting the first scrambling pixel, which can be used as the initial key in the encryption and $\{C_R^{(1)}, C_G^{(1)}, C_B^{(1)}; C_R^{(2)}, C_G^{(2)}, C_B^{(2)}; \dots; C_R^{(n)}, C_G^{(n)}, C_B^{(n)}\}$ are results of the n th round encryption. Generally, $n \geq 2$. The relationship among the ciphertext, plaintext (or intermediate ciphertext), and the key not only is XOR but also includes nonlinear module. Thus, the proposed algorithm can resist plaintext attack. Then convert each component into matrices $C_R^{(n)}, C_G^{(n)},$ and $C_B^{(n)}$, whose size is $m \times n$. Finally, the color cipher C_{RGB} is combined.

Decryption is the inverse of encryption, but decryption starts with the last pixel and goes back to the first. The process of decryption is given as follows:

- (1) Splitting the ciphered image C_{RGB} into three separated components and then converting them into encrypted pixel sequences $C_R, C_G,$ and C_B ($1 \times mn$).
- (2) Formula (17) is used to obtain the secret key sequences $M_R, M_G,$ and $M_B,$ and formulas (21)–(23) are used to obtain the shuffled sequences $S_R(i), S_G(i),$ and $S_B(i)$ when the round number $n = 2$.

$$\begin{cases} C_R^{(1)}(i) = \text{mod}((C_R^{(2)}(i) \oplus C_R^{(2)}(i-1) - M_R(i+1)), 256), \\ S_R(i) = \text{mod}((C_R^{(1)}(i) \oplus C_R^{(1)}(i-1) - M_R(i+1)), 256), \end{cases} \quad i = mn, mn-1, \dots, 1, \quad (21)$$

$$\begin{cases} C_G^{(1)}(i) = \text{mod}((C_G^{(2)}(i) \oplus C_G^{(2)}(i-1) - M_G(i+1)), 256), \\ S_G(i) = \text{mod}((C_G^{(1)}(i) \oplus C_G^{(1)}(i-1) - M_G(i+1)), 256), \end{cases} \quad i = mn, mn-1, \dots, 1, \quad (22)$$

$$\begin{cases} C_B^{(1)}(i) = \text{mod}((C_B^{(2)}(i) \oplus C_B^{(2)}(i-1) - M_B(i+1)), 256), \\ S_B(i) = \text{mod}((C_B^{(1)}(i) \oplus C_B^{(1)}(i-1) - M_B(i+1)), 256), \end{cases} \quad i = mn, mn-1, \dots, 1. \quad (23)$$

- (3) Use the vectors S_R , S_G , and S_B as input with Algorithm 2 to generate the deshuffled vectors I_R , I_G , and I_B .
- (4) Obtain pixel sequences I_R , I_G , and I_B , and combine them into the plain image P .

4. Simulation and Experimental Analysis

For all the analysis, the control parameters $c_1 = c_2 = c = 15$, the round number $n = 2$, the initial value $(x_0, y_0, z_0) = (0.1, 0.2, 0.3)$, and $\{C_R(0), C_G(0), C_B(0)\} = \{234, 15, 167\}$. The proposed color image cryptosystem is executed on the standard test image named "Lena" with the size $512 \times 512 \times 3$. The ciphertext of the three color components of the color image is shown in Figure 8.

In order to demonstrate that the proposed image encryption algorithm is secure against most common attacks, key space and key sensitivity tests are analyzed, and security analyses such as chosen plaintext attack, histogram analysis, correlation of the image, difference measurement, and information entropy are also carried out.

4.1. Key Space Analysis. In order to resist brute-force attacks, it is necessary to extend a key space as large as feasible. Generally, the security will be accepted when the key space is greater than 2^{128} . The proposed algorithm takes the initial three states of formula (1) as the initial secret keys, expressed by double-precision real type. So the key space is $2^{64} \times 2^{64} \times 2^{64} = 2^{192}$. In addition, $\{D_R(0), D_G(0), D_B(0)\}$ can also be the initial key. So the key space of the proposed algorithm is 2^{216} . Therefore, it is sufficiently large to prevent a brute-force attack [35, 44, 45]. The comparison of key space sizes between the proposed scheme and similar works is displayed in Table 2.

4.2. Key Sensitivity Analysis. A secure image encryption scheme requires a high secret key sensitivity. It means that even a very small change between the initial keys can cause two completely different decrypted images. The plaintext and the ciphertext are shown in Figures 9(a) and 9(b). In Figure 9(c), the right decryption is shown and the wrong result is shown in Figure 9(d), where the initial value is $\tilde{K} = \{x_0 + \delta, y_0, z_0\}$ and $\delta = 10^{-16}$. It is easy to distinguish that the last image is completely different from the original image. The proposed scheme is sensitive to the key.

4.3. Image Histogram Analysis. For the three color components of RGB images, the graph with the number of pixels at each gray level is histogram. Histogram analyses for the original image and the encrypted image by the proposed scheme are carried out in this paper. Histograms for three components of the original and encrypted images are shown in Figure 10. From Figures 10(b), 10(d), and 10(f), the histograms are quite uniform and they are different from the plaintext. It means that the result of the algorithm can resist the known plaintext attack [47].

It is necessary to verify the security of the encrypted image with histogram analysis, but it is not enough. In order to further verify the uniform distribution of the ciphertext, the Chi-square test is applied. It is as follows:

$$\chi^2 = \sum_{i=0}^{255} \frac{(o_i - e_i)^2}{e_i}, \quad (24)$$

where o_i are the occurrence times for every gray level (0 to 255) of the cipher and e_i is the mean occurrence frequency of the uniform distribution, which is 1024 in the image with the size of 512×512 . For a secure cryptosystem, the values of χ^2 in encrypted images must be less than the values of χ^2 in plain images. In Table 3, values of χ^2 in the plain image are much larger than values of χ^2 in the encryption image, which means the security of the proposed algorithm has good encryption effect.

4.4. Correlations of Adjacent Pixels. Besides histograms analysis, the correlation between adjacent pixels in the plain and encrypted image is conducted. The correlation coefficients ρ of several adjacent pixel pairs (including horizontal, vertical, and diagonal pixel pairs) which are selected from the image are computed. The formula is as follows:

$$\rho = \frac{\sum_{i=1}^{M_0} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^{M_0} (x_i - \bar{x})^2)(\sum_{i=1}^{M_0} (y_i - \bar{y})^2)}}, \quad (25)$$

where x_i and y_i represent the gray values of two adjacent pixels in the plain and encrypted image and M_0 is the number of adjacent pixels pairs selected randomly from the plain or encrypted image. ρ , \bar{x} , and \bar{y} represent the two means of two adjacent pixels. When $\rho \rightarrow 1$, it will indicate that the adjacent pixels are highly correlated, and when $\rho \rightarrow 0$, it will mean that the adjacent pixels are low correlated.

For the correlation analysis experiment, we randomly selected 10000 pairs of adjacent pixels from the plain and encrypted images in horizontal, vertical, and diagonal directions. The experimental results are shown in Figure 11, where (i, j) represents the coordinate of pixels in an image. From Figure 11, the correlation of the plain image is significantly higher than that of the encrypted image.

In addition, the correlation coefficients ρ of the original image are computed, which are listed in Table 4. ρ of the original image are close to 1. Otherwise, the encrypted ρ are close to 0. It means that the proposed algorithm removed the correlation between adjacent pixels of the original image. Then, comparisons are conducted among different algorithms in Table 4. The correlation coefficient of the plain image is extremely different from the encrypted image and the former is close to zero. The encrypted ρ of ours is more close to zero than others.

4.5. The Difference Measurements. The degradation rate of the image after encryption can also prove the encrypted effect of an encryption system. To measure the difference

```

Input:  $M_R$  and  $M_G$  and  $M_B$ ,  $S_R$ ,  $S_G$ , and  $S_B$ 
Output:  $I_R$ ,  $I_G$  and  $I_B$ 
Initialize:  $k_r \leftarrow 0$ ,  $i \leftarrow 1$ 
while  $k_r \leq mn$ 
  if  $(S_R(K_R(k_r) + 1) \geq 0)$ 
     $I_R(k_r) \leftarrow S_R(K_R(k_r) + 1)$ ;
     $S_R(K_R(k_r) + 1) \leftarrow -1$ ;
  else
     $i \leftarrow K_R(k_r) + 1$ ;
     $I_R(k_r) \leftarrow S_R(i)$ ;
     $S_R(i) \leftarrow -1$ ;
  end
   $k_r \leftarrow k_r + 1$ ;
end

```

ALGORITHM 2: Deshuffling the images.

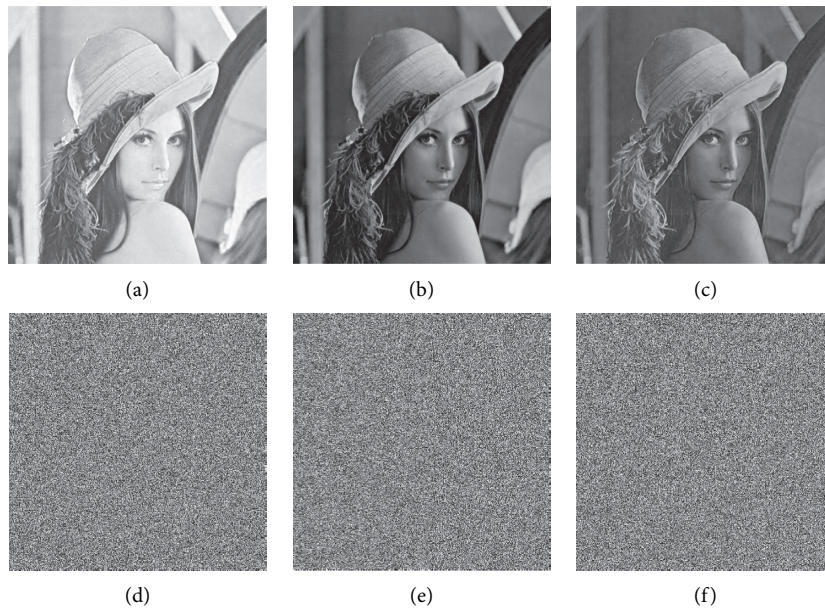


FIGURE 8: Every component of plaintext and its ciphertext. (a) Component R of plaintext; (b) component G of plaintext; (c) component B of plaintext; (d) component R of ciphertext; (e) component G of ciphertext; (f) component B of ciphertext.

TABLE 2: Comparison of key spaces among different schemes.

	The number of keys	Key space size
Our cryptosystem	6	2^{216}
Reference [44]	7	2^{130}
Reference [35]	3	2^{140}
Reference [45]	8	2^{160}
Reference [46]	8	2^{280}

between the original and the encrypted images, we have the two following effective statistical tools.

4.5.1. The Structural Similarity Index. The structural similarity (SSIM) index can indicate the similarity between the two images. The SSIM belongs to $[-1, 1]$. When the SSIM is 1, it indicates that the two images are completely similar. It is

defined by the attribute of the object structure in the reflection scene independent of brightness and contrast, which is from the angle of image composition. The value of SSIM is composed of brightness, contrast, and structure of images. Mean values are used by estimating the brightness, and the standard deviation is used by estimating the contrast, and the covariance is used by measuring the similarity of the structure. The formula used to calculate SSIM of two images is as follows:

$$\text{SSIM}(X, Y) = \frac{(2u_X u_Y + C_1)(2\sigma_{XY} + C_1)}{(u_X^2 + u_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)}, \quad (26)$$

where u_X and u_Y represent the means of gray pixels in two images; σ_X and σ_Y are the standard deviations of the two images; σ_X^2 and σ_Y^2 are the variances of the two images; σ_{XY}

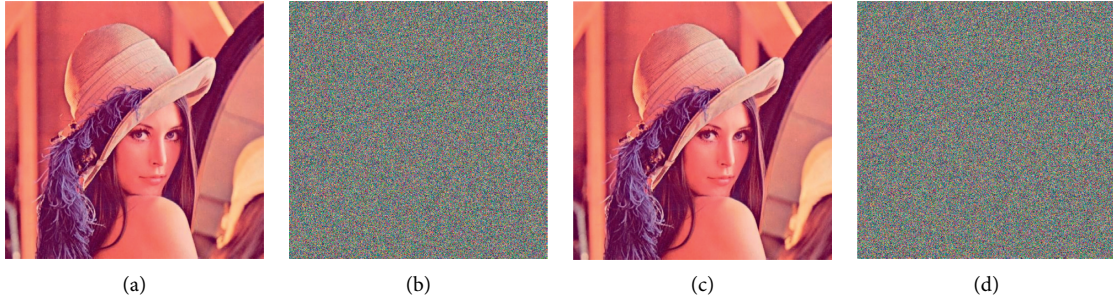


FIGURE 9: Decrypting Lena image by two secret keys $K = \{x_0, y_0, z_0\}$ and $\tilde{K} = \{x_0 + \delta, y_0, z_0\}$, where $\delta = 10^{-16}$. (a) The original image; (b) encrypted image with K ; (c) decrypted image with K ; (d) decrypted image with the wrong key \tilde{K} .

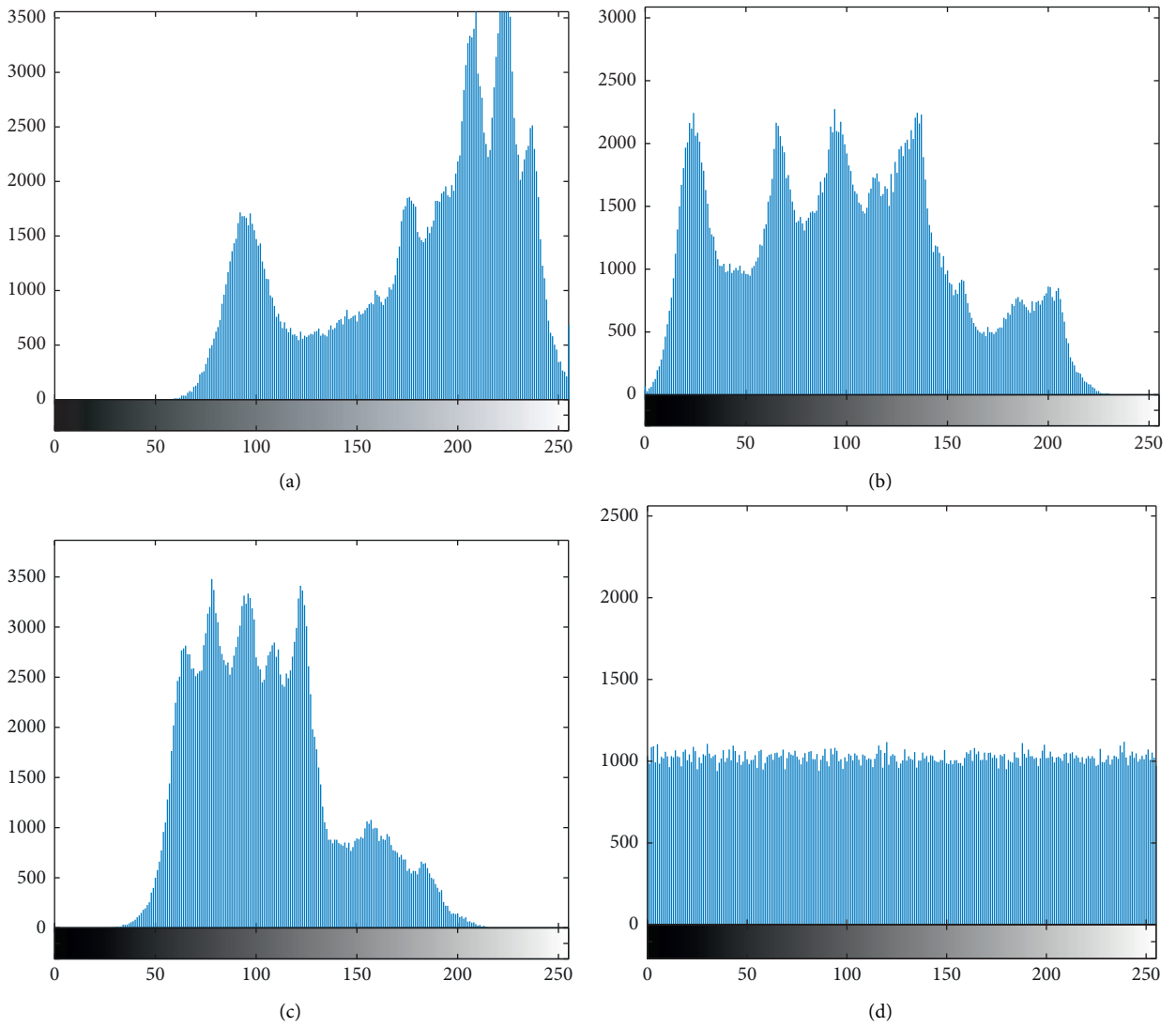


FIGURE 10: Continued.

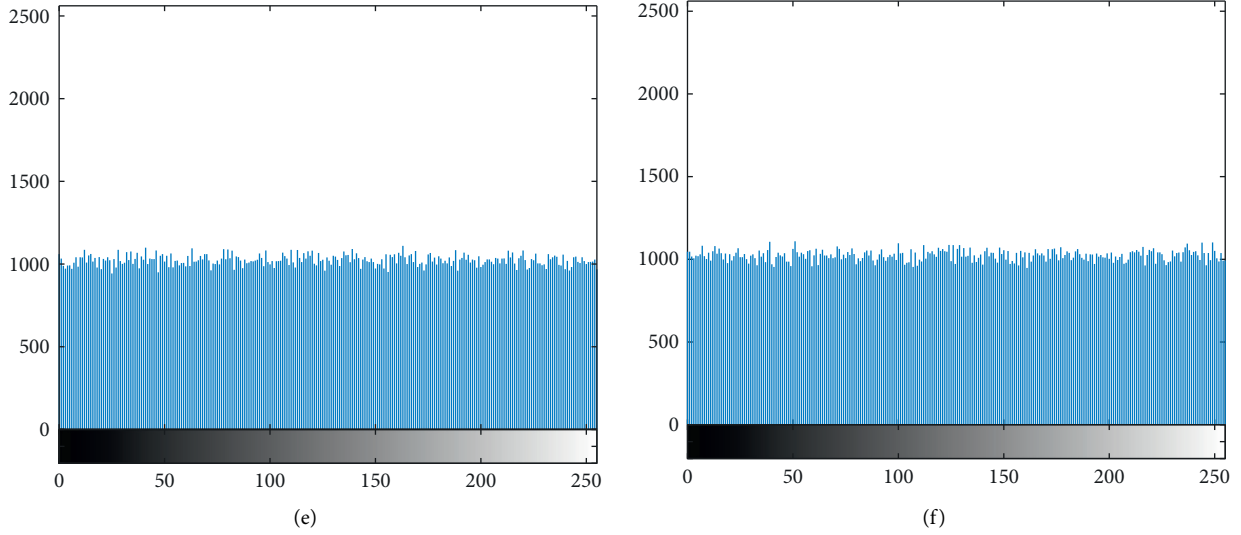


FIGURE 10: Histogram of every component of RGB (Lena); (a) histogram of R of plaintext; (b) histogram of G of plaintext; (c) histogram of B of plaintext; (d) histogram of R of ciphertext; (e) histogram of G of ciphertext; (f) histogram of B of ciphertext.

TABLE 3: Values of χ^2 for plain and encrypted Lena images.

	χ^2		
	Red	Green	Blue
Original image	243712.39	118826.39	335466.77
Proposed algorithm	300.1914	272.8633	273.4277

represents the covariance of the two images; C_1 and C_2 are two constants, where $C_1 = K_1 \times L$ and $C_2 = K_2 \times L$. Generally, $K_1 = 0.01$, $K_2 = 0.03$, and $L = 255$. The SSIM of different encryption schemes are listed in Table 5. The SSIM between the original image and other encrypted schemes of “Lena” approach zero. Compared with others, the proposed algorithm has higher superiority.

4.5.2. Peak Signal-to-Noise Ratio Analysis. Peak signal-to-noise ratio (PSNR) is the most common and widely used objective evaluation index of images. For a perfect image encryption scheme, the smaller values of the PSNR are (generally, less than 10), the better schemes are. The calculation is as follows:

$$\text{MSE} = \frac{1}{mn} \sum_{i,j} (C(i, j) - I(i, j))^2, \quad (27)$$

$$\text{PSNR} = 10 \log_{10} \left(\frac{L^2}{\text{MSE}} \right),$$

where MSE is the mean square error of an image; $C(i, j)$ is a pixel of the encrypted image and $I(i, j)$ is a pixel of the original image, the coordinate of which is (i, j) ; L is the range of pixel in the image. We calculated PSNR of each color component of the encrypted image (Lena) and found that it was less than 10. Values of PSNR of this encryption scheme are compared with the results of other schemes; see Table 6. From the comparison in Table 6, we can see that the

results of PSNR of this scheme are better than those of other existing algorithms.

4.6. Analysis of Antidifferential Attack. In the encryption algorithm, diffusion is an important property, which was proposed by Shannon in [43]. A good encryption system must have good diffusivity. It means that one pixel in the original image is changed, and the encrypted image will be changed completely in an unpredictable way.

The important significance of the diffusion depends on how complex the algorithm is, which can resist the analysis of the algorithm by the attacker. The number of pixel change rate (NPCR) is usually used to test the effect of changing a pixel in the encrypted scheme, which calculates the percentage of two different image pixels.

The average intensity of the two images is tested by UACI. Here, C_1 and C_2 are two cipher images whose corresponding plain images have only one pixel difference. $D(i, j)$ is defined as

$$D(i, j) = \begin{cases} 0, & C_1(i, j) = C_2(i, j), \\ 1, & C_1(i, j) \neq C_2(i, j), \end{cases} \quad (28)$$

$$\text{NPCR} = \frac{\sum_{i=1}^m \sum_{j=1}^n D(i, j)}{mn},$$

and UACI is defined as

$$\text{UACI} = \frac{\sum_{i=1}^m \sum_{j=1}^n |C_1(i, j) - C_2(i, j)|}{255 \times m \times n}, \quad (29)$$

where m and n are rows and columns of the image, respectively. Ideally, the means of NPCR and UACI are $\text{NPCR} = (1 - 2^{-n}) \times 100\%$ and $\text{UACI} = 1/2^{2n} \sum_{i=1}^{2^n-1} i(i+1)/2^n - 1100\%$. For grayscale image with 256 levels, $n = 8$. The expected values of NPCR and

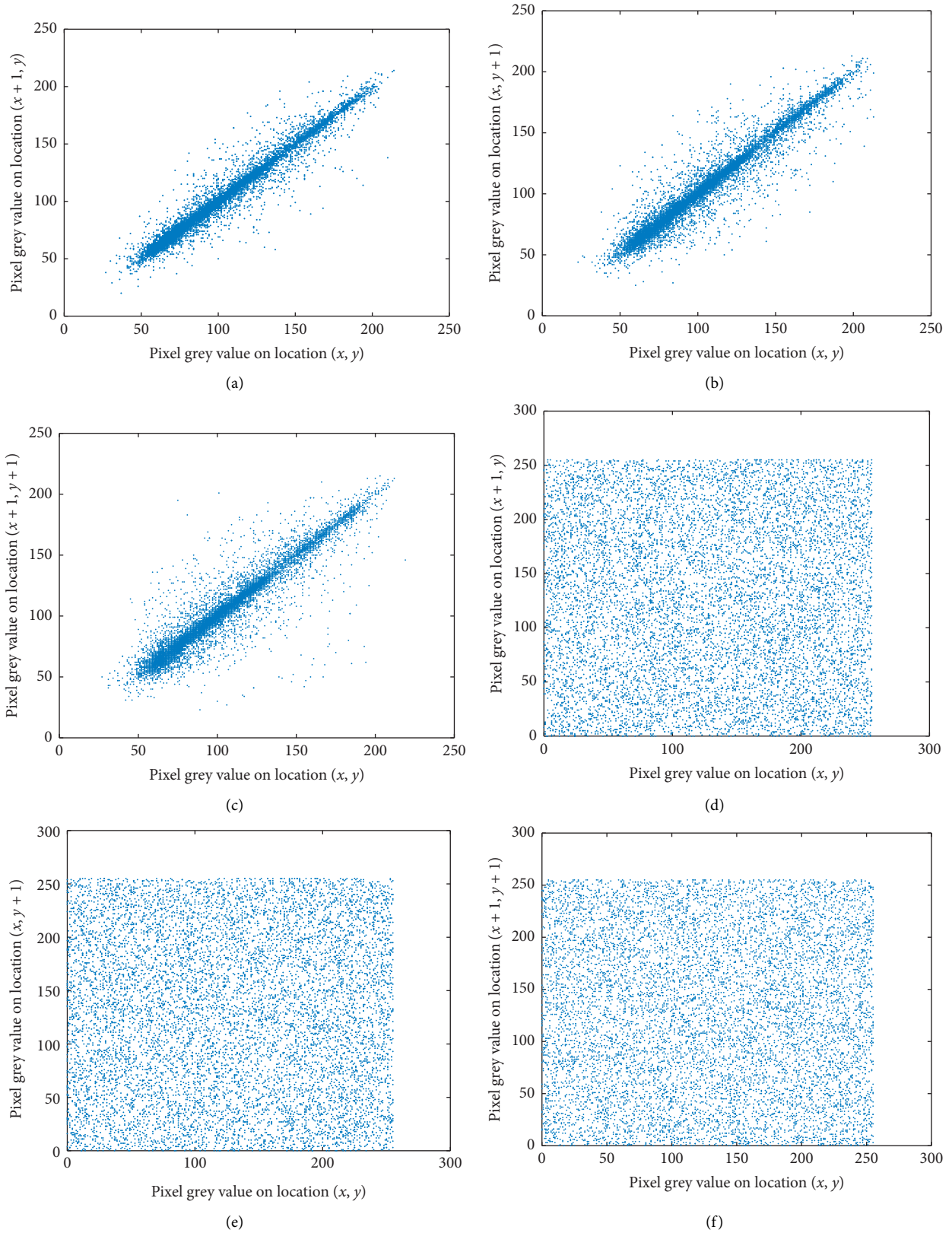


FIGURE 11: The correlation plots of two adjacent pixels for plaintext and ciphertext. (a) Horizontal correlation of plaintext; (b) vertical correlation of plaintext; (c) diagonal correlation of plaintext; (d) horizontal correlation of ciphertext; (e) vertical correlation of ciphertext; (f) diagonal correlation of ciphertext.

TABLE 4: The correlation coefficients between the proposed method and other algorithms.

	Correlation direction		
	Diagonal	Horizontal	Vertical
Original image	0.9501	0.9690	0.9835
Proposed algorithm	-0.0033	-0.0012	-0.0027
Reference [48]	0.0036	0.0053	0.0085
Reference [49]	0.0024	0.0042	0.0033
Reference [50]	—	0.0681	0.0845
Reference [51]	0.0030	-0.0082	0.0027

TABLE 5: SSIM between the plain and other encrypted images.

Algorithm	SSIM			Average SSIM
	Red	Green	Blue	
Proposed algorithm	0.010050	0.009141	0.010104	0.009765
Reference [52]	0.0194	0.0448	0.04475	0.0372
Reference [53]	—	—	—	0.3795
Reference [54]	—	—	—	0.0425

TABLE 6: PSNR results between the proposed algorithm and other algorithms (Lena).

Algorithms	PSNR			Average PSNR
	Red	Green	Blue	
Proposed algorithm	7.8415	8.5890	9.5995	8.6767
Reference [55]	—	—	—	10.8314
Reference [56]	—	—	—	9.5513
Reference [57]	7.8160	8.6070	9.6404	8.6877
Reference [58]	—	—	—	9.2322

UACI are $\text{NPCR}_E = 99.6094070$ and $\text{UACI}_E = 33.463507$, respectively.

In the experiment, 100 group pixels of Lena image were selected for encryption. Every group has two images. One is the original image, and the other is image with one pixel changed, which is an image where one pixel is changed randomly in the original image. The results of NPCR and UACI are shown in Figures 12 and 13. Results of the proposed algorithm are distributed near the ideal value (horizontal lines in the figure). The mean values of NPCR and UACI in the proposed scheme are 99.6214% and 33.4149%, respectively, which are very close to the ideal values.

The comparison with other algorithms is shown in Table 7. The results show that the proposed algorithm can resist plaintext attack, ciphertext attack, and known plaintext attack well, and it is also superior to other algorithms. The reason is, in other schemes, the ciphertext diffusion effect of the algorithm works only in one round of pixel substitution, in which the change of any one pixel in plaintext can only affect the ciphertext behind the changed pixel. In this paper, two or more rounds of diffusion are carried out. Therefore, each pixel in the encrypted image will be affected.

4.7. *Analysis of Chosen Plaintext Attack.* The ability of a scheme to resist the chosen plaintext attack should be tested in the following way. The formula is as follows [61]:

$$O1(i, j) \oplus O2(i, j) = E1(i, j) \oplus E2(i, j), \quad (30)$$

where $O1$ and $O2$ are two plain images and $E1$ and $E2$ are two encrypted images which are encrypted by the same plain images. When the equation holds right, the algorithm will be highly vulnerable to chosen plaintext attack. Figure 14(a) indicates $E1 \oplus E2$ (XOR operation to the encrypted images of Lena and baboon), and Figure 14(b) indicates $O1 \oplus O2$ (XOR operation to the plain images of Lena and baboon). Obviously, Figures 14(a) and 14(b) are completely different, indicating that the equation is not tenable. Therefore, the algorithm can resist chosen plaintext attack.

4.8. *Analysis of Plaintext Attacks.* In many methods of cryptanalysis, attackers try to identify the relationship between plaintext and ciphertext by searching ways to reduce the key space or the equivalent key space. This kind of attack usually uses white or black pixels to generate ciphertext by the proposed algorithm. Then the key is inferred from the corresponding ciphertext image. In order to resist this attack, this encryption scheme should eliminate any relationship between ciphertext and plaintext.

The proposed scheme, even if a specific plaintext is selected, such as black and white images, cannot generate recognizable patterns. It is because the encryption algorithm not only depends on the change of pixel position but also depends on the high complexity of the novel chaotic and good multiple diffusion characteristics of the encryption algorithm. Especially when the algorithm is used to encrypt adjacent columns/rows, the adjacent pixels will have little correlation.

The results of our proposed algorithm are depicted in Figure 15. The size of the white and black images is 512×512 . They are encrypted by the proposed algorithm. From Figures 15(b) and 15(d), the encrypted images are different from the original images. Then, our proposed encryption algorithm can resist the known plaintext attack.

4.9. Analysis of Noise Attack

4.9.1. *Analysis of Pepper and Salt Noise Attack.* The ability of the encryption system to resist noise attack is tested by adding salt and pepper noise with different intensities when encrypting the image. Figure 16 shows the decrypted images where densities of 0.05 and 0.1 are added, respectively. The decrypted images become slightly blurred, but the contents of the images can still be recognized.

4.9.2. *Analysis of Gaussian Noise.* The Gaussian noise with variance of 0.01 and zero mean was added to the encryption process, and the result is shown in Figure 17(a). Take the Gaussian noise with variance of 0.5 and zero mean, and the result is shown in Figure 17(b). Although the decrypted image is still fuzzy, it can still distinguish the basic image

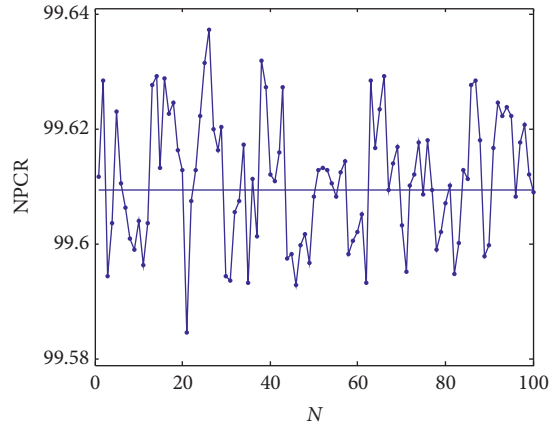
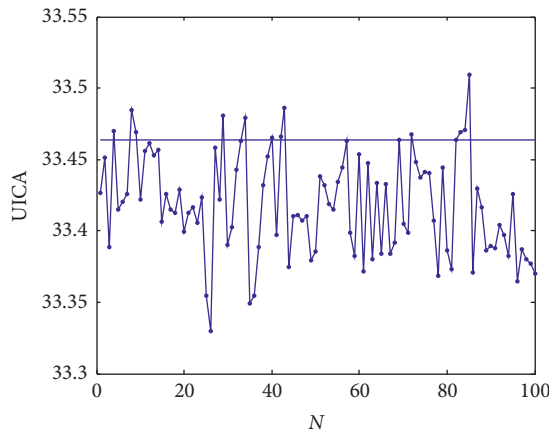
FIGURE 12: Test results of NPCR (N is the test group label).FIGURE 13: Test results of UACI (N is the test group label).

TABLE 7: NPCR and UACI results between the proposed algorithm and other schemes (Lena).

Algorithms	NPCR	UACI
Proposed algorithm	0.9962	0.3341
Reference [59]	0.9936	0.3272
Reference [60]	0.9961	0.3346
Reference [36]	0.9960	0.3347

content. It illustrates that the proposed algorithm can resist the Gaussian noise.

4.10. Information Entropy. Information entropy (EN) can describe the complexity, which can quantify the randomness of a chaotic system. Let s represent a source of information, and the entropy $H(s)$ can be calculated by

$$H(s) = - \sum_{i=0}^{2^n-1} P(s_i) \log_2(P(s_i)), \quad (31)$$

where $P(s_i)$ is the probability of the symbol s_i which can appear in the chaotic system. For a random signal consisting of 2^n symbols, $H(s)$ is equal to 8. The information entropy value of the proposed scheme is calculated. The results

between the proposed algorithm and other schemes are shown in Table 8 and our values are 7.9984, 7.9982, and 7.9979, respectively, which are higher than others, ensuring that our scheme is more complex.

4.11. Computational Complexity and Speed Test. The computational complexity of algorithms is often used to describe the execution time of programs or the space occupied by algorithms in memory or disk. It is often represented by symbol O .

The function $T(n)$ represents the time of an algorithm (or the number of steps), where n is the size of the problem to be solved and $n \rightarrow g(n)$. Theoretically, the function $T(n) = O(g(n))$. It means that there is a positive constant δ which makes $0 \leq T(n) \leq \delta g(n)$. Given that the size of the image is $m \times n$, the times of scrambling statements are $m \times n$ during the image encryption. Take two rounds as an example; the times of the diffusion statement are $2m \times n$. The times of decrypted statement are the same as those of the encryption. So, we can write the expression as $T(n) = O(mn)$. Therefore, the complexity of the algorithm is $O(mn)$. Thus, the proposed algorithm can resist different cryptographic analysis.

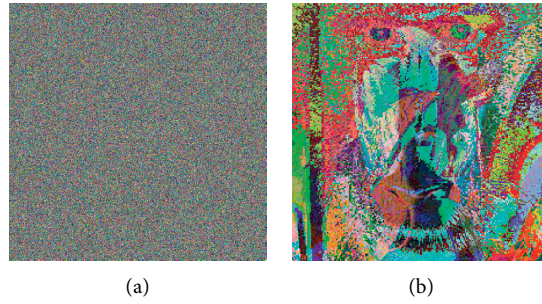


FIGURE 14: The result of chosen plaintext attack analysis: (a) $E1 \oplus E2$; (b) $O1 \oplus O2$.

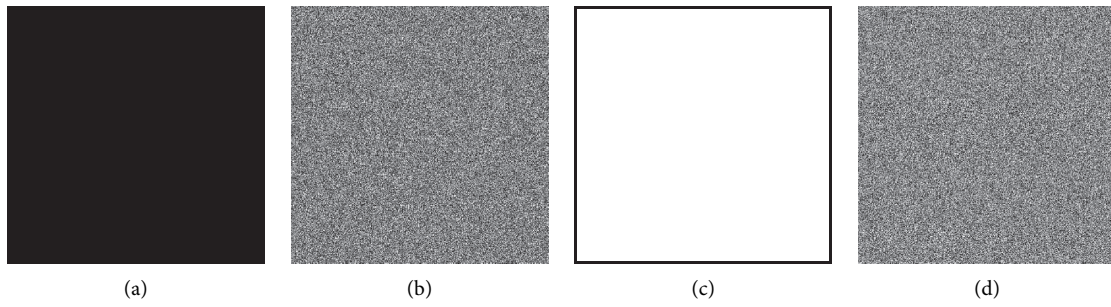


FIGURE 15: Results of the black and white images by the proposed algorithm. (a) Black plaintext; (b) black ciphertext; (c) white plaintext; (d) white ciphertext.



FIGURE 16: The decryption image with different densities of salt and pepper noise. (a) 0.05 and (b) 0.1.

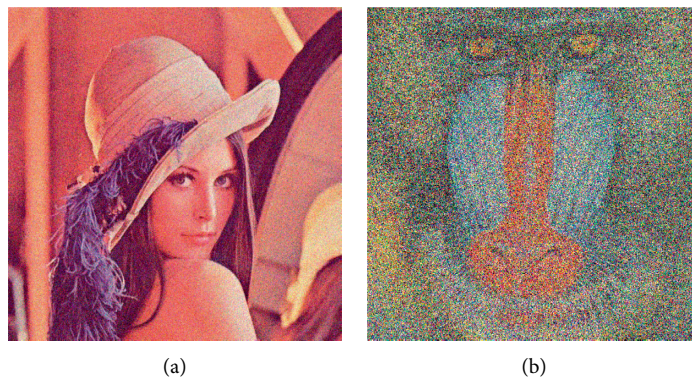


FIGURE 17: The decryption image of the plain image by adding different variance Gaussian noise.

TABLE 8: The results of information entropy.

Methods	Information entropy			
	Red	Green	Blue	Average
Our proposed algorithm	7.9984	7.9982	7.9983	7.9983
Reference [62]	7.9868	7.9880	7.9884	7.9877
Reference [50]	—	—	—	7.9971

TABLE 9: Encrypted speed of each scheme.

Image	DES time (s)	AES time (s)	Logistic map time (s)	Our proposed time (s)
Lena 512×512	2.39694	0.90037	0.76321	0.68795
Baboon 256×256	0.88076	0.46158	$3.5478e - 002$	$2.4457e - 002$
House 128×128	0.45123	0.25487	$1.2347e - 002$	$0.4567e - 002$

The speed of every scheme is shown in Table 9. We implement our scheme and other schemes using Matlab R2016b on an Intel Core i5-4590 @ 3.30 GHz Processor, 4 GB RAM, and Windows 10 operating system. Compared with DES, AES, and logistic mapping encryption scheme, our chaotic encrypted algorithm is more quick than traditional ones.

5. Conclusion

This paper has proposed a new color image encryption based on 3D-PHM. 3D-PHM shows better chaotic complexity and performance than the original mappings. It enlarges the dimensions of Henon mapping and the complexity of low-dimensional chaotic mapping is increased, and the method can also be applied to other low-dimensional chaotic mappings. At the same time, the parameter range of 3D-PHM is also enlarged, which increases the key space of the original mapping. Based on the new chaotic mapping, this paper proposes the color image encryption scheme, which is associated with the key, plaintext, and intermediate ciphertext. Security and performance evaluation shows that the proposed cipher has various desirable characteristics such as efficiency, flexibility, and resistance against cryptanalytic attacks.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61471158).

References

- [1] M. Kanafchian and B. Fathi-Vajargah, "A novel image encryption scheme based on clifford attractor and noisy logistic map for secure transferring images in navy," *International Journal of E-Navigation and Maritime Economy*, vol. 6, pp. 53–63, 2017.
- [2] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.
- [3] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process: Image Communication*, vol. 52, pp. 6–19, 2017.
- [4] S. Tedmori and N. Al-Najdawi, "Image cryptographic algorithm based on the haar wavelet transform," *Information Sciences*, vol. 269, pp. 21–34, 2014.
- [5] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.
- [6] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 2016.
- [7] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2018.
- [8] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, 2017.
- [9] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.
- [10] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Processing*, vol. 164, pp. 249–266, 2019.
- [11] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dynamics*, vol. 96, pp. 601–613, 2019.
- [12] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *Journal of the Franklin Institute*, vol. 348, no. 8, pp. 1797–1813, 2011.
- [13] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.
- [14] Y. Z. Z. Hua and S. Yi, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, 2018.
- [15] J. S. Teh, K. Tan, and M. Alawida, "A chaos-based keyed hash function based on fixed point representation," *Cluster Computing*, vol. 22, no. 2, pp. 649–660, 2019.

- [16] B. Yang and X. Liao, "Period analysis of the logistic map for the finite field," *Science China Information Sciences*, vol. 60, no. 2, pp. 45–59, 2017.
- [17] B. Yang and X. Liao, "Some properties of the logistic map over the finite field and its application," *Signal Processing*, vol. 153, pp. 231–242, 2018.
- [18] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. H. Fahmy, "Finite precision logistic map between computational efficiency and accuracy with encryption applications," *Complexity*, vol. 2017, Article ID 8692046, 21 pages, 2017.
- [19] X. Tong and M. Cui, "Image encryption scheme based on 3d baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, no. 4, pp. 480–491, 2009.
- [20] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.
- [21] Y. Zhou, Z. Hua, C. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Transactions on Cybernetics*, vol. 45, no. 9, p. 2001, 2012.
- [22] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Processing*, vol. 147, pp. 133–145, 2018.
- [23] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, and J. Harkin, "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation," *International Journal of Bifurcation and Chaos*, vol. 27, no. 3, Article ID 1750033, 2017.
- [24] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.
- [25] W. Yue, Z. Yicong, and L. Bao, "Discrete wheel-switching chaotic system and applications," *IEEE Transaction on Circuits and Systems-I: Regular Papers*, vol. 61, no. 12, pp. 3469–3477, 2014.
- [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. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.
- [28] 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.
- [29] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.
- [30] C. Liu and Q. Ding, "A modified Algorithm for the logistic sequence based on PCA," *IEEE Access*, vol. 8, pp. 45254–45262, 2020.
- [31] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "Modified substitution-diffusion image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 10, pp. 2755–2765, 2010.
- [32] 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.
- [33] W. Yue, Z. Yicong, and B. Long, "Image encryption based on three-dimensional bitmatrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.
- [34] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical Review Letters*, vol. 88, no. 17, 4 pages, Article ID 174102, 2002.
- [35] X. J. Tong, Z. Wang, M. Zhang, Y. Liu, H. Xu, and J. Ma, "An image encryption algorithm based on the perturbed high-dimensional chaotic map," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1493–1508, 2015.
- [36] W. Yao, X. Zhang, Z. Zheng, and W. Qiu, "A colour image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems," *Nonlinear Dynamics*, vol. 81, no. 1–2, pp. 151–168, 2015.
- [37] O. E. Lanford, "Informal remarks on the orbit structure of discrete approximations to chaotic maps," *Experimental Mathematics*, vol. 7, no. 4, pp. 317–324, 1998.
- [38] G. Yuan and J. A. Yorke, "Collapsing of chaos in one dimensional maps," *Physica D: Nonlinear Phenomena*, vol. 136, no. 1–2, pp. 18–30, 2000.
- [39] C. Dellago and W. G. Hoover, "Finite-precision stationary states at and away from equilibrium," *Physical Review E*, vol. 62, no. 5, pp. 6275–6281, 2000.
- [40] S. Li, X. Mou, and Y. Cai, "Improving security of a chaotic encryption approach," *Physics Letters A*, vol. 290, no. 3–4, pp. 127–133, 2001.
- [41] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, Oxford University Press on Demand, Oxford, UK, 2000.
- [42] A. Boyarsky and Y. S. Lou, "Approximating measures invariant under higher-dimensional chaotic transformations," *Journal of Approximation Theory*, vol. 65, no. 2, pp. 231–244, 1991.
- [43] C. E. Shannon, "Communication theory of secrecy systems*," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [44] M. F. Haroun and T. A. Gulliver, "A new 3D chaotic cipher for encrypting two data streams simultaneously," *Nonlinear Dynamics*, vol. 81, no. 3, pp. 1053–1066, 2015.
- [45] X. Wang and K. Guo, "A new image alternate encryption algorithm based on chaotic map," *Nonlinear Dynamics*, vol. 76, no. 4, pp. 1943–1950, 2014.
- [46] S. Som, S. Dutta, R. Singha, A. Kotal, and S. Palit, "Confusion and diffusion of color images with multiple chaotic maps and chaos-based pseudorandom binary number generator," *Nonlinear Dynamics*, vol. 80, no. 1–2, pp. 615–627, 2015.
- [47] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.
- [48] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *Plos One*, vol. 10, no. 3, 28 pages, Article ID e0119660, 2015.
- [49] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.
- [50] R. Rhouma, S. Meherzi, and S. Belghith, "OCML-based colour image encryption," *Chaos, Solitons & Fractals*, vol. 40, no. 1, pp. 309–318, 2009.
- [51] F. Chunlei and D. Qun, "A novel image encryption scheme based on self-synchronous chaotic stream cipher and wavelet transform," *Entropy*, vol. 20, no. 6, p. 13, 2018.
- [52] A. Vaish and M. Kumar, "Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain," *Optik*, vol. 145, pp. 273–283, 2017.
- [53] G. Bhatnagar, Q. M. J. Wu, and B. Raman, "Image and video encryption based on dual space-filling curves," *The Computer Journal*, vol. 55, no. 6, pp. 667–685, 2012.
- [54] H. A. Atee, R. Ahmad, N. M. Noor, A. M. S. Rahma, and M. S. Sallam, "A novel extreme learning machine-based cryptography system," *Security and Communication Networks*, vol. 9, no. 18, pp. 5472–5489, 2016.

- [55] N. A. Abbas, "Image encryption based on independent component analysis and arnold's cat map," *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 139–146, 2016.
- [56] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, no. 5, pp. 1137–1148, 2015.
- [57] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 995–1015, 2014.
- [58] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.
- [59] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.
- [60] M. Farajallah, S. E. Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *International Journal of Bifurcation & Chaos*, vol. 26, no. 2, p. 21, Article ID 1650021, 2016.
- [61] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11477–11489, Nov 2019.
- [62] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.