IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 15, 2021, accepted March 26, 2021, date of publication April 1, 2021, date of current version April 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3070350

2D-SCMCI Hyperchaotic Map for Image Encryption Algorithm

JILEI SUN
Department of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210000, China
Department of Information Engineering, Binzhou University, Binzhou 256600, China
e-mail: bzxysjl@163.com

ABSTRACT Chaos has unpredictability and initial condition sensitivity, which known as a best candidate for cryptography application. However, there are many defects for the existing chaotic cryptography systems due to the use of chaotic maps that without complexity dynamic properties. To overcome these weaknesses, this work designed a 2D-SCMCI hyperchaotic map based on Cascade Modulation Couple (CMC) and two 1D-chaotic map. The dynamic characteristics of the 2D-SCMCI hyperchaotic map are analyzed through attractor trajectory, 0-1 test, bifurcation diagram, Lyapunov exponents and spectrum entropy (SE) complexity. The results of analysis indicate that 2D-SCMCI hyperchaotic map has rich dynamic performance and randomness, which illustrates that it is more suitable for image encryption algorithm. Therefore, an image encryption algorithm is proposed by 2D-SCMCI hyperchaotic map. In encryption algorithm, the image is scrambled by row and column, forward and backward diffusion are used to diffuse image pixel values. The security performances analysis results indicate that the introduced algorithm has better security characteristics.

INDEX TERMS 2D-SCMCI hyperchaotic map, image encryption algorithm, dynamic characteristic, cryptographic analysis.

I. INTRODUCTION

At present, the digital information is transmitted and generated by all kinds of different network [1]. Digital image is an important information carrier and it is widely used as a data model. However, there are some national secrets and personal privacy in a large amount of digital images. Therefore, the protection of the image information security becomes an important research topic. To maintain the security of image information, the scholars have proposed many technologies, for instance, data hiding [2], encryption [3] and watermarking [4]. For these technologies, image encryption technology is the most direct methods to convert a visual original image into a noise image [5]. For an image encryption algorithm, it contains scrambling and diffusion parts [6]–[8]. The scrambling is a change in pixel position, while diffusion is a change in pixel value [9], [10].

So far, the use of chaotic image encryption algorithms have attracted more and more attentions. Chaotic is nonlinear, random, unpredictable. There are some special characteristics, for example, dense periodic orbits, initial value sensitivity and unpredictability [11]–[13]. So chaotic is more suitable for image encryption algorithm. Ever since an image encryption algorithm by 2D chaotic map was first designed by Fridrich [14], researchers have introduced various image encryption algorithms through chaotic system [15], [16], [16]–[33].

For the image encryption algorithm using chaotic maps, their security mainly depends on the complexity of chaotic system. For the existing chaotic maps, they have some defects, such as, chaotic degradation may occur on a platform with limited precision, whose output distribution is not uniform. Then they have not complexity dynamic, which their trajectories are estimated [34]. In addition, their range of chaotic is small, which will be subject to external interference and destroy chaotic characteristic [35]. What's more, researches indicate that some encryption schemes by existing chaotic maps are likely to be easily attacked [36].

Recently, some new chaotic maps are used in image encryption algorithm, their output trajectories are not distributed throughout the phase space and they have not complexity dynamic behaviors, which they generated chaotic sequences have not better randomness. To address this weakness, this study designed an 2D-SCMCI hyperchaotic map based on Cascade Modulation Couple (CMC) and two

The associate editor coordinating the review of this manuscript and approving it for publication was Jeon Gwanggil.

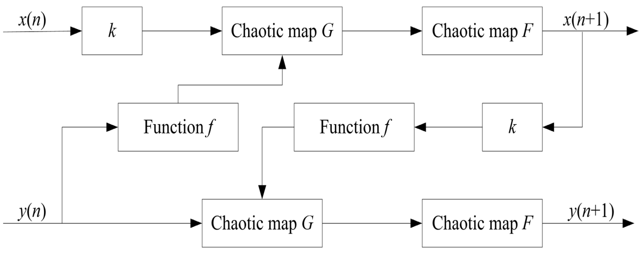


FIGURE 1. Schematic diagram of cascade modulation couple.

1D-chaotic map. And compared with complexity of the chaotic maps available today. In addition, using the 2D-SCMCI hyperchaotic map to introduced an image encryption algorithm.

This work is organized in the following. In section 2, the model of the 2D-SCMCI hyperchaotic map is introduced. The complexity dynamic behaviors of the 2D-SCMCI hyperchaotic map are analyzed in section 3. In section 4, image encryption algorithm using the 2D-SCMCI hyperchaotic map is described. The security characteristics of the algorithm are researched in section 5. In section 6, some conclusions are given.

II. THE MODEL OF THE 2D-SCMCI HYPERCHAOTIC MAP

A. THE PRINCIPLE CASCADE MODULATION COUPLE

Assuming that f is a linear function, and F and G denote two 1D chaotic maps, respectively, based on 1D cascade model [37] and closed-loop modulation couple model [38], Cascade Modulation Couple is proposed. The corresponding definition is

$$\begin{cases} x(n+1) = F(f(y(n)) \times G(kx(n))) \\ x(n+1) = F(f(kx(n+1)) \times G(y(n))) \end{cases} \tag{1}$$

where x and y mean that system variables, k represents modulation parameter. The schematic diagram of model as Fig. 1. In the Fig. 1, firstly, chaotic map G is modulated by linear function f, then the serves as input of chaotic map F, G and F are cascaded. In addition, system variables x and y are coupled 2D chaotic system through function f. The function f is named coupling function.

B. THE MODEL OF THE 2D-SCMCI HYPERCHAOTIC MAP

Based on the principle cascade modulation couple, setting the $f(x) = x + h$, chaotic map F is 1D-Sine chaotic map [39], G is 1D-Iterative chaotic map [40], then a 2D-SCMCI map is obtained, and its system equation is expressed by

$$\begin{cases} x(n+1) = rsin(\pi((y(n)+h)k\sin(\frac{a\pi}{x(n)}))) \\ y(n+1) = rsin(\pi((kx(n+1)+h)\sin(\frac{a\pi}{x(n)}))) \end{cases} \tag{2}$$

where k is modulation parameter, h, r and a represent the system parameters. $x(n)$ and $y(n)$ means that two values at step n.

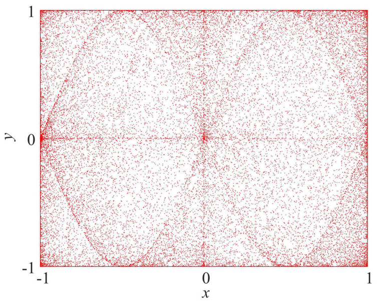


FIGURE 2. Attractor phase diagram of 2D-SCMC hyperchaotic map.

III. THE DYNAMIC ANALYSIS OF THE 2D-SCMCI HYPERCHAOTIC MAP

A. ATTRACTOR PHASE DIAGRAM

Setting the modulation parameters $k = 1$, system parameters $h = 2$, $r = 1$ and $a = 1$, initial value $x0 = 0.3$, $y0 = 0.4$. In this case, Lyapunov exponents of the 2D-SCMCI map are calculated as 3.7547 and 2.4832. The 2D-SCMCI map is hyperchaotic map due to it has two positive Lyapunov exponents. The attractor phase diagram of 2D-SCMCI hyperchaotic map is Fig. 2. As we can be seen in Fig. 2, the system is a universal attractor, which indicates that the 2D-SCMCI hyperchaotic map has good ergodicity. In addition, the attractors are relatively evenly distributed, which illustrate that the 2D-SCMCI hyperchaotic sequence has good randomness.

B. 0-1 TEST

0-1 test is proposed by Gottwald and Melbourne [41], it is an effective and reliable binary algorithm to check whether the system is chaos, its algorithm is described as follows:

For a discrete set of data $x(h)$, here, the sampling time is $(h = 1, 2, 3, \ldots.)$, which is the observable data of a one-dimensional dynamic system. Choosing an arbitrary constant $c \in R^+$, and the definition is

$$p(h) = \sum_{j=1}^{h} x(j)\cos(\theta(j)), \quad h = 1, 2, 3, \ldots \tag{3}$$

$$s(h) = \sum_{j=1}^{h} x(j)\cos(\theta(j)), \quad h = 1, 2, 3, \ldots \tag{4}$$

where

$$\theta(j) = jc + \sum_{j=1}^{h} x(j), \quad j = 1, 2, 3, \ldots n \tag{5}$$

According to the function $p(h)$ or $s(h)$, the root mean square displacement is defined by

$$M(h) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} [p(j+j-p(j))]^2 \tag{6}$$

where $h = 1, 2, 3, \ldots$

Obviously, it's bounded or linearly increasing over time, and in particular, if $p(h)$ $(s(h))$ is Brownian motion, which

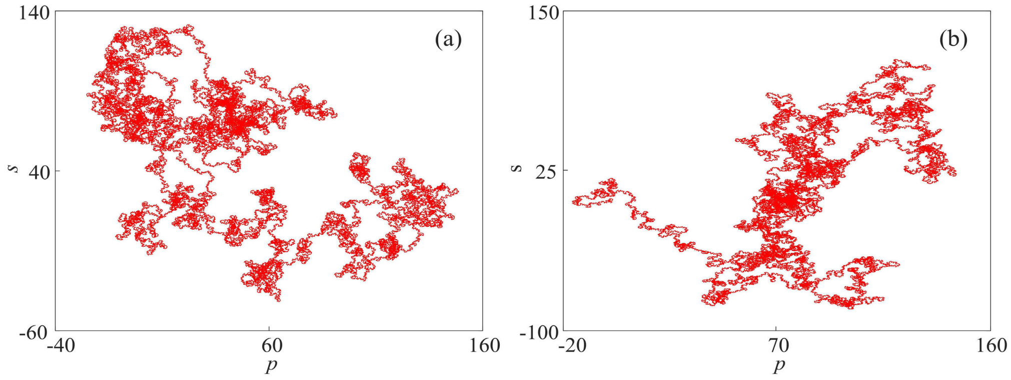


FIGURE 3. 0-1 test results, (a) x sequence, (b) y sequences.

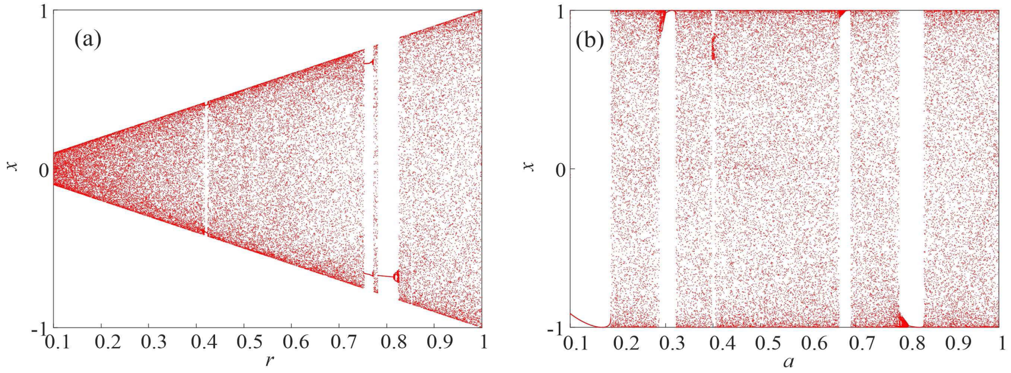


FIGURE 4. Bifurcation diagram, (a) $r \in [0.1, 1]$, (b) $a \in [0.1, 1]$.

means $M(h)$ is linearly increasing over time. If $p(h)$ ($s(h)$) is bounded, which means $M(h)$ is also bounded. Finally, its asynchronous growth rate should be examined by

$$K = \lim_{h\to\infty} \frac{\log M(h)}{\log h} \tag{7}$$

If K is close to 0, which means the motion is regular (periodic or quasi-periodic). If K is close to 1, which means the motion is chaos.

For the sequences of the 2D-SCMCI hyperchaotic map, when the modulation parameters $k = 1$, system parameters $h = 2$, $r = 1$ and $a = 1$, initial value $x0 = 0.3$, $y0 = 0.4$, the sequences are generated by the 2D-SCMCI hyperchaotic map to 0-1 test, and then we obtained test result of (p, s) diagram as Fig. 3. The result indicates that the sequence trajectories are similar to Brownian motion. Therefore, the 2D-SCMCI map is chaotic map.

C. BIFURCATION DIAGRAM

Bifurcation diagram is an intuitive and visual observation method to analyze the dynamic characteristic of chaotic systems. It is also a widely used method to evaluate chaotic system dynamics. Bifurcation diagrams of 2D-SCMCI hyperchaotic map with the parameters r and a are shown in Fig. 4. The Bifurcation diagrams indicate that the chaotic states of the 2D-SCMCI hyperchaotic map are distributed over large parameter range, and periodic states are distributed over a very small range. Therefore, the 2D-SCMCI hyperchaotic map has robust chaotic performance and the outputs of the system are more randomness.

D. LYAPUNOV EXPONENT

For the chaotic behaviors, the researchers have different views in different fields. However, Lyapunov exponent (LE) is generally accepted method for chaotic behavior analysis. The QR decomposition algorithm [42] is used to calculate the LE of the 2D-SCMCI hyperchaotic map, the corresponding definition is introduced in the following.

For the chaotic map $Hy(n)$, where

$$Hy(h) = \begin{cases} H_1 y_1(h) \\ H_1 y_2(h) \\ \vdots \\ H_n y_h(h) \end{cases} \tag{8}$$

where h represents the number of the chaotic map equations. Then, the Jacobian matrix of the chaotic map $Hy(h)$ is

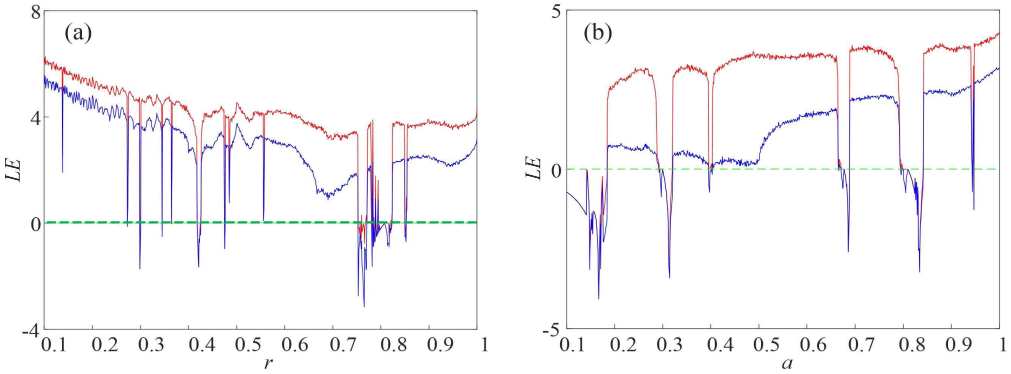


FIGURE 5. Lyapunov exponent, (a) $r \in [0.1, 1]$, (b) $a \in [0.1, 1]$.

TABLE 1. Dynamical behavior of the different parameter values.

Parameter	parameter range values	Lyapunov exponents	System states
r	$\{[0.1, 0.271], [0.276, 0.297], [0.302, 0.343], [0.347, 0.364], [0.366, 0.417]\}$	$+, +$	Hyperchaotic
	$\{[0.428, 0.474], [0.477, 0.752], [0.770, 0.783], [0.824, 0.85], [0.853, 1]\}$	$+, +$	Hyperchaotic
	$\{[0.272, 0.275], [0.298, 0.301], 0.365\}$	$+, 0$	Chaotic
	$\{[0.344, 0.346], [0.475, 0.476], [0.784, 0.794], [0.851, 0.852]\}$	$+, -$	Chaotic
	$\{[0.418, 0.427], [0.753, 0.769], [0.795, 0.823]\}$	$-, -$	Periodic
a	$\{[0.1, 0.184], [0.292, 0.231], [0.395, 0.401], [0.670, 0.688], [0.780, 0.842]\}$	$-, -$	Periodic
	[0.944, 0.945]	$+, -$	Chaotic
	$\{[0.185, 0.291], [0.232, 0.394], [0.402, 0.669], [0.89, 0.799], [0.843, 0.943], [0.946, 1]\}$	$+, +$	Hyperchaotic
k	[0, 1]	$+, +$	Hyperchaotic
h	[1, 2]	$+, +$	Hyperchaotic

obtained by

$$J = \begin{vmatrix} \frac{\partial H_1 y_1(h)}{dy_1} & \frac{\partial H_1 y_1(h)}{dy_2} & \cdots & \frac{\partial H_1 y_1(h)}{dy_h} \\ \frac{\partial H_1 y_2(h)}{dy_2} & \frac{\partial H_2 y_2(h)}{dy_2} & \cdots & \frac{\partial H_2 y_2(h)}{dy_h} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial H_h y(h)}{dy_2} & \frac{\partial H_1 y(h)}{dy_2} & \cdots & \frac{\partial H_n y_h(h)}{dy_h} \end{vmatrix} \tag{9}$$

Then, the results of Jacobian matrix J and QR decomposition algorithm is

$$\begin{aligned} qr(J_m J_{m-1} \cdots J_1) &= qr(J_m J_{m-1} \cdots J_2(J_1 Q_0)) \\ &= qr(J_m J_{m-1} \cdots J_3(J_2 Q_1))R_1 \\ &= \cdots \\ &= qr(J_m J_{m-1} \cdots J_i(J_{i-1} Q_{i-2})) \\ &\quad R_{i-2} \cdots R_1 \\ &= \cdots \\ &= Q_m R_m \cdots Q_1 R_1 \end{aligned} \tag{10}$$

where $qr(.)$ indicates the QR decomposition function, m is the number of iteration. Then LE of the chaotic map is calculated by

$$LE_k = \frac{1}{m} \sum_{i}^{m} \ln |R_i(k, k)| \tag{11}$$

The LE of 2D-SCMCI hyperchaotic map is calculated by QR decomposition algorithm, the LE results as Fig. 5. The results in Fig. 5 indicate that the 2D-SCMCI hyperchaotic map has two positive LE values in large parameter rang, only has a few parameter range is periodic states. Therefore, the 2D-SCMCI hyperchaotic map has more complexity dynamic behavior. The corresponding results are listed in Table. 1

E. COMPLEXITY ANALYSIS

Complexity is a measure to analyze randomness of the chaotic sequence. The higher complexity value, means that the sequence is closer to a random sequence, and application system security is also higher. In this experiments, Spectral Entropy (SE) complexity algorithm is used to calculate complexity of the 2D-SCMCI hyperchaotic sequence. The SE value is obtained through the energy distribution in the Fourier transform domain and Shannon entropy. The algorithm process is given in the following.

For the chaotic pseudo-random sequence $y(n), n = 0, 1, 2, \ldots, M-1$ with the length of M, it is calculated through

$$y(n) = y(n) - \frac{1}{M} \sum_{n=0}^{M-1} y(n) \tag{12}$$

Then the sequence $y(n)$ is discrete fourier calculated by

$$Y(h) = \sum_{n=0}^{N-1} y(n)^{-j\frac{2\pi}{M}nh} = \sum_{n=0}^{M-1} y(n) W_M^{nh} \tag{13}$$

where $h = 0, 1, 2, \ldots, M-1$.

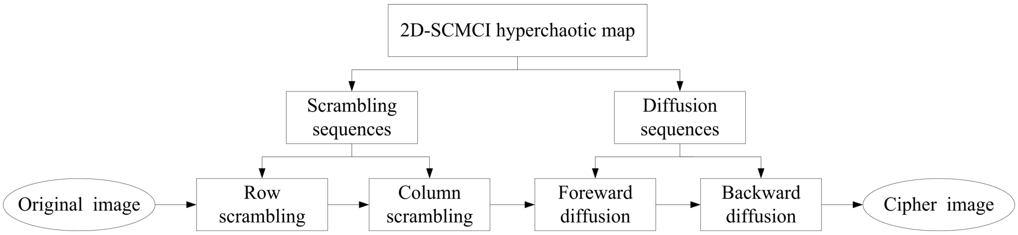


FIGURE 6. The flowchart of the proposed encryption algorithm.

TABLE 2. SE complexity values of the different chaotic maps.

System	Parameter	SE_1	SE_2	SE_3	$\overline{SE}$	Rank
2D-SCMCI	$r = 1, a = 1, k = 1, h = 2$	0.927	0.931	0.928	0.928	1
Grid sinusoidal cavity [43]	$\omega = \pi, a = 1, c = 50$	0.915	0.886	0.881	0.894	2
2D-SLMM [39]	$a = 1$	0.812	0.819	0.705	0.779	3
2D-LASM [39]	$\mu = 1$	0..363	0.363	0.375	0.367	5
Sine [39]	$a_0 = 1, \omega = \pi$	0.868	0.871	0.859	0.866	4

TABLE 3. PE complexity values of the different chaotic maps.

System	Parameter	PE_1	PE_2	PE_3	$\overline{PE}$	Rank
2D-SCMCI	$r = 1, a = 1, k = 1, h = 2$	0.979	0.976	0.974	0.976	1
2D-SLMM [39]	$\alpha = 1$	0.721	0.727	0.748	0.722	2
2D-Logistic [44]	$r = 1.18$	0.652	0.644	0.645	0.647	5
Logistic [44]	$u = 4$	0.678	0.680	0.680	0.679	3
Sine [39]	$a_0 = 1, \omega = \pi$	0.672	0.666	0.669	0.669	4

Based on Paserval theorem, for the sequence $Y(h)$, its half is selected to calculate the relative power spectrum. Then power spectrum value of the frequency point is

$$p(h) = \frac{1}{M}|Y(h)|^2 \tag{14}$$

where $h = 0, 1, 2, \ldots, M/2 - 1$. The all power is

$$p_{tot}(h) = \frac{1}{M}\sum_{h=0}^{M/2-1}|Y(h)|^2 \tag{15}$$

Then the relative power spectrum probability P_h is calculated by

$$P_h = \frac{p(h)}{p_{tot}} = \frac{\frac{1}{M}|Y(h)|^2}{\frac{1}{M}\sum\limits_{h=0}^{M/2-1}|Y(h)|^2} = \frac{|Y(h)|^2}{\sum\limits_{h=0}^{M/2-1}|Y(h)|^2} \tag{16}$$

The *se* of signal can be calculated by the relative power spectrum probability P_h and Shannon entropy.

$$se = -\sum_{h=0}^{M/2-1} P_h \ln P_h \tag{17}$$

Finally, the *se* is normalized, and then SE complexity is

$$SE(N) = \frac{se}{\ln(M/2)} \tag{18}$$

For the different initial values, SE complexity values of the others chaotic maps are listed in Table. 2. In addition, PE complexity values of the others chaotic maps are listed in Table. 3. The complexity results in Table indicate that the complexity value of the 2D-SCMCI hyperchaotic map is the largest. Therefore, the sequence of the 2D-SCMCI hyperchaotic map has better randomness.

IV. IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

A. ENCRYPTION ALGORITHM

An image encryption algorithm is introduced by 2D-SCMCI hyperchaotic map. The flowchart of the designed encryption algorithm as Fig.6. The process of encryption is described in the following.

- Step 1: A plain-image I of size $M \times N$ is read.
- Step 2: Giving the initial and parameter values of the 2D-SCMCI hyperchaotic map, then the 2D-SCMCI hyperchaotic map is iterated $(m + H)$ times, here $H = max(M, N)$. Two chaotic sequences x and y of length $(m + H)$ are obtained.
- Step 3: To get the more stable chaotic sequences, for the sequences x and y, theirs the first m values are discarded. Two chaotic sequences X and Y of length M and N are obtained.
- Step 4: Based on chaotic sequences x and y, two vectors r and c are obtained by

$$\begin{cases} r = \text{mod}(\text{floor}(|x(i)| \times 10^{16}), \dfrac{M}{2}) \\ c = \text{mod}(\text{floor}(|y(i)| \times 10^{16}), \dfrac{N}{2}) \end{cases} \tag{19}$$

- Step 5: Using chaotic sequences X and vector r, The image I is row scrambled. The scrambling principle as Fig. 7. Here, the row length of the image is 8, $r = 3$, the row is divided into red and green, if $X > 0$,

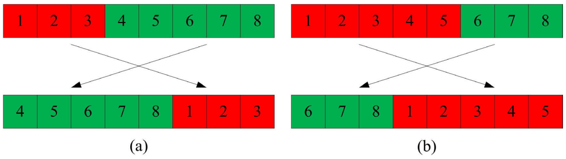


FIGURE 7. The principle of the scrambling algorithm.

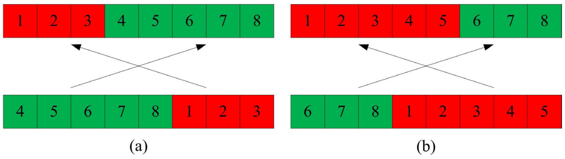


FIGURE 8. The inverse of scrambling principle.

the scrambling is Fig. 7 a, if $X < 0$, the scrambling is Fig. 7 b.

- Step 6: According to the scrambling principle in Fig. 7, chaotic sequences Y and vector c, the scrambled result is column scrambled.
- Step 7: The parameter values and initial values of the 2D-SCMCI hyperchaotic map are given, then the 2D-SCMCI hyperchaotic map is iterated $(n+M\times N)$ times. We obtained the sequences x and y of length $(n+M\times N)$.
- Step 8: To get the more stable chaotic sequences, for the chaotic sequences x and y, theirs the first n values are discarded. Two sequences x and y are operated by

$$\begin{cases} x_g(i) = \mathrm{mod}(\mathrm{round}(1000(\left|x(i)\times 10^{16}\right| \\ -\mathrm{floor}(|x(i)|\times 10^{16}))), 256) \\ y_g(i) = \mathrm{mod}(\mathrm{round}(1000(\left|y(i)\times 10^{16}\right| \\ -\mathrm{floor}(|y(i)|\times 10^{16}))), 256) \end{cases} \tag{20}$$

- Step 9: Based on chaotic sequences x_g and y_g, two matrixes $S1$ and $S2$ are obtained. And then the scrambled result is diffused.
- Step 10: Forward diffusion:

$$\begin{cases} F(1,1) = \mathrm{mod}(D(1,1)+S1(1,1), 256) \\ F(1,j) = \mathrm{mod}(D(1,j)+S1(1,j) \\ +F(1,j-1), 256) \\ F(i,1) = \mathrm{mod}(D(i,1)+S1(i,1) \\ +F(i-1,1), 256) \\ F(i,j) = \mathrm{mod}(D(i,j)+S1(i,j) \\ +F(i,j-1)+A(i-1,j), 256) \end{cases} \tag{21}$$

where F means diffusion result, D is scrambled result in step 6, $i = 2, 3, 4, \ldots M, j = 2, 3, 4, \ldots N$.

- Step 11: Backward diffusion:

$$\begin{cases} C(M,N) = \mathrm{mod}(F(M,N)+S2(M,N), 256) \\ C(M,j) = \mathrm{mod}(F(M,j)+S2(M,j) \\ +C(M,j+1), 256) \\ C(i,N) = \mathrm{mod}(F(i,N)+S2(i,N) \\ +C(i+1,N), 256) \\ C(i,j) = \mathrm{mod}(F(i,j)+S2(i,j) \\ +C(i,j+1)+C(i+1,j), 256) \end{cases} \tag{22}$$

where F is forward diffusion result, C represents backward diffusion result, $i = M, M-1, M-2, \ldots 2$, $j = N, N-1, N-2, \ldots 2$.

- Step 12: The final diffusion matrix C obtained by the above operation is cipher image.

B. DECRYPTION ALGORITHM

The decryption process refers to the inverse of the encryption process, its main process is described in the following.

- Step 1: Inputting the cipher image.
- Step 2: The matrixes $S1$ and $S2$ are obtained as in step 6∼9 in encryption algorithm.
- Step 3: Inverse of backward diffusion:

$$\begin{cases} C(M,N)=\mathrm{mod}(768+T(M,N)-S2(M,N), 256) \\ C(M,j) = \mathrm{mod}(512+T(M,j)-S2(M,j) \\ -C(M,j+1), 256) \\ C(i,N) = \mathrm{mod}(512+T(i,N)-S2(i,N) \\ -C(i+1,N), 256) \\ C(i,j) = \mathrm{mod}(768+T(i,j)-S2(i,j) \\ -C(i,j+1)-C(i+1,j), 256) \end{cases} \tag{23}$$

where T is cipher image, C means inverse backward diffusion result, $i = M, M-1, M-2, \ldots 2, j = N$, $N-1, N-2, \ldots 2$.

- Step 4: Inverse of forward diffusion:

$$\begin{cases} A(1,1) = \mathrm{mod}(768+C(1,1)-S1(1,1), 256) \\ A(1,j) = \mathrm{mod}(512+C(1,j)-S1(1,j) \\ -A(1,j-1), 256) \\ A(i,1) = \mathrm{mod}(512+C(i,1)-S1(i,1) \\ -A(i-1,1), 256) \\ A(i,j) = \mathrm{mod}(768+C(i,j)-S1(i,j) \\ -A(i,j-1)-A(i-1,j), 256) \end{cases} \tag{24}$$

where A is inverse of forward diffusion result, $i = 2, 3, 4, \ldots M, j = 2, 3, 4, \ldots N$.

- Step 5: The vectors r and c, chaotic sequences XX and YY are generated as step 2∼4 of the encryption algorithm.
- Step 6: Using chaotic sequences XX and vector r, inverse of row scrambling is operated. The scrambling principle as Fig. 8. Here, the row length of the image is 8, $r = 3$, the row is divided into red and green, if $XX < 0$, the inverse of row scrambling is Fig. 8 a, if $XX > 0$, the inverse of row scrambling is Fig. 8 b.
- Step 7: Inverse of scrambling is operated, and then the decryption image is obtained.

V. SIMULATION AND SECURITY ANALYSIS OF ENCRYPTION ALGORITHM

In the experiment, to confirm the security of the designed encryption algorithm, using MATLAB R2018a software

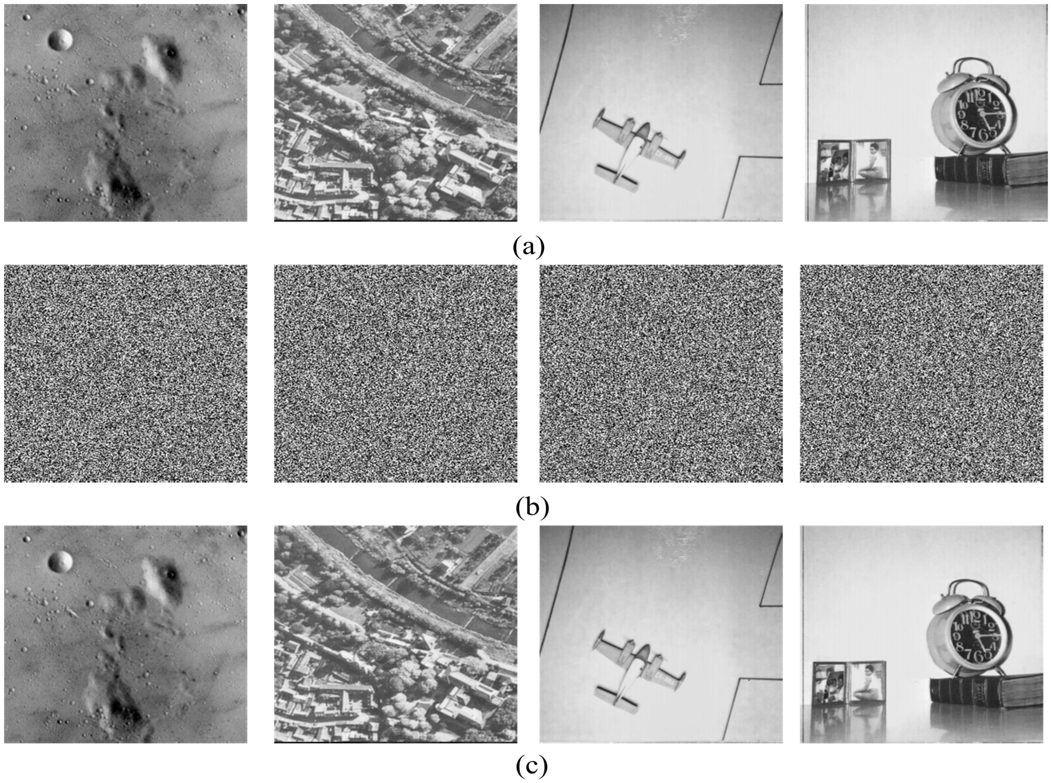


FIGURE 9. Simulation results, (a) Original images 5.1.09 ~ 5.1.12, (b) Cipher images 5.1.09 ~ 5.1.12, (c) Decryption images 5.1.09 ~ 5.1.12.

platform, the introduced algorithm is simulated numerically. The original images use the size of 256 × 256 and 8-bit standard 5.1.09 ∼ 5.1.12 images.

A. SIMULATION RESULTS

Setting the parameters and initial values of the 2D-SCMCI hyperchaotic map $k = 1$, $h = 2$, $r = 1$ and $a = 1$, initial value $x0 = 0.3$, $y0 = 0.4$, the number of iterations $m = 5000$, $n = 4000$. Then the image encryption algorithm is operated on MATLAB software, the corresponding results are Fig. 9. The original images 5.1.09 ∼ 5.1.12 as Fig. 9 (a), the corresponding cipher image as Fig. 9 (b), decryption image as Fig. 9 (c). The results in Fig. 9 indicate that all the cipher images are disorganized and have no obvious texture, which illustrates that the designed encryption algorithm is feasible.

B. KEY SPACE

For the encryption system, it should have enough secret key space to effective against exhaustive attacks. In particular, encryption and decryption is very fast cryptographic system, the key space is greater than 128b. In our algorithm, the key has parameters of the 2D-SCMCI hyperchaotic map k, h, r and a, initial values $x0$ and $y0$. The experiment shows that the parameter effective range is 10^{-15}, initial value effective range is 10^{-16}. Therefore, the key space is $\log_2^{10^{60}+10^{32}} \approx 199$b, it is greater than 128b, which means that the designed algorithm can resist exhaustive attacks.

C. KEY SENSITIVITY

Key sensitivity means that if the encryption key is different, it will produce different cipher image, similarly, if the decryption key is different, decrypted results of the same cipher image will also different. A good encryption algorithm for the sensitivity of key is very important. The key sensitivity shows that the algorithm resist choose plaintext or ciphertext attacks. The smaller the key sensitivity is, the better the algorithm is against select plaintext or ciphertext attacks. To test the key sensitivity of the designed algorithm, the encryption key and decryption key are changed 10^{-15}, 5.1.09 image is used to test, the corresponding result is shown in Fig. 10. The result illustrates that the designed encryption scheme is very sensitivity for its key, and it can against select plaintext or ciphertext attacks.

D. INFORMATION ENTROPY

Information entropy main reflects uncertainty of image information, it reflects pixel value distribution of image. The greater the value of image information entropy, the more uniform the distribution of image gray value is. The less visible the relationship between pixels, the less easily the image information can be deciphered. According to Shannon

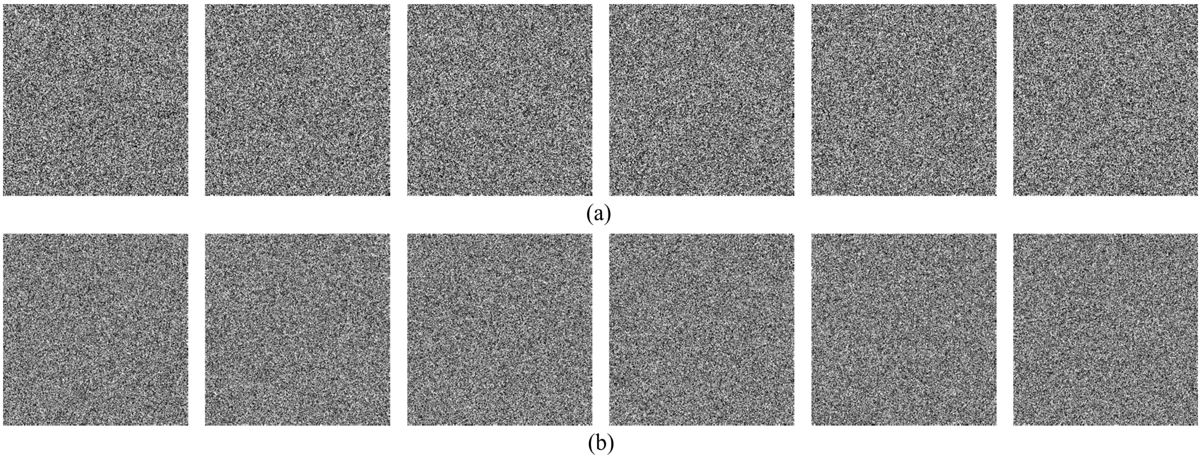


FIGURE 10. Key sensitivity, (a) Encryption key changed 10^{-15}, (b) Decryption key changed 10^{-15}.

TABLE 4. Information entropy values of images.

Images	5.1.09	5.1.010	5.1.11	5.1.12
Original image	6.7093	7.3188	6.4523	6.7057
Cipher image	7.9974	7.9970	7.9971	7.9968

TABLE 5. Comparison of information entropy with existing algorithms.

Images	Ours	Algorithm [16]	Algorithm [17]	Algorithm [18]
Camera	**7.9973**	7.9948	7.4740	7.9938
Couple	**7.9972**	7.9953	7.4101	7.9937
Boat	**7.9973**	7.9956	7.4232	7.9944
Lake	**7.9968**	7.9948	7.7877	7.9939

principle, the information entropy is calculated by

$$H = -\sum_{i=0}^{n} p(x_i) \log_2^{p(x_i)} \tag{25}$$

where n represents image gray level number, $p(x_i)$ is the number of the gray value (x_i). If the probability of all gray values is exactly the same, the maximum value of information entropy reaches 8. In this experiment, the information entropy of 5.1.09 $\sim$ 5.1.12 images and cipher images are calculated, the results are listed in Table. 4. The data in Table. 4 illustrate that information entropy values of cipher image are close to 8, so the cipher images have better randomness. In addition, information entropy of Couple, Camera, Lake and Boat are calculated, and compared results with existing algorithms [16]–[18] are shown in Table. 5. The results in Table. 5 indicate that the designed scheme encrypts cipher images with more randomness.

E. GRAY HISTOGRAM

Gray histogram reflects the distribution of image gray values. For cipher image, its distribution of gray histogram should be uniform, and compared with the histogram distribution of the original image, there are significant differences. Fig. 11 means that gray histogram of plaintext image, gray histogram of cipher image and gray histogram of decryption image. The result indicates that the gray histogram distribution of cipher image is almost uniform, which illustrates that the designed algorithm can resist powerful attack of statistical analysis.

F. CORRELATION OF ADJACENT PIXELS

Correlation of adjacent pixels is an important method to measure encryption algorithm. First, 2000 pairs of adjacent pixels are randomly selected from the original and cipher images to analyze the correlation, and then the correlation coefficients were calculated from horizontal (H), vertical (V) and diagonal (D) directions. The calculation formula of correlation coefficient as

$$\begin{cases} E(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} [x_i - E(x)]^2 \\ \mathrm{Conv}(x, y) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \\ R_{xy} = \dfrac{\mathrm{Conv}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases} \tag{26}$$

where x and y represent the gray value of adjacent pixels in image.

Correlation coefficients distributions between adjacent pixels of the plaintext images and encrypted images in H, V and D directions are Fig. 12 and Fig. 13. The results indicate that the correlations between adjacent pixels of plaintext image in all directions have certain relationship, the correlations between adjacent pixels of cipher images are evenly distributed across the entire pixel space, so between adjacent pixels of cipher image in all directions are no correlations. In addition, Table. 6 indicates that correlation coefficients of the original images are close to 1, correlation coefficients of the cipher images are close to 0, which further demonstrates that the designed algorithm destroys the correlation between adjacent pixels of original images. In addition, the correlation coefficients of

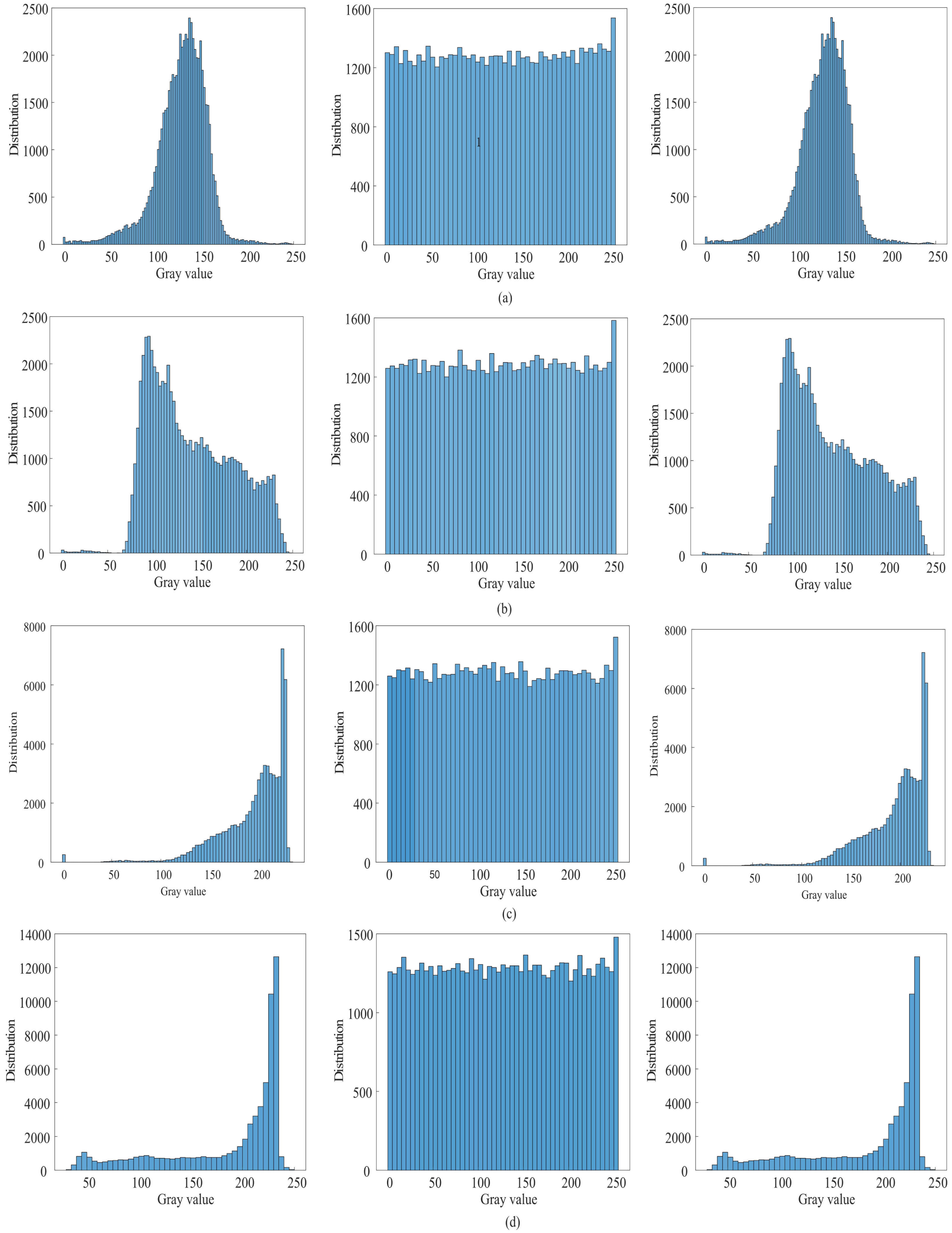


FIGURE 11. Gray histogram, (a) 5.1.09 image, (b) 5.1.10 image, (c) 5.1.11 image, (d) 5.1.12 image.

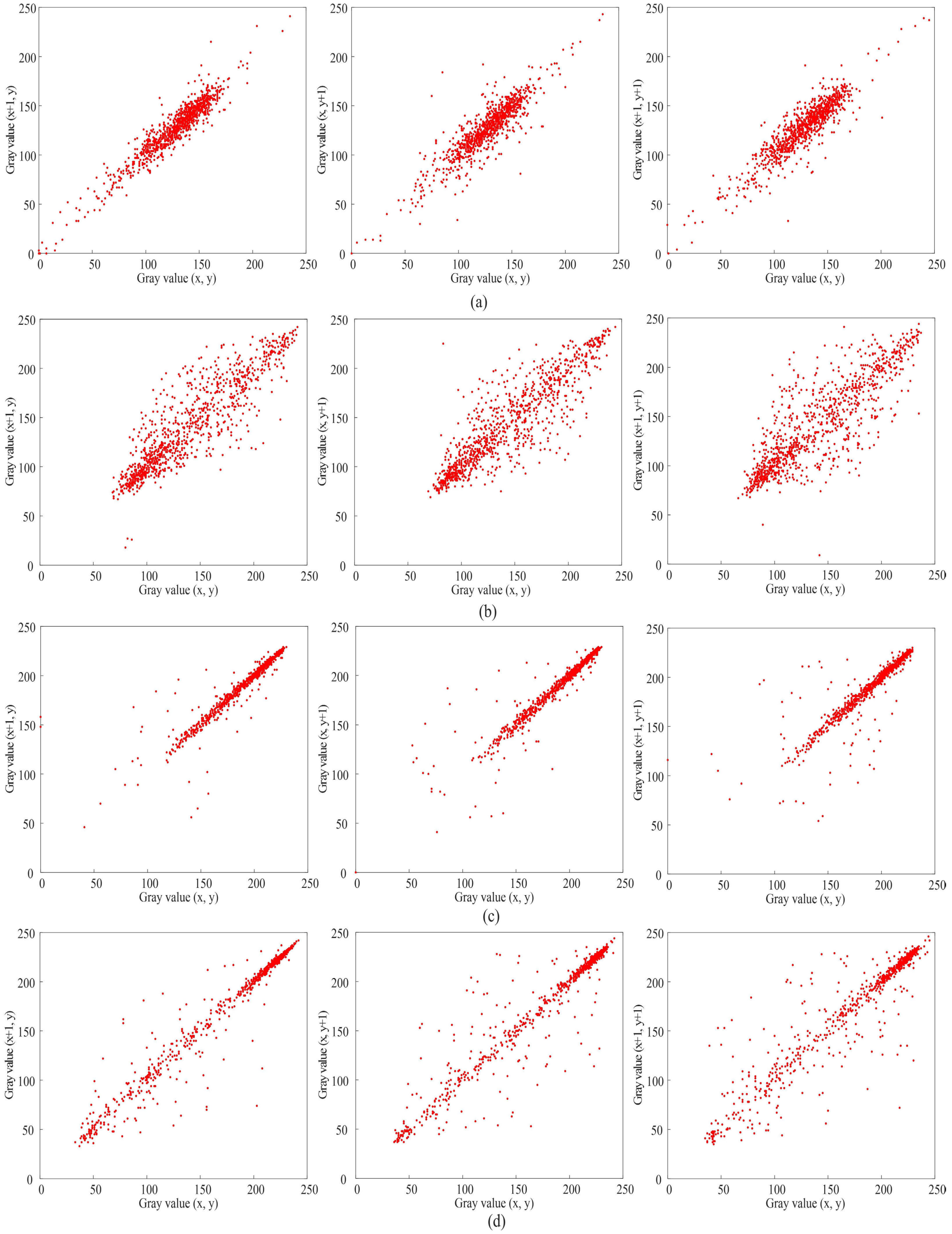
the Couple, Camera, Lake and Boat images are compared with other algorithms [15]–[20], [45], [46] in Table. 7. The results show that the designed algorithm has better encryption effect.

G. DIFFERENTIAL ATTACKS

The ability of the differential attack is tested through unified average changing intensity (UACI) and the number of pixels change rate (NPCR), their calculation formula is

TABLE 6. Correlation coefficients of different images.

Images	Plaintext image			Cipher image		
	H	V	D	H	V	D
5.1.09	0.9389	0.9025	0.9021	-0.0009	0.0025	0.0011
5.1.10	0.8662	0.9048	0.8288	-0.0025	0.0025	-0.0042
5.1.11	0.9526	0.9537	0.9059	-0.0015	0.0001	-0.0074
5.1.12	0.9743	0.9571	0.9399	0.0015	-0.0038	-0.0011



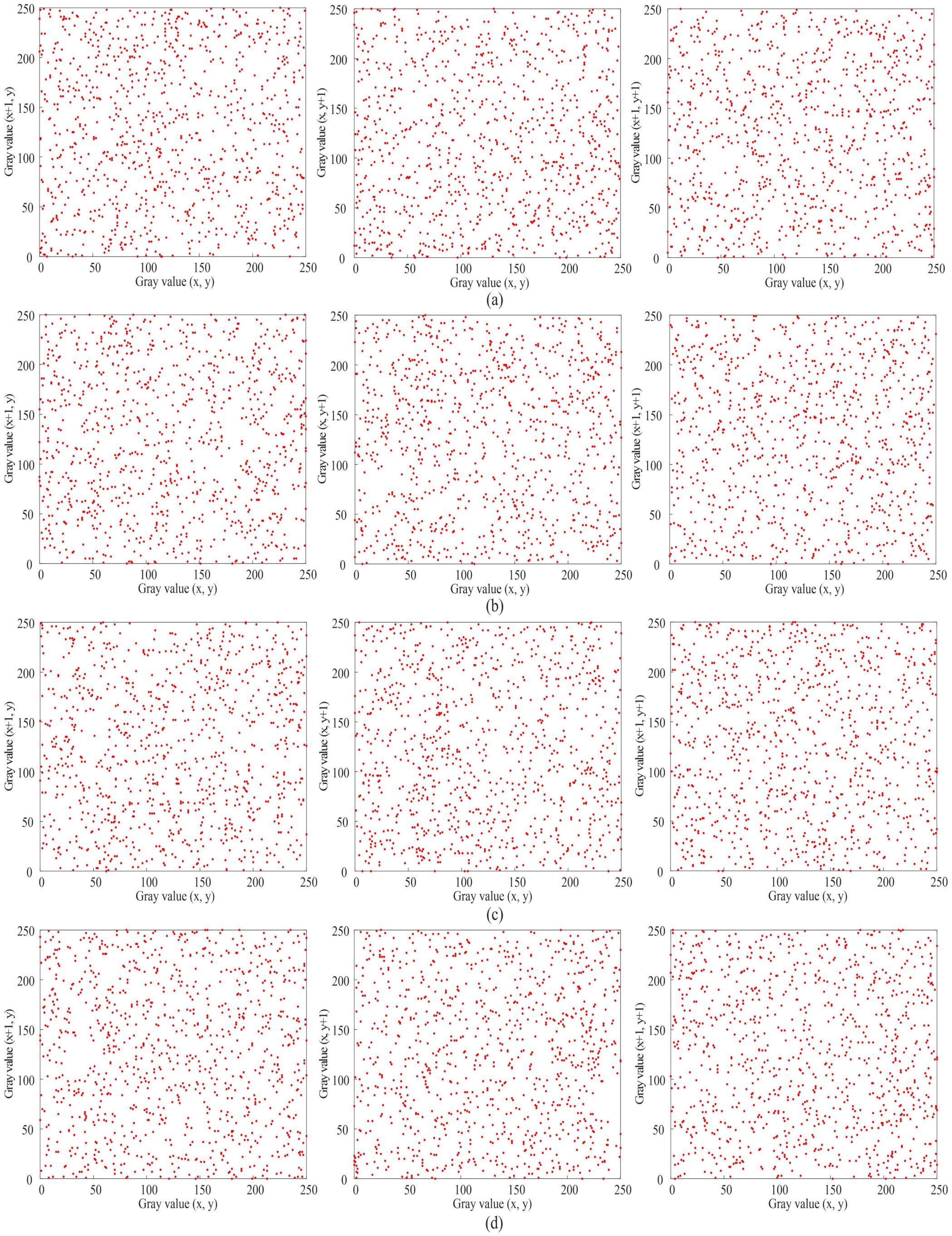
(a)

(b)

(c)

(d)

FIGURE 12. Correlation coefficients distribution between adjacent pixels in horizontal, vertical and diagonal directions of the original images, (a) 5.1.09 image, (b) 5.1.10 image, (c) 5.1.11 image, (d) 5.1.12 image.



(a)

(b)

(c)

(d)

FIGURE 13. Correlation coefficients distributions between adjacent pixels in horizontal, vertical and diagonal directions of the cipher images, (a) 5.1.09 image, (b) 5.1.10 image, (c) 5.1.11 image, (d) 5.1.12 image.

described by

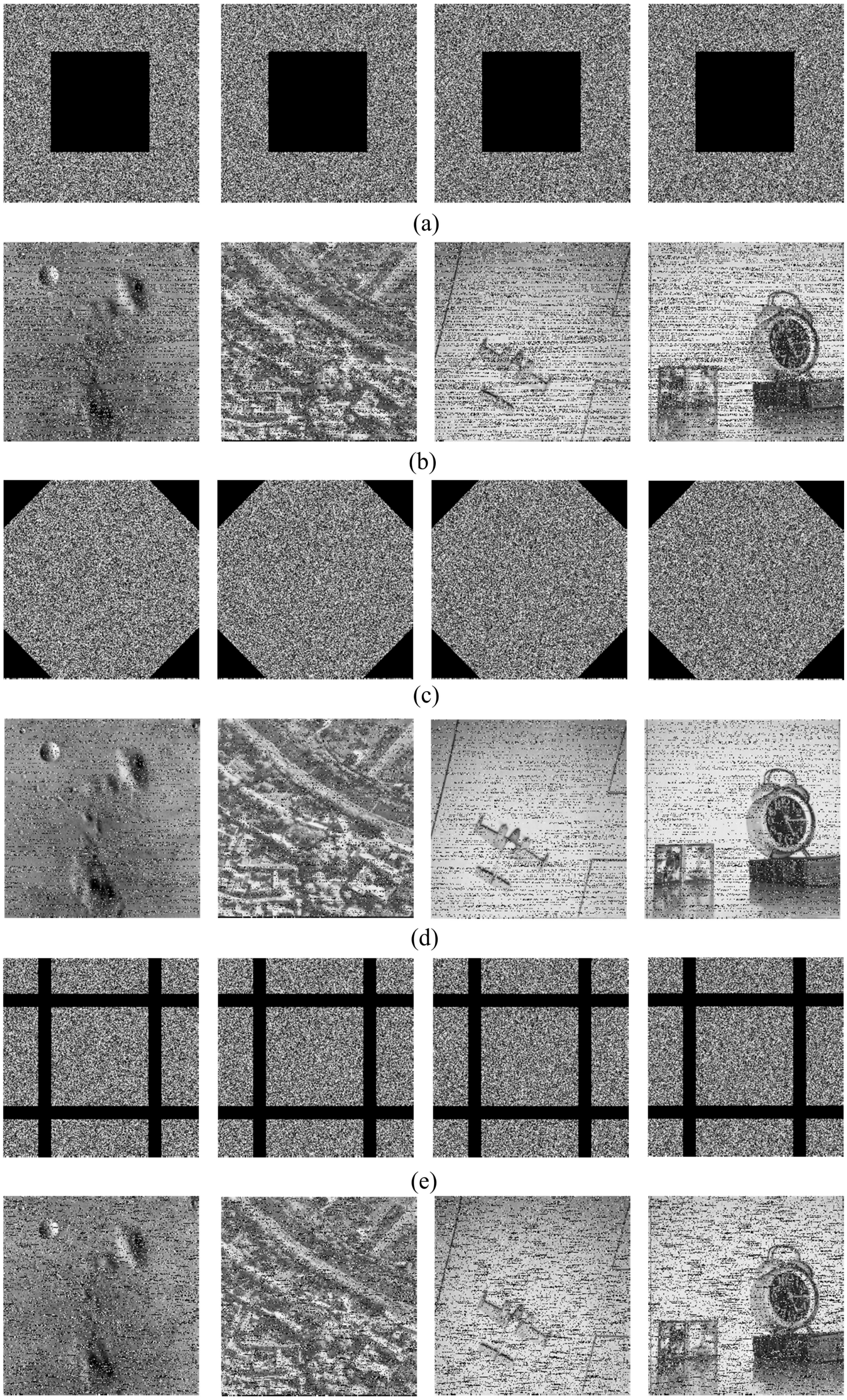
$$\begin{cases} \text{UPCR} = \sum_{i,j} \dfrac{D(i,j)}{M \times N} \times 100\% \\ \text{UACI} = \sum_{i,j} \dfrac{\left|C(i,j) - C'(i,j)\right|}{255 \times M \times N} \times 100\% \end{cases} \tag{27}$$

$$D(i,j) = \begin{cases} 0, C(i,j) = C'(i,j) \\ 1, C(i,j) \neq C'(i,j) \end{cases} \tag{28}$$

where the pixel value of the cipher image is $C(i, j)$. The pixel value of the cipher image in which the original image changes the pixel value is $C'(i, j)$.

Recently, the ideal values of NPCR and UACI are proposed by Wu and Noonan [47]. For a significance level is α, its critical NPCR value N_α^* is

$$N_\alpha^* = \frac{F - \Phi^{-1}(\alpha)\sqrt{F/L}}{F + 1} \tag{29}$$



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 14. Data loss analysis, (a), (c) and (e) are cipher image of lost date, (b), (d) and (f) are restored cipher image of lost date.

In general, when the NPCR > N_{α}^{*}, which show that it can prevent differential attack. If the significance level is α, the critical UACI values ($U_{\alpha}^{*}-$, $U_{\alpha}^{*}+$) are calculated by

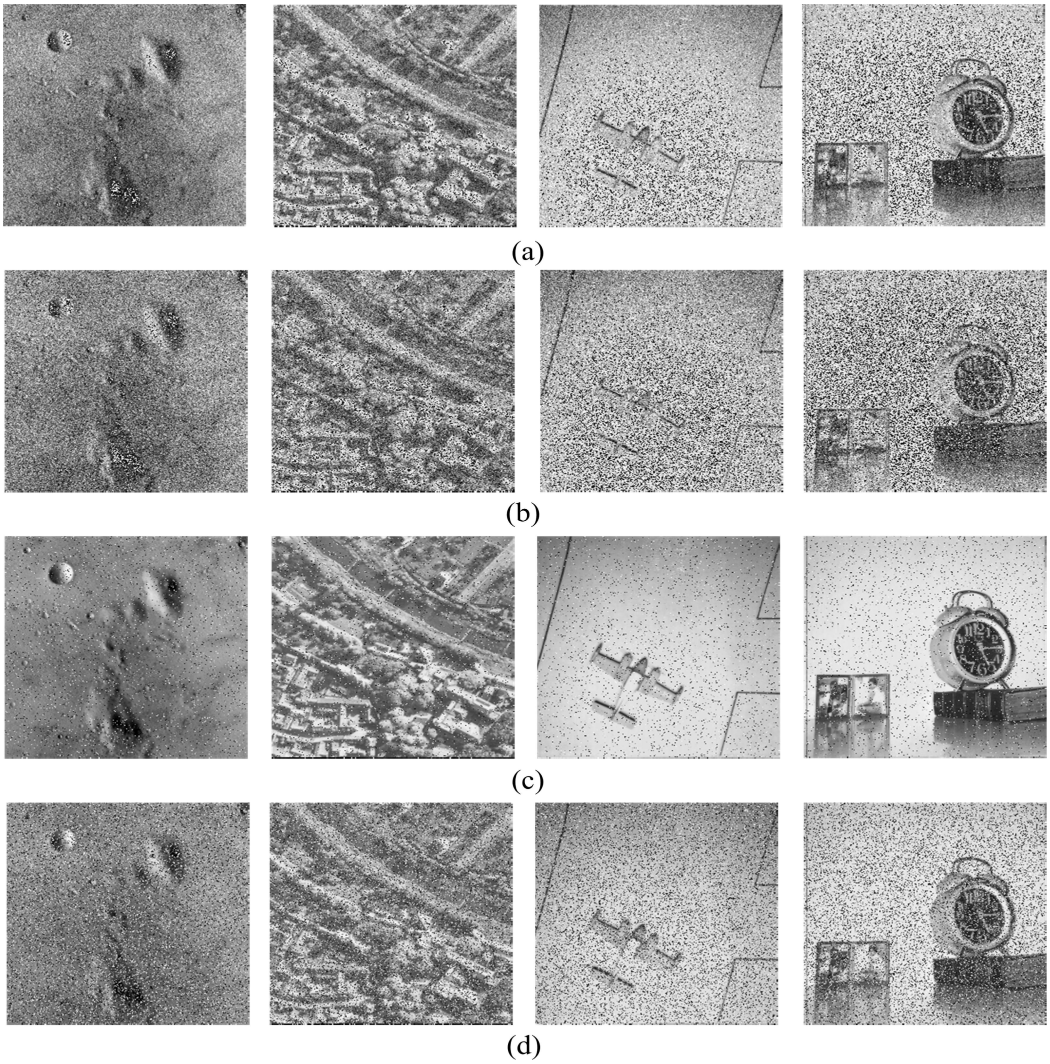
$$\begin{cases} U_{\alpha}^{*-} = \mu_u - \Phi^{-1}(\alpha/2)\sigma_u \\ U_{\alpha}^{*+} = \mu_u + \Phi^{-1}(\alpha/2)\sigma_u \end{cases} \tag{30}$$

where

$$\mu_u = \frac{F+2}{3F+3} \tag{31}$$

and

$$\sigma_u = \frac{(F+2)(F^2+2F+3)}{18(F+1)^2 FL} \tag{32}$$


(a)

(b)

(c)

(d)

FIGURE 15. **Noise test results, (a) Gaussian noise test results with mean 0.01, variance 0.001, (b) Gaussian noise test results with mean 0.01, variance 0.002, (c) The test results of Pepper and Salt noise with intensity of 0.01, (d) The test results of Pepper and Salt noise with intensity of 0.05.**

TABLE 7. **Correlation coefficients of the existing algorithms.**

Algorithm	Images	H	V	D
Ours	Cipher image "Couple"	**0.0065**	**-0.0051**	**-0.0027**
Algorithm [15]		0.0086	0.0060	0.0017
Algorithm [16]		-0.0382	0.0083	0.0277
Algorithm [17]		0.1539	0.1342	-0.0029
Algorithm [18]		-0.0290	-0.0166	0.0281
Ours	Cipher image "Camera"	**0.0027**	**-0.0002**	**0.0035**
Algorithm [19]		0.0079	-0.0005	-0.0044
Algorithm [45]		-0.0264	0.26375	0.0272
Algorithm [46]		0.0341	-0.0509	-0.0216
Algorithm [20]		0.0685	0.0821	0.0821
Ours	Cipher image "Lake"	**0.0018**	**0.0035**	**0.0005**
Algorithm [19]		-0.0012	0.0095	-0.0093
Algorithm [45]		-0.0306	0.3188	-0.0137
Algorithm [46]		0.0600	0.0196	-0.0231
Algorithm [20]		0.2071	0.2128	0.2102
Ours	Cipher image "Boat"	**0.0065**	**-0.0031**	**0.0019**
Algorithm [15]		0.0086	0.0060	0.0017
Algorithm [16]		0.0250	0.0186	-0.0051
Algorithm [17]		0.1830	0.1316	0.0599
Algorithm [18]		-0.0037	-0.0177	-0.0131

If $U_{\alpha}^{*-} < UACI_{test} < U_{\alpha}^{*+}$, which indicates that algorithm pass test and prevent differential attack. The ideal values of the different size of image [47] are obtained in Table 8.

In this test, we randomly changed and selected the pixel of original image. For the "5.1.09 5.1.14" of images are calculated 200 times, the mean values of NPCR and UACI are listed in Table 9 and Table 10. For the "Couple", "Camera", "Lake" and "Boat", the comparison results between them and existing encryption schemes [16], [17], [19], [21] as Table 11 and Table 12. The results indicate that the designed algorithm has ability to resist differential attacks.

H. DATA LOSS

Information is vulnerable to data loss during transmission or storage, so it is very important that analysis algorithm to resist the ability of data loss. For this experimental, the cipher image is lost to different degrees of data, and then the decryption algorithm is used to restore the operation. The test results are Fig. 14. The results indicate that the designed algorithm can prevent data loss to some extent.

TABLE 8. The ideal values of NPCR and UACI.

Images size	NPCR (%)			UACI(%)		
	$N^*_{0.05}$	$N^*_{0.01}$	$N^*_{0.001}$	$(U^{*-}_{0.05}, U^{*+}_{0.05})$	$(U^{*-}_{0.01}, U^{*+}_{0.01})$	$(U^{*-}_{0.001}, U^{*+}_{0.001})$
256 × 256	99.5693	99.5527	99.5341	(33.2824, 33.6447)	(33.2255, 33.7016)	(33.1594, 33.7677)
512 × 512	99.5893	99.5810	99.5717	(33.3730, 33.5541)	(33.3445, 33.5826)	(33.3115, 33.6156)
1024 × 1024	99.5994	99.5952	99.5906	(33.4183, 33.5088)	(33.4040, 33.5231)	(33.3875, 33.5396)

TABLE 9. NPCR test value.

Images	$NPCR_{Min}(\%)$	$NPCR_{Max}(\%)$	$NPCR_{Mean}(\%)$	Critical NPCR(%)		
				$N^*_{0.05} = 99.5693\%$	$N^*_{0.01} = 99.5527\%$	$N^*_{0.001} = 99.5341\%$
5.1.09	99.65	99.56	99.61	passed	passed	passed
5.1.10	99.65	99.54	99.61	passed	passed	passed
5.1.11	99.65	99.56	99.62	passed	passed	passed
5.1.12	99.65	99.58	99.61	passed	passed	passed

TABLE 10. UACI test value.

Images	$UACI_{Min}(\%)$	$UACI_{Max}(\%)$	$UACI_{Mean}(\%)$	Critical UACI(%)		
				$U^{*-}_{0.05} = 33.2824\%$ $U^{*+}_{0.05} = 33.6447\%$	$U^{*-}_{0.01} = 33.2255\%$ $U^{*+}_{0.01} = 33.7016\%$	$U^{*-}_{0.001} = 33.1594\%$ $U^{*+}_{0.001} = 33.7677\%$
5.1.09	33.40	33.68	33.54	passed	passed	passed
5.1.10	33.28	33.58	33.46	passed	passed	passed
5.1.11	33.29	33.60	33.43	passed	passed	passed
5.1.12	33.27	33.68	33.44	passed	passed	passed

TABLE 11. $\overline{NPCR}$ with existing algorithms.

Images	Algorithm [16]	Algorithm [17]	Algorithm [19]	Algorithm [21]	Ours
	$\overline{NPCR}(\%)$	$\overline{NPCR}(\%)$	$\overline{NPCR}(\%)$	$\overline{NPCR}(\%)$	$\overline{NPCR}(\%)$
Couple	99.49	98.31	No	99.62	**99.61**
Camera	99.47	98.43	99.61	99.59	**99.61**
Lake	99.50	98.49	99.61	99.58	**99.60**
Boat	99.47	98.26	No	99.61	**99.61**

TABLE 12. $\overline{UACI}$ with existing algorithms.

Images	Algorithm [16]	Algorithm [17]	Algorithm [19]	Algorithm [21]	Ours
	$\overline{UACI}(\%)$	$\overline{UACI}(\%)$	$\overline{UACI}(\%)$	$\overline{UACI}(\%)$	$\overline{UACI}(\%)$
Couple	33.44	16.78	No	33.40	**33.50**
Camera	33.31	16.77	33.47	33.56	**33.52**
Lake	33.68	18.27	33.45	33.57	**33.51**
Boat	33.45	16.17	No	33.28	**33.47**

I. NOISE ATTACK

Noise attack is common attack method. To test the ability of the proposed algorithm to resist noise attack, Gaussian noise and Pepper and Salt noise are used to test experiment. The test results as Fig. 15. The Gaussian noise test results with mean 0.01, variance 0.001 and 0.002 are Fig. 15 (a) and (b). The test results of Pepper and Salt noise with intensity of 0.01 and 0.05 as Fig. 15 (c) and (d). The results in Fig. 15 indicate that the designed algorithm can prevent noise attack to some degree.

VI. CONCLUSION

This paper firstly designed a 2D-SCMCI hyperchaotic map by Cascade Modulation Couple, 1D-Sine chaotic map and 1D-Iterative chaotic map. The dynamic performances analysis of the 2D-SCMCI hyperchaotic map indicate that 2D-SCMCI hyperchaotic map has universal attractor, good randomness and ergodicity, and the valve of complexity is higher. In addition, using 2D-SCMCI hyperchaotic map, we designed an image encryption algorithm, and security of the proposed encryption algorithm is analyzed. And compared with the security of existing image encryption algorithms. Results illustrate that the designed encryption scheme has better key sensitivity and it can resist violent attack, differential attack, noise attack and so on. Therefore, we proposed algorithm has better security performances in digital image encryption.

REFERENCES

[1] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[2] Y.-T. Lin, C.-M. Wang, W.-S. Chen, F.-P. Lin, and W. Lin, "A novel data hiding algorithm for high dynamic range images," *IEEE Trans. Multimedia*, vol. 19, no. 1, pp. 196–211, Jan. 2017.

[3] A. V. Diaconu, "Circular inter–intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci.*, vols. 355–356, pp. 314–327, Aug. 2016.

[4] I.-C. Dragoi and D. Coltuc, "On local prediction based reversible watermarking," *IEEE Trans. Image Process.*, vol. 24, no. 4, pp. 1244–1246, Apr. 2015.

[5] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultimediaMag.*, vol. 25, no. 4, pp. 46–56, Oct. 2018.

[6] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, ''Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption,'' *Signal Process.*, vol. 142, pp. 340–353, Jan. 2017.

[7] Z. Hua, S. Yi, and Y. Zhou, ''Medical image encryption using high-speed scrambling and pixel adaptive diffusion,'' *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.

[8] N. Zhou, H. Jiang, L. Gong, and X. Xie, ''Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging,'' *Opt. Lasers Eng.*, vol. 110, pp. 72–79, Nov. 2018.

[9] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, ''Novel quantum image encryption using one-dimensional quantum cellular automata,'' *Inf. Sci.*, vol. 345, pp. 257–270, Jun. 2016.

[10] Y. Q. Zhang and X. Y. Wang, ''A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice,'' *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

[11] F. Yang, J. Mou, C. Luo, and Y. Cao, ''An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence,'' *Phys. Scripta*, vol. 94, no. 8, Aug. 2019, Art. no. 085206.

[12] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, ''Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit,'' *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[13] X. Chai, Y. Chen, and L. Broyde, ''A novel chaos-based image encryption algorithm using DNA sequence operations,'' *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[14] J. Fridrich, ''Image encryption based on chaotic maps,'' in *Proc. IEEE Int. Conf. Syst., Man, Cybern. Comput. Cybern. Simulation*, Oct. 1997, pp. 1105–1110.

[15] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, ''Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform,'' *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105821.

[16] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, ''Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing,'' *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

[17] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, ''Optical image encryption technique based on compressed sensing and arnold transformation,'' *Optik*, vol. 124, no. 24, pp. 6590–6593, Dec. 2013.

[18] R. Ponuma and R. Amutha, ''Compressive sensing based image compression-encryption using novel 1D-chaotic map,'' *Multimedia Tools Appl.*, vol. 77, no. 15, pp. 19209–19234, Aug. 2018.

[19] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, ''Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system,'' *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105816.

[20] L. Gong, K. Qiu, C. Deng, and N. Zhou, ''An optical image compression and encryption scheme based on compressive sensing and RSA algorithm,'' *Opt. Lasers Eng.*, vol. 121, pp. 169–180, Oct. 2019.

[21] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, ''A color image cryptosystem based on dynamic DNA encryption and chaos,'' *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[22] F. Yang, J. Mou, H. Yan, and J. Hu, ''Dynamical analysis of a novel complex chaotic system and application in image diffusion,'' *IEEE Access*, vol. 7, pp. 118188–118202, 2019.

[23] H. Liu, A. Kadir, and J. Liu, ''Color pathological image encryption algorithm using arithmetic over galois field and coupled hyper chaotic system,'' *Opt. Lasers Eng.*, vol. 122, pp. 123–133, Nov. 2019.

[24] H. Liu, Y. Zhang, A. Kadir, and Y. Xu, ''Image encryption using complex hyper chaotic system by injecting impulse into parameters,'' *Appl. Math. Comput.*, vol. 360, pp. 83–93, Nov. 2019.

[25] Z. Hua, Y. Zhang, and Y. Zhou, ''Two-dimensional modular chaotification system for improving chaos complexity,'' *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, 2020.

[26] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, ''A joint color image encryption and compression scheme based on hyper-chaotic system,'' *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2333–2356, Jun. 2016.

[27] Q. Xu, K. Sun, C. Cao, and C. Zhu, ''A fast image encryption algorithm based on compressive sensing and hyperchaotic map,'' *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.

[28] J. Mou *et al.*, ''Image compression and encryption algorithm based on hyper-chaotic map,'' *Mobile Netw. Appl.*, no. 3, pp. 1–13, 2019.

[29] H. Liu and A. Kadir, ''Asymmetric color image encryption scheme using 2D discrete-time map,'' *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.

[30] X. Wang and S. Gao, ''Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network,'' *Inf. Sci.*, vol. 539, pp. 195–214, Oct. 2020.

[31] X. Wang and S. Gao, ''Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,'' *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[32] X. Wang, L. Feng, and H. Zhao, ''Fast image encryption algorithm based on parallel computing system,'' *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[33] Y. Xian and X. Wang, ''Fractal sorting matrix and its application on chaotic image encryption,'' *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[34] Z. Chen, X. Yuan, Y. Yuan, H. H.-C. Iu, and T. Fernando, ''Parameter identification of chaotic and hyper-chaotic systems using synchronization-based parameter observer,'' *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 9, pp. 1464–1475, Sep. 2016.

[35] Z. Hua, B. Zhou, and Y. Zhou, ''Sine-Transform-Based chaotic system with FPGA implementation,'' *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2557–2566, Mar. 2018.

[36] E. Y. Xie, C. Li, S. Yu, and J. Lü, ''On the cryptanalysis of Fridrich's chaotic image encryption scheme,'' *Signal Process.*, vol. 132, pp. 150–154, Mar. 2017.

[37] S. B. He, K. H. Sun, and C. X. Zhu, ''Complexity analyses of multi-wing chaotic systems,'' *Chin. Phys. B*, vol. 22, no. 5, pp. 220–225, 2013.

[38] W. Liu, K. Sun, and C. Zhu, ''A fast image encryption algorithm based on chaotic map,'' *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[39] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, ''2D sine logistic modulation map for image encryption,'' *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[40] F. K. Diakonos and P. Schmelcher, ''On the construction of one-dimensional iterative maps from the invariant density: The dynamical route to the beta distribution,'' *Phys. Lett. A*, vol. 211, no. 4, pp. 199–203, Feb. 1996.

[41] G. A. Gottwald and I. Melbourne, ''Testing for chaos in deterministic systems with noise,'' *Phys. D: Nonlinear Phenomena*, vol. 212, nos. 1–2, pp. 100–110, Dec. 2005.

[42] L. Dieci and E. S. Van Vleck, ''Perturbation theory for approximation of Lyapunov exponents by QR methods,'' *J. Dyn. Differ. Equ.*, vol. 18, no. 3, pp. 815–840, Jul. 2006.

[43] M. Yu, K. Sun, W. Liu, and S. He, ''A hyperchaotic map with grid sinusoidal cavity,'' *Chaos, Solitons Fractals*, vol. 106, pp. 107–117, Jan. 2018.

[44] W. Yue, G. Yang, H. Jin, and J. P. Noonan, ''Image encryption using the two-dimensional logistic chaotic map,'' *J. Electron. Imag.*, vol. 21, no. 1, p. 3014, 2012.

[45] J. Wu, F. Guo, P. Zeng, and N. Zhou, ''Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence,'' *J. Mod. Opt.*, vol. 60, no. 20, pp. 1760–1771, Nov. 2013.

[46] C. Capus and K. Brown, ''Short-time fractional Fourier methods for the time-frequency representation of chirp signals,'' *J. Acoust. Soc. Amer.*, vol. 113, no. 6, p. 3253, 2003.

[47] Y. Wu and J. Noonan, ''NPCR and UACI randomness tests for image encryption,'' *Cyber J.: Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun.*, vol. 2, pp. 31–38, Jan. 2011.

JILEI SUN was born in Zibo, Shandong, China, in 1977. He received the M.S. degree in computer application technology from the Shandong University of Technology, Zibo, in 2006. Since 2006, he has been a Lecture with the Department of Information Engineering, Binzhou University. He is the author of three books and five articles. His research interests include computer vision, machine learning, and image encryption.