IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 7, 2019, accepted July 18, 2019, date of publication July 25, 2019, date of current version August 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2931052

Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion

XINGYUAN WANG, SUO GAO, LONGJIAO YU, YUMING SUN, AND HUAIHUAI SUN
School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

Corresponding authors: XingYuan Wang (xywang@dlmu.edu.cn) and Suo Gao (1418159118@qq.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672124 and Grant 61370145, and in part by the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund under Grant MMJJ20170203.

ABSTRACT In this paper, an image encryption algorithm based on bit-combination scrambling and dynamic diffusion is proposed based on multiple chaotic systems. First, the plaintext image is scrambled. On the basis of the decimal system, the pixel value of the gray-scale plaintext image is divided into three groups: units, tens, and hundreds' digit. Each group performs different rounds of Arnold mapping, and the parameters of the Arnold mapping and the number of mapping wheels are determined by the plaintext image. The scrambled image is generated by combination. This algorithm avoids the periodicity of Arnold mapping. Second, the dynamic diffusion operation is designed. This operation can start from any position of the plaintext pixel value and combine chaotic sequence to do XOR around this point. Therefore, it has N modes of diffusion, where N is the number of pixel values. Third, this method is extended to color image encryption. The comparison test results show that this method has better security and can resist common attack methods.

INDEX TERMS Bit-combination scrambling, chaos image encryption, decimal system, dynamic diffusion.

I. INTRODUCTION

In recent years, with the rapid development of the Internet, we use the Internet to transmit information more and more frequently. However, due to the openness and sharing of the network, it poses a great threat to the transmission of information. Attackers can intercept information or change the data of the information in order to destroy the transmission of the data. As a result, more and more people call for greater detection of the network, security of the protection data and privacy. As the main carrier of information transfer, it is important to find a general image encryption algorithm [1]–[4]. With the development of chaos theory, because the complex dynamic behavior and the sensitivity of initial value of chaotic system [5]–[8], chaos has a good effect on the field of encryption [9]–[11]. Therefore, more and more chaotic image encryption algorithms were proposed based on chaos theory [12]–[15]. The theory of chaos provides a good guarantee for information transmission.

Chaotic system is the key core of chaotic image encryption. A chaotic system with complex dynamic behavior will bring good results to image encryption. There are several types of chaotic systems [16]–[18]:

(1) Low dimensional chaotic system. Such as Logistic mapping, Chebyshev mapping, and Tent mapping [19], [20]. Zhou and Parvaz constructed a one-dimensional chaotic system with more complex dynamic behavior by using two one-dimensional systems, which were applied to chaotic image encryption [21], [22].

(2) High dimensional chaotic system. Such as, Wang system, Lorenz system, and Chen system. Combining Lorenz system and DNA computation, a color image encryption algorithm was proposed by Zhang and Wei [23].

(3) Space-time chaotic system. Such as CML system, MLNCML system, and MCML system. A symmetric image encryption algorithm based on MLNCML system was proposed by Zhang and Wang [24]. A nonlinear diffusion image encryption algorithm based on MCML system was proposed by Wang *et al.* [25].

In this paper, a dynamic diffusion encryption algorithm based on Logistic mapping and 2D-LASM [26] system is proposed. This algorithm is generated by the interaction of the two systems rather than relying on a single system.

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

So this algorithm increases the size of secret key space.

Common Arnold mapping is periodic, and the original image will be obtained after multiple rounds of encryption [27], [28]. In this paper, an encryption algorithm is designed to solve this problem. The parameters of the Arnold mapping and the number of Arnold mapping rounds are determined by the plaintext. A one-secret encryption method is used, and the different plaintext can generate different parameters and the number of the Arnold mapping wheels. In addition, some algorithms can not have a good effect on all black and all white images, and the encryption algorithm proposed in this paper can not only encrypt black and white images, but also encrypt color images. References [29] and [30] must carry out multi-wheel encryption on the image to achieve a safe effect which wastes much of the encryption time, but this article only needs one round to reach the safe effect.

The rest of the organization of this article is as follows. In the second chapter, chaotic systems are introduced. The third chapter is the proposed encryption algorithm and decryption algorithm. The fourth chapter is the performance analysis of gray image, including experimental simulation and some common security analysis. The fifth chapter is color image encryption, as well as simple security analysis. The sixth chapter is a summary of the full text, and puts forward the direction of future work.

II. CHAOS SYSTEM

This chapter introduces the chaotic system used in encryption algorithm and the parameters when it reaches chaos.

A. LOGISTIC AND 2D-LASM SYSTEM

In this paper, two low dimensional chaotic systems, Logistic mapping and 2D-LASM system are used. The mathematical expression formula of Logistic mapping is as follows:

$$x_{n+1} = \mu x_n(1 - x_n). \tag{1}$$

where $x_n \in (0, 1)$, when parameter $\mu \in (3.5699456, 4]$, the Logistic map is chaotic. Further processing of the Logistic mapping becomes the following form:

$$f : x_{i+1} = 4\mu x_i(1 - x_i). \tag{2}$$

where $\mu \in (0, 1]$. Logistic map is chaotic when $\mu \in (0.87, 1]$.

Another low-dimensional chaotic system is 2D-LASM system [26]. The mathematical expression formula is as follows:

$$\begin{cases} g : y_{i+1} = \sin(\pi\mu_1(z_{i+1} + 3)y_i(1 - y_i)), \\ h : z_{i+1} = \sin(\pi\mu_1(y_i + 3)z_i(1 - z_i)). \end{cases} \tag{3}$$

When $\mu \in [0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93] \cup \{1\}$, 2D-LASM system enters chaotic state.

B. ARNOLD MAPPING

The Arnold mapping formula is as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod } M). \tag{4}$$

where p and q are parameters of Arnold mapping. The value of p and q are positive integers, M is the size of the image.

III. THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The encryption algorithm proposed in this paper is a process of scrambling to diffusion. The size of plaintext image is $M \times M$ for encryption. If plaintext does not conform to this size, then it is necessary to carry out the operation to make the size of plaintext images conform to the scale.

On the basis of decimal system and Arnold mapping, a scrambling algorithm based on bit-combination is proposed. On the basis of binary and XOR theory, a dynamic diffusion encryption algorithm is proposed.

A. PARAMETERS AND INITIAL VALUES OF CHAOTIC SYSTEMS

A bit stream of 165 length is given, which is recorded as K. K as part of the secret keys. K is grouped as follows, and the parameters and initial values of the chaotic system are produced by Eq. (5).

$$\begin{aligned} k_1 &= K(1:33), \quad \mu = \text{bin2dec}(k_1)/10^{11} + 0.9, \\ k_2 &= K(34:66), \quad \mu_1 = \text{bin2dec}(k_2)/10^{11} + 0.6, \\ k_3 &= K(67:99), \quad x(0) = \text{bin2dec}(k_3)/10^{10}, \\ k_4 &= K(100:132), \quad y(0) = \text{bin2dec}(k_4)/10^{10}, \\ k_5 &= K(133:165), \quad z(0) = \text{bin2dec}(k_5)/10^{10}. \end{aligned} \tag{5}$$

In Eq. (5), bin2dec(x) represents the conversion of binary numbers to decimal numbers.

According to Eq. (5), the calculated parameters and initial values are replaced to Eq. (2) and Eq. (3), the first 200 points are abandoned and the three chaotic sequences are recorded as F, G, and H.

B. SCRAMBLING ALGORITHM

On the basis of decimal system and Arnold mapping, a position scrambling algorithm is proposed.

Definition 1: Define a function $V(x, n)$, the value of n and x are positive integers. The function of $V(x, n)$ is to take the post n bit of the integer x.

Example 1: Suppose $x = 987654301$, then $V(x, 2) = 01$ and $V(x, 3) = 301$.

Definition 2: Define a function $E(x)$, the value of x is an array. The function of $E(x)$ is to find the maximum number of repeated elements in the array x.

Example 2: Suppose $x = [1, 2, 4, 2, 3, 3, 3, 3, 3, 3]$, then $E(x) = 6$.

For plaintext image $P_{M\times M}$, the scrambling algorithm proposed in this paper is as follows:

Step 1: For plaintext image P, generate a secret key associated with it, R is calculated by Eq. (6):

$$R = V((\sum_{i=1}^{M}\sum_{j=1}^{M} P(i,j))^2, 4). \tag{6}$$

Step 2: In Eq. (4), the parameters of Arnold mapping include p and q, and the number of Arnold mapping rounds w. According to the key generated by Eq. (6), define the parameters p and q as:

$$\begin{aligned} p &= V(R, 2) + 1, \\ q &= \text{floor}(R/100) + 1. \end{aligned} \tag{7}$$

The number of encrypted wheels w_1, w_2, w_3 are defined as:

$$\begin{aligned} w &= V(R, 3), \\ w_1 &= \text{floor}(w/100) + 2, \\ w_2 &= \text{floor}(\text{mod}(w, 100)/10) + 2, \\ w_3 &= \text{mod}(w, 10) + 2. \end{aligned} \tag{8}$$

If $E(P) = M \times M$, proceed to Step 3, otherwise proceed to Step 4.

Step 3:

$$\begin{aligned} L &= F(w : M \times M - w + 1), \\ P_{M\times M} &= \text{floor}(\text{ mod }(L_{M\times M} \times 10^{10} + P_{M\times M}, 256)). \end{aligned} \tag{9}$$

Turn back to Step 1.

Step 4: The plaintext images are grouped according to one bit, ten bits and one hundred bit, each group is produced by Eq. (10).

$$\begin{aligned} P_1(i,j) &= \text{floor}(P(i,j)/100), \\ P_2(i,j) &= \text{floor}(\text{mod}(P(i,j), 100)/10), \\ P_3(i,j) &= \text{mod}(P(i,j), 10). \end{aligned} \tag{10}$$

In Eq. (10), floor(x) is a downward integer function. mod(x) is the residual function. i and j are coordinates of pixel values. The values of them are $0 < i \le M$ and $0 < j \le M$.

Step 5: P_1, P_2, P_3 are generated by Eq. (10), and they do Arnold mapping of w_1, w_2, w_3 round respectively. Arnold mapping rounds are determinated by Eq. (8). Finally, three confusion matrices S_1, S_2, S_3 are produced. S_1, S_2, S_3 make the following combination to generate scrambling matrix Z.

$$S_4 = S_3(i,j) \times 100 + S_2(i,j) \times 10 + S_1(i,j), \tag{11}$$

$$Z = \text{mod}(S_4, 256), \tag{12}$$

$$S_5 = S_4 - Z. \tag{13}$$

In Eq. (12), Z is a scrambled matrix. In Eq. (13), S_5 is given as a secret key.

C. DYNAMIC DIFFUSION

In this paper, a dynamic diffusion strategy is proposed for differential attacks. Follow these steps to do dynamic diffusion:

Step 1: There is a plaintext image P. Changed a pixel value of P and generate another image which is Q. Record the location of different points between P and Q as (i, j). If there is only one image which is P. We can define $i = 1$ and $j = 1$.

Step 2: Using the dec2bin(x) to convert the scrambled image Z to binary image Z.

Step 3: Dynamic diffusion

$$\begin{aligned}
C(i,j) &= Z(i,j) \\
&\quad \oplus \text{floor}(\text{mod}(0.986 \times \sin(\pi F(\text{mod}(i^2+j^2, M)+1)) \\
&\quad \times 10^{10}, 256)) \oplus C'. \\
C(s,j) &= Z(s,j) \\
&\quad \oplus \text{floor}(\text{mod}(0.973 \times \sin(\pi H(\text{mod}(s^2+j^2, M)+1)) \\
&\quad \times 10^{10}, 256)) \oplus C(s-1,j), \quad i < s \le M. \\
C(s,j) &= Z(s,j) \\
&\quad \oplus \text{floor}(\text{mod}(0.956 \times \sin(\pi H(\text{mod}(s^2+j^2, M)+1)) \\
&\quad \times 10^{10}, 256)) \oplus C(s+1,j), \quad 1 \le s < i. \\
C(s,t) &= Z(s,t) \\
&\quad \oplus \text{floor}(\text{mod}(0.934 \times \sin(\pi G(\text{mod}(s^2+t^2, M)+1)) \\
&\quad \times 10^{10}, 256)) \oplus C(s,t-1), \\
&\quad 1 \le s \le M, j < t \le M. \\
C(s,t) &= Z(s,t) \\
&\quad \oplus \text{floor}(\text{mod}(0.912 \times \sin(\pi G(\text{mod}(s^2+t^2, M)+1)) \\
&\quad \times 10^{10}, 256)) \oplus C(s,t+1), \\
&\quad 1 \le s \le M, 1 \le t < j.
\end{aligned} \tag{14}$$

In Eq. (14), $C' = \text{mod}(w, 256)$. $F(y)$, $G(y)$, and $H(y)$ are the y component of the chaotic sequence F, G, and H.

Finally, the ciphertext image C is generated. The encryption flow chart is shown in Fig. 1.

D. DECRYPTION PROCESS

In this paper, the symmetric encryption method is adopted, the encryption process is reversible. So decryption is the inverse process of encryption, the specific encryption process is as follows:

Step 1: If secret key K is known, Eq. (5) is used to generate the initial value $x(0)$, $y(0)$, $z(0)$ and parameters μ, α, β of chaotic system. Bring in Eq. (2) and Eq. (3) and give up the first 200 points to generate chaotic sequences F, G, and H.

Step 2: Generate secret keys R related to plaintext by Eq. (6). The parameters of Arnold mapping and initial value of diffusion C' are calculated according to R.

Step 3: The inverse of the diffusion generates a scrambling matrix Z by ciphertext C.

$$\begin{aligned}
Z(i,j) &= C(i,j) \oplus C' \oplus \text{floor}(\text{mod}(0.986 \\
&\quad \times \sin(\pi F(\text{mod}(i^2+j^2, M)+1)) \times 10^{10}, 256)). \\
Z(s,j) &= C(s,j) \oplus C(s-1,j) \oplus \text{floor}(\text{mod}(0.973 \\
&\quad \times \sin(\pi H(\text{mod}(s^2+j^2, M)+1)) \\
&\quad \times 10^{10}, 256)), \quad i < s \le M. \\
Z(s,j) &= C(s,j) \oplus C(s+1,j) \oplus \text{floor}(\text{mod}(0.956 \\
&\quad \times \sin(\pi H(\text{mod}(s^2+j^2, M)+1)) \times 10^{10}, 256)), \\
&\quad 1 \le s < i.
\end{aligned}$$

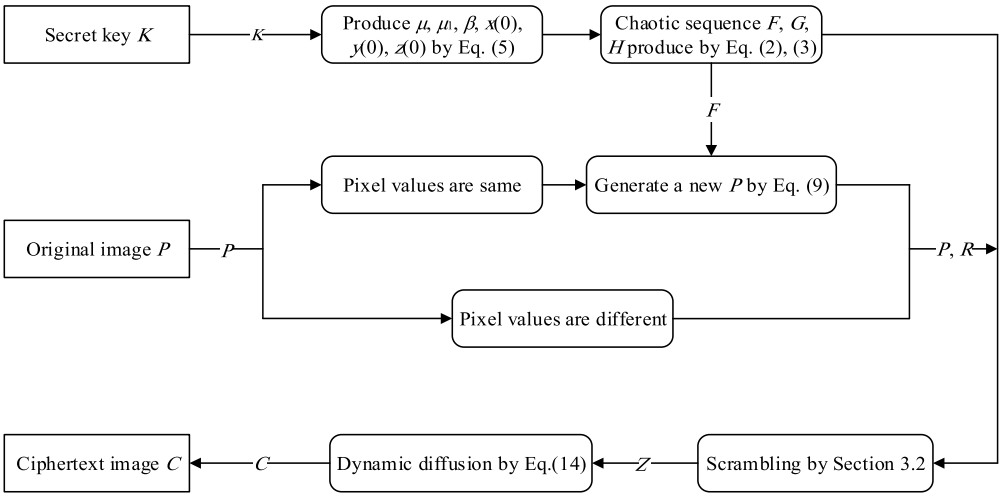


FIGURE 1. Encryption flow chart.

$$Z(s,t) = C(s,t) \oplus C(s,t-1) \oplus \text{floor}(\text{mod}(0.934 \times \sin(\pi G(\text{mod}(s^2+t^2, M)+1)) \times 10^{10}, 256)), \quad 1 \le s \le M,\ j < t \le M.$$

$$Z(s,t) = C(s,t) \oplus C(s,t+1) \oplus \text{floor}(\text{mod}(0.912 \times \sin(\pi G(\text{mod}(s^2+t^2, M)+1)) \times 10^{10}, 256)), \quad 1 \le s \le M, 1 \le t < j. \tag{15}$$

Step 4: The scrambling matrix Z is scrambled inversely to produce the matrix P.

Step 5: The P s processed and the plaintext image is finally generated by Eq. (16):

$$P = \text{mod}(P, 256). \tag{16}$$

IV. PERFORMANCE ANALYSIS OF GRAY IMAGE

This chapter introduces gray images simulation and some common security analysis, including key space analysis, secret key meter perceptual analysis, differential attack, statistical analysis, information entropy analysis, robustness analysis and so on.

A. GRAY IMAGE SIMULATION

This section shows some common gray images simulation, the size of gray images are 512×512, the simulation includes the encryption and decryption display of gray images, the experimental results are shown in Fig. 2.

B. KEY SPACE ANALYSIS AND PERCEPTUAL ANALYSIS

The secret key space of this paper includes the secret key R related to the plaintext and the bit stream K of length 165. The matrix S_5 generated in the encryption process by Eq. (12). So the size of key space is more than $2^{165} > 2^{100}$. This is enough to resist violent attacks.

In addition, a good algorithm is sensitive to the secret key. In other words, to make a small change in the secret key, and then restore, we will get a completely different result. k_5 is selected to change one bit in this article,

$$k_5 = 10001011000001001001011101011101 0.$$

Change the last bit of the k_5 to generate a new secret key:

$$k_5' = 10001011000001001001011101011101 1.$$

Restore by the wrong secret key and the correct secret key, respectively, and the results are shown in Fig. 3.

C. DIFFERENTIAL ATTACK

The aim of differential attack is plaintext image, change a pixel value and restore image, observe the gap between the two restored plaintext, find the rule and crack algorithm. In this paper, according to this characteristic, a dynamic diffusion encryption algorithm is designed. Changing the different pixel points of plaintext will produce completely different cryptography systems, so that there are more options for encryption.

NPCR (Number of Pixels Change Rate, NPCR) and UACI (Unified Average Changing Intensity, UACI) are two important indicators of differential attack, which are calculated by Eq. (17) and Eq. (18).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100, \tag{17}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100. \tag{18}$$

In Eq. (17) and Eq. (18), c_1 and c_2 are two images, the size of them are $W \times H$. If $c_1(i,j) \neq c_2(i,j)$, then $D(i,j) = 1$, otherwise, $D(i,j) = 1$. In theory, the closer the value of NPCR and UACI is to 99.6093% and 33.4635%, the better the encryption algorithm is.

In this paper, we select P (1, 1) and P (256, 256) to change the pixel value of two points. And calculate their NPCR and UACI results as shown in Table 1. Compared with the

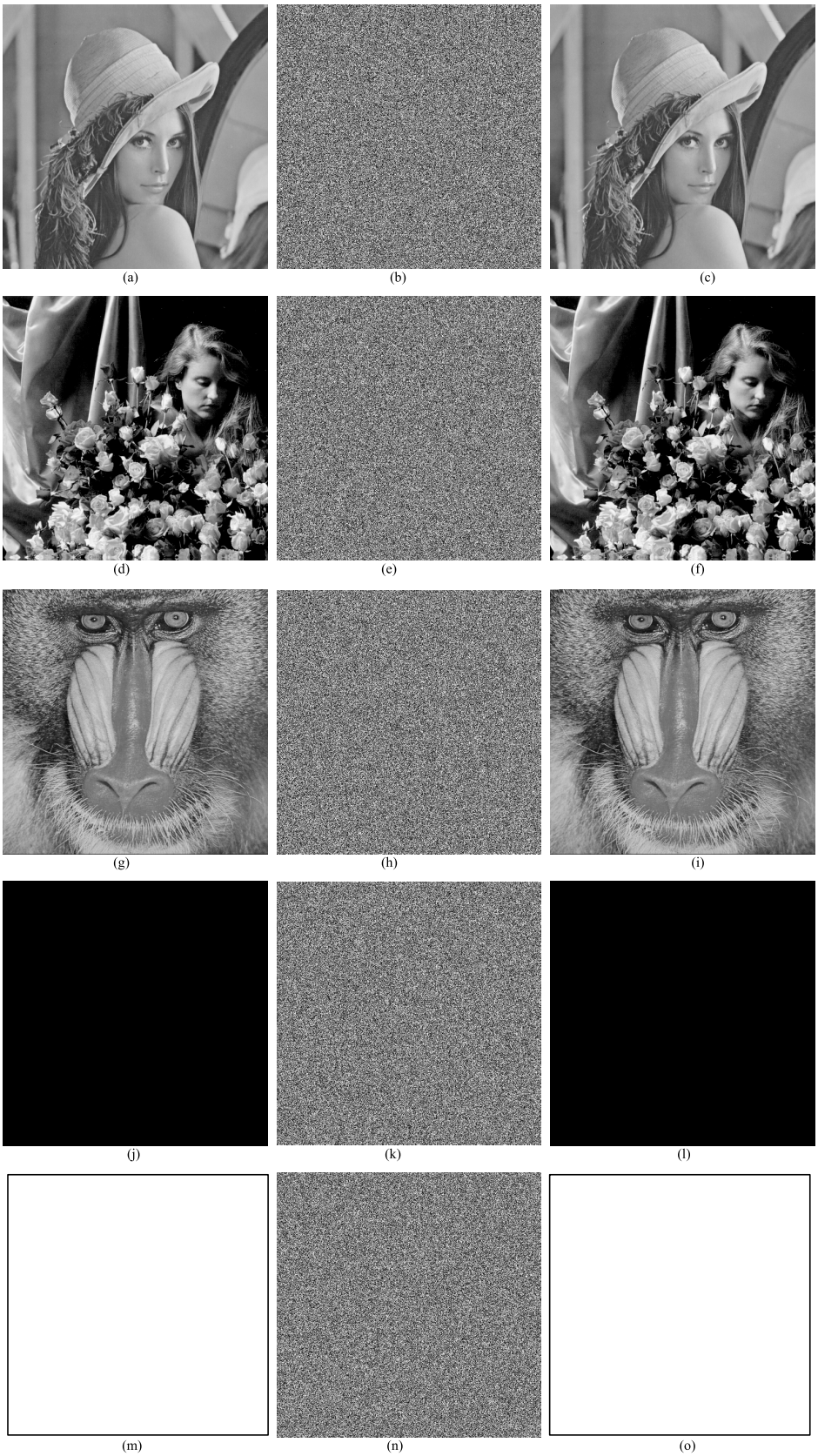
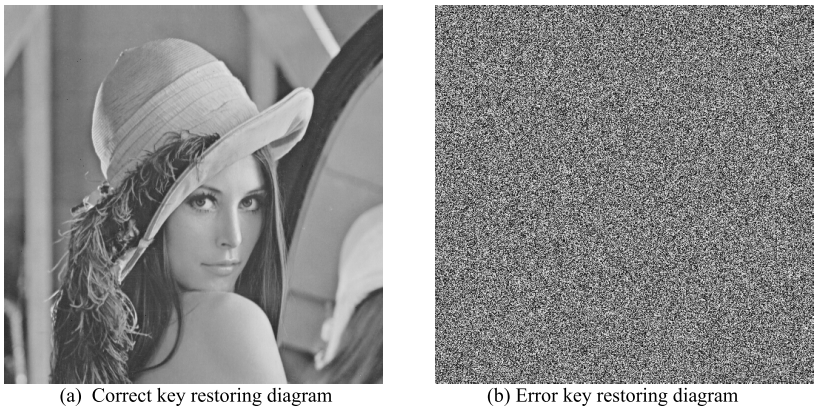


FIGURE 2. Encryption and decryption of gray-scale images. (a) Plaintext of Lena. (b) Ciphertext of Lena. (c) Decryption of Lena. (d) Plaintext of Flower. (e) Ciphertext of Flower. (f) Decryption of Flower. (g) Plaintext of Baboon. (h) Ciphertext of Baboon. (i) Decryption of Baboon. (j) Plaintext of Black. (k) Ciphertext of Black. (l) Decryption of Black. (m) Plaintext of White. (n) Ciphertext of White. (o) Decryption of White.



(a) Correct key restoring diagram (b) Error key restoring diagram

FIGURE 3. Sensitivity of secret key.

TABLE 1. NPCR and UACI.

Image	Change P (1,1)		Change P (256,256)	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Lena	99.6170	33.4481	99.6017	33.4580
Flower	99.5968	33.3308	99.5968	33.4957
Baboon	99.5792	33.5129	99.6193	33.4313
Black	99.6219	33.4519	99.5972	33.5607
White	99.6178	33.5323	99.5995	33.4354

TABLE 2. The average of NPCR and UACI and comparison with other algorithms.

Image	#Mean	Ref. [4]	Ref. [8]	Ref.[11]	Ref. [13]
NPCR (%)	99.6041	99.6265	99.6177	99.6184	99.6069
UACI (%)	33.4663	33.6183	33.6694	33.5739	33.4558

representative articles Ref. [4], [8], [11], [13], the comparison results of NPCR and UACI are shown in Table 2.

The experimental results and comparison show that the NPCR and UACI of the algorithm are close to the theoretical value, so the encryption algorithm proposed in this paper has a good ability to resist differential attacks.

D. HISTOGRAM ANALYSIS

Histogram analysis is to detect whether the distribution of ciphertext pixel value is uniform, and a good encryption algorithm ciphertext histogram should be uniform. Otherwise, the encryption algorithm is not secure, and the attacker can find the law from the ciphertext and crack the algorithm.

Fig. 4 shows the grayscale Lena, Flower, Baboon, Black and White plaintext histogram and ciphertext histogram. By observing Fig. 4, the distribution of plaintext histogram is uneven, but when the encryption algorithm is used in this paper, the distribution of ciphertext histogram is uniform. Therefore, it is difficult for attackers to find a rule in ciphertext to crack the algorithm. Therefore, this paper has a good ability to resist statistical attacks.

E. χ^2 TEXT

More intuitively, we can also use χ^2 tests to detect whether the histogram distribution is uniform, and the value of χ^2 is calculated by Eq. (19).

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0}. \tag{19}$$

In Eq. (19), i represents pixel value, the value of i is an integer between 0 and 255. v_i represents the times of the pixel value i appears in the image. v_0 is the expected frequency of a pixel value i, $v_0 = (M \times N)/256$. Commonly used significant level is $\alpha = 0.05$, and $\chi^2_{0.05} = 293.24783$. At this time, we think that the histogram distribution is uniform in the case of significant horizontal $\alpha = 0.05$.

Different differential attack positions are selected and Eq. (16) is used to detect the χ^2 value of plaintext image and the χ^2 value of ciphertext image. The test results are shown in Table 3.

It is easy to see from Table 3 that the χ^2 value of plaintext is very large, but through the encryption algorithm in this paper, the χ^2 value of ciphertext is very small. Under the confidence level $\alpha = 0.05$, the χ^2 values are all less than 293.24783, so we can say that the histogram distribution is uniform under the confidence level $\alpha = 0.05$.

F. CORRELATION ANALYSIS

In addition to the above histogram analysis, there is also a detection index in statistical analysis, the correlation of adjacent pixel values, which includes horizontal adjacent pixel correlation, vertical adjacent pixel correlation, diagonal adjacent pixel correlation. In a good encryption system, the closer the correlation of each adjacent pixel value of the encrypted ciphertext is to 0, the better the encryption effect is.

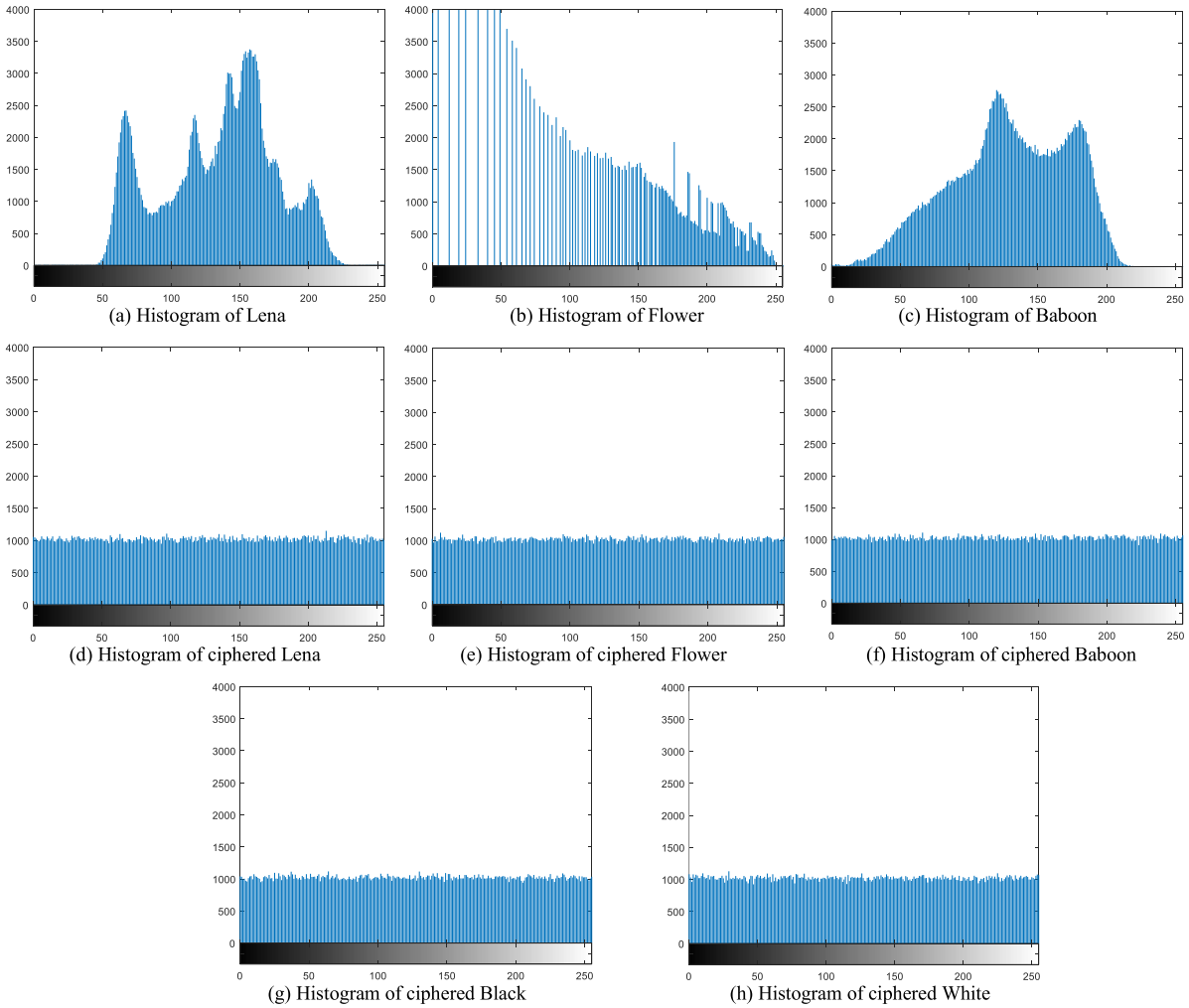


FIGURE 4. Histograms of plain images and ciphered images.

TABLE 3. χ^2 text results.

Image	Lena	Flower	Baboon	Black	White
Plaintext image	242173	4533849	187662	-	-
Change P (1,1)	284.3145	232.7383	242.2598	252.5625	265.2676
Change P (256,256)	269.4922	267.1738	228.2852	256.7363	243.6406

The attacker can not get the effective information from the ciphertext, and the encryption algorithm is well protected.

In this paper, 5000 pixel points are selected in Lena, Flower, Baboon, Black, White plaintext and ciphertext to test. Random Lena, Flower and Baboon are shown in one direction of adjacent pixel values as shown in Fig. 5. The adjacent pixel values in three directions of Black and White ciphertext are selected to display, and the results are shown in Fig. 6.

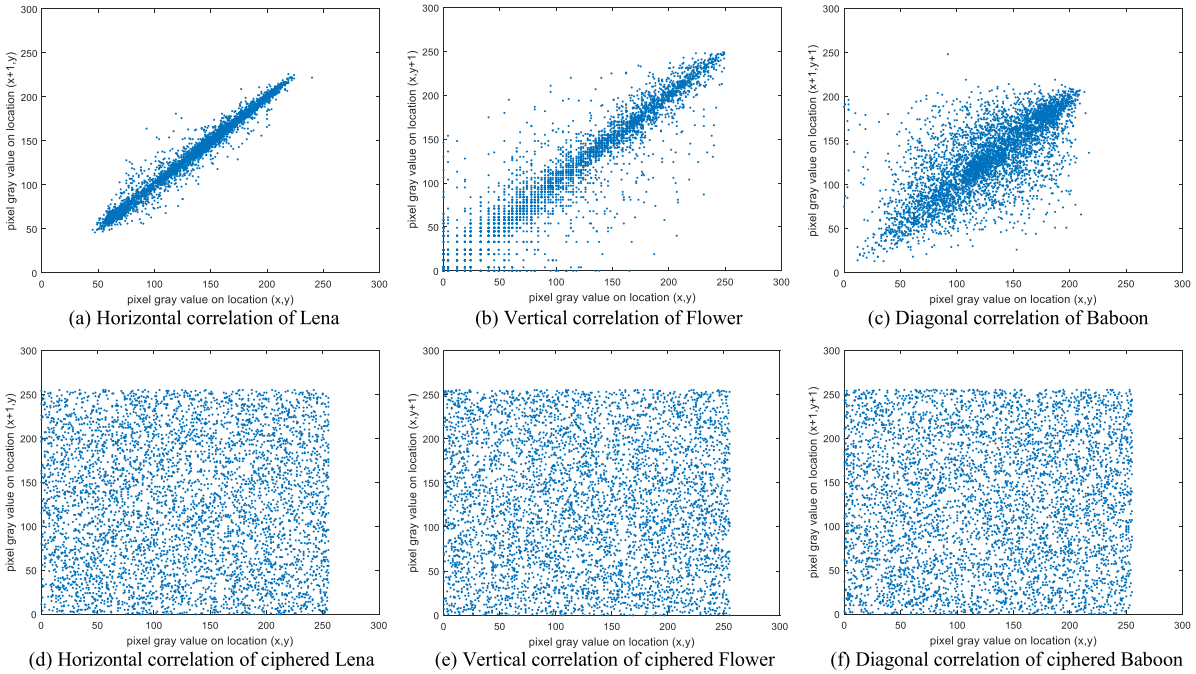
More intuitively, we use Eq. (20) and Eq. (21) to calculate the correlation of adjacent pixel values,

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{20}$$

$$\begin{aligned} \mathrm{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \\ D(x) &= \frac{1}{N}\sum_{i+1}^{N}(x_i - E(x))^2, \\ E(x) &= \frac{1}{N}\sum_{i=1}^{N}x_i. \end{aligned} \tag{21}$$

The calculated results are displayed in Table 4. And compared with the ciphertext correlation of Ref. [4], [8], [11], [13], the results are shown in Table 5.

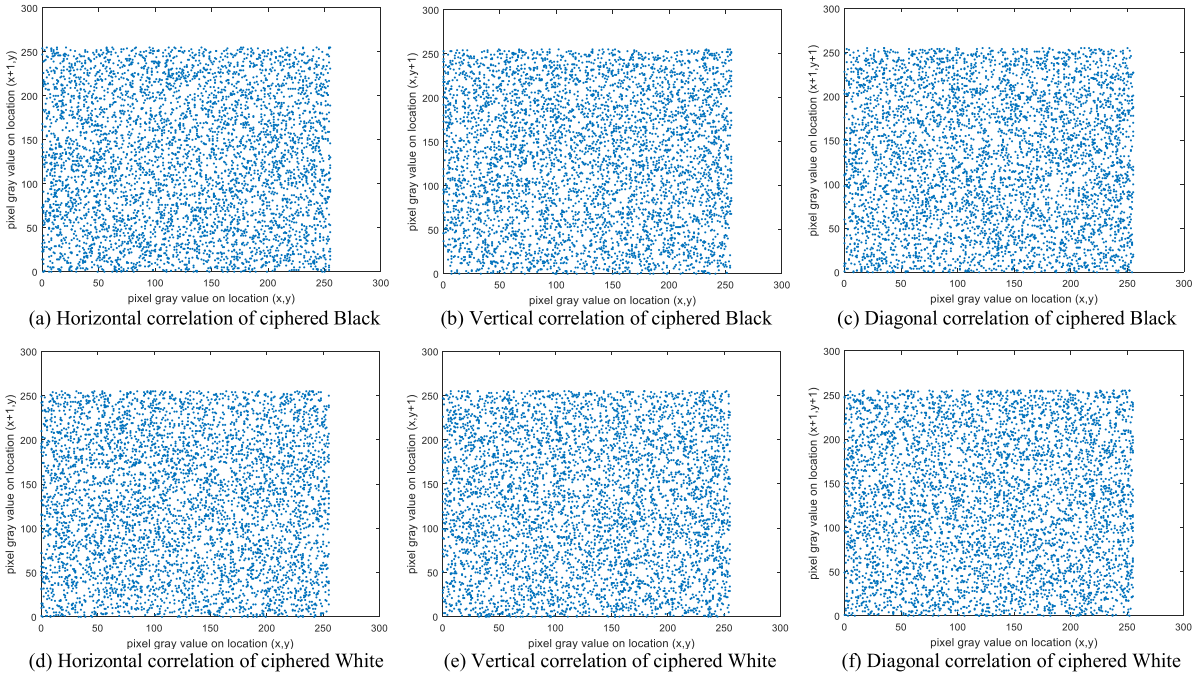
By comparing the algorithm with some representative literature, it can be found that the correlation in the three



(a) Horizontal correlation of Lena (b) Vertical correlation of Flower (c) Diagonal correlation of Baboon

(d) Horizontal correlation of ciphered Lena (e) Vertical correlation of ciphered Flower (f) Diagonal correlation of ciphered Baboon

FIGURE 5. **Correlation coefficients of Lena, Flower, and Baboon.**



(a) Horizontal correlation of ciphered Black (b) Vertical correlation of ciphered Black (c) Diagonal correlation of ciphered Black

(d) Horizontal correlation of ciphered White (e) Vertical correlation of ciphered White (f) Diagonal correlation of ciphered White

FIGURE 6. **Correlation coefficients of Black and White.**

directions of plaintext is very high. After the encryption of this algorithm, the correlation in the three directions of ciphertext becomes very low, Therefore, this paper has better security and can resist statistical attacks.

G. INFORMATION ENTROPY ANALYSIS

Information entropy represents the degree of information confusion, and the more confused the pixel value, the closer of information entropy is to 8 and the less likely the information is leaked, the entropy of the information is calculated by Eq. (22):

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i) \log_2 \frac{1}{p(s_i)}. \tag{22}$$

In Eq. (22), $p(s_i)$ represents the probability of s_i occurrence.

The gray level Lena, Flower, Baboon, Black, and White are used for detection. The size of this image is 512×512.

TABLE 4. Correlation coefficients of images.

Image	Plain			Proposed Change P (1,1)			Proposed Change P (256,256)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9709	0.9847	0.9587	0.0017	− 0.0024	0.00002	0.0019	− 0.0011	− 0.0003
Flower	0.9586	0.9662	0.9357	0.0002	− 0.0003	0.0011	0.0045	− 0.0006	− 0.0004
Baboon	0.8649	0.7584	0.7261	− 0.0002	− 0.0006	0.0005	0.0031	− 0.0051	0.0008
Black	-	-	-	0.0005	0.0045	0.0030	0.0004	− 0.0031	− 0.0012
White	-	-	-	0.0021	0.0003	− 0.0013	− 0.0016	0.0012	0.0002

TABLE 5. Comparison of the correlation coefficients of images.

Image	Lena	Ref. [4]	Ref. [8]	Ref. [11]	Ref. [13]
H	0.0019	0.0024	− 0.0048	0.0022	− 0.0052
V	− 0.0011	− 0.0086	− 0.0112	0.0016	0.0222
D	− 0.0003	0.0402	− 0.0045	0.0007	− 0.0103

TABLE 6. Information entropy of images.

Image	Plain	Change P (1, 1)	Change P (256, 256)	Ref. [4]	Ref. [8]	Ref. [11]	Ref. [13]
Lena	7.2185	7.9992	7.9993	7.9965	7.9991	-	7.9992
Flower	5.8874	7.9994	7.9993	-	-	-	-
Baboon	7.3585	7.9993	7.9994	-	-	-	7.9991
Black	-	7.9993	7.9993	-	-	-	7.9992
White	-	7.9993	7.999.3	-	-	-	7.9994
#Average	-	7.9993		7.9965	7.9977	7.9992	7.9992

The information entropy of plaintext and ciphertext are given in Table 6 by selecting different differential attack positions, and compared with the Ref. [4], [8], [11], [13].

The experimental results show that the entropy of ciphertext information is close to 8. The possibility of information disclosure is very small, and the attacker can hardly find effective information from ciphertext, so the algorithm proposed in this paper has good security.

H. ROBUSTNESS ANALYSIS

Robustness is an important index to test the anti-interference ability of cryptography. In the process of transmission, the information may be lost or polluted by noise, so it is necessary to design an encryption algorithm. Even if part of the information is lost, the part of the plaintext information can be obtained by decrypting the program. We detect the robustness of the proposed method by clipping attack and noise pollution.

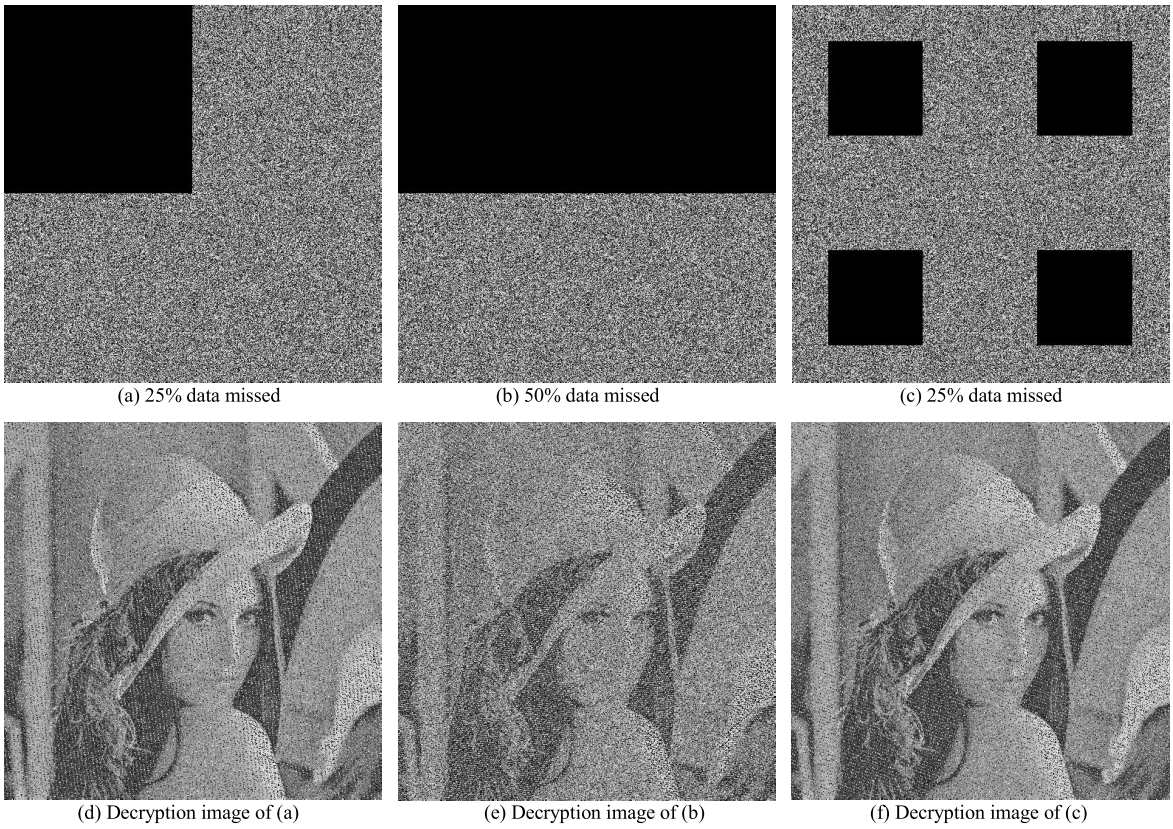
Fig. 7 shows different degrees of clipping attacks, we can see that although the ciphertext has lost some information, some plaintext information can also be obtained through the decryption algorithm. So the encryption algorithm in this paper has a good ability to resist clipping attacks.

Fig. 8 shows different degrees of salt& pepper noise attacks, we can see that after different degrees of noise attacks, plaintext image can also be obtained by reduction algorithm, so the algorithm proposed in this paper has a good ability to resist noise attacks.

I. PSNR ANALYSIS

Peak signal-to-noise ratio (PSNR) is an index to test the relationship between plaintext image and ciphertext image. PSNR is calculated by Eq. (23) [31].

$$PSNR = 20 \times \log_{10}(\frac{P_{\max}}{\sqrt{MSE}}),$$



(a) 25% data missed (b) 50% data missed (c) 25% data missed

(d) Decryption image of (a) (e) Decryption image of (b) (f) Decryption image of (c)

FIGURE 7. Clipping attack.

TABLE 7. PSNR results of ciphertext images.

Image	Change P (1,1)	Change P (256,256)	Ref. [31]	Ref. [32]
Baboon	9.5309	9.5397	8.8532	14.1072
Girl	8.1114	8.0908	8.3028	15.3412
Boat	8.9445	8.9661	9.1257	14.1845
Peppers	8.8702	8.8673	8.1840	14.3908
Lena	9.5389	9.5452	8.3655	14.1954

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{n-1}(P(i,j) - C(i,j)). \tag{23}$$

In Eq. (23), $P_{\max}$ is the maximum gray scale value of a plaintext image, $P_{\max} = 255$. $P(i,j)$ is the pixel value of plaintext in (i,j). $C(i,j)$ is the pixel value of ciphertext in (i,j). The PSNR value of a good algorithm should be small so that the algorithm has a higher security.

The results of the PSNR are shown in Table 7 and compared with the algorithm proposed in Ref. [31], [32]

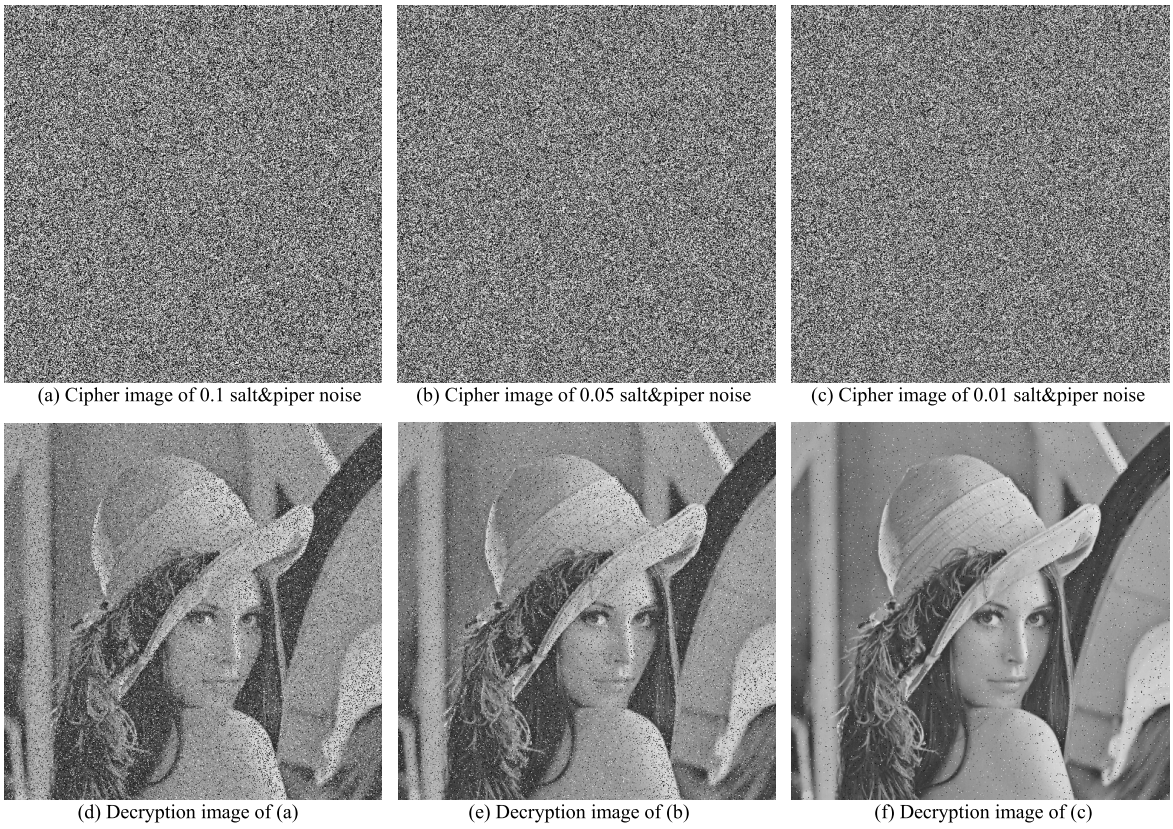
As you can see from Table 7, the algorithm proposed in this paper has a smaller PSNR. It shows that there is a great difference between plaintext and ciphertext., so the algorithm proposed in this paper has higher security.

J. CORRELATIONS ANALYSIS BETWEEN PLAINTEXT IMAGES AND CIPHERTEXT IMAGES

We can use the Eq. (24) to detect the correlation between plaintext and ciphertext [31].

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(P_{ij} - \bar{P})(C_{ij} - \bar{C})}{\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(P_{ij} - \bar{P}_{ij})^2)(\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij} - \bar{C}_{ij})^2)}}. \tag{24}$$

In Eq. (24), $\bar{P}$ is the average of plaintext pixels and $\bar{C}$ is the average of ciphertext pixels. The smaller the value of CC, the greater the difference between plaintext and



(a) Cipher image of 0.1 salt&piper noise (b) Cipher image of 0.05 salt&piper noise (c) Cipher image of 0.01 salt&piper noise

(d) Decryption image of (a) (e) Decryption image of (b) (f) Decryption image of (c)

FIGURE 8. Different noise attacks.

TABLE 8. Correlation coefficient between plaintext and ciphertext images.

Image	Change P (1,1)	Change P (256,256)	Ref. [31]	Ref. [32]
Baboon	0.0014	0.0026	0.0003	0.0097
Girl	0.0023	− 0.0021	0.0025	0.0091
Boat	− 0.0014	0.0025	− 0.0018	0.0093
Peppers	− 0.0021	− 0.0022	− 0.0022	0.0084
Lena	0.0003	0.0015	0.0037	0.0059

ciphertext images. The result of CC is showed in Table 8, and compares it with Ref. [31], [32].

By comparison, we can find that the value of CC is smaller in this article. So it can be explained, there is a great difference between plaintext image and ciphertext image. The algorithm proposed in this paper has better security.

K. LOCAL INFORMATION ENTROPY

We can use local information entropy to test the degree of confusion of local images in ciphertext, and the local information entropy is calculated by Eq. (25).

$$\overline{H_{k,T_B}}(P) = \sum_{i=1}^{k} \frac{H(P_i)}{k}. \tag{25}$$

In Eq. (25), P is the image, k and T_B represent k groups of randomly selected T_B pixels from P. $H(P_i)$ represents the Information Entropy of P_i consisting of T_B Pixels.

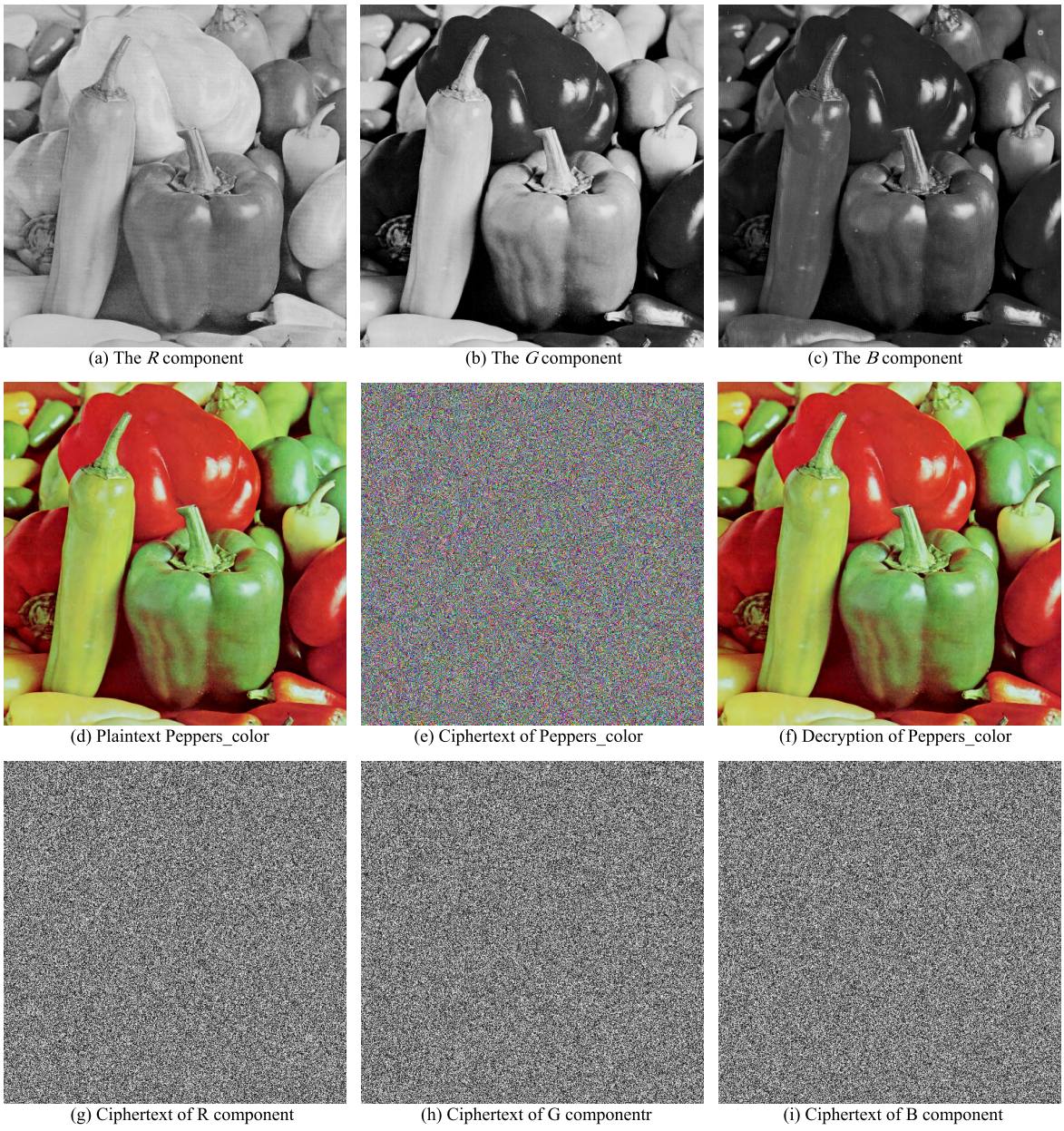
At $k = 30$, $T_B = 1936$ and confidence level $\alpha = 0.01$, the local information entropy should be between 7.901722822 and 7.903215812 [33]. Table 9 shows the results of the local information entropy test and determines whether they have passed the test. All the test data have passed the local information entropy test, so the algorithm proposed in this paper is more secure.

L. SPEED OF ENCRYPTION

The user will consider how to select an encryption algorithm from two aspects. The first point of view is from the

TABLE 9. Local information entropy.

Image	Lena	Flower	Baboon	Black	white
Local information entropy	7.9020	7.9031	7.9018	7.9022	7.9025
Pass or Fail	Pass	Pass	Pass	Pass	Pass



(a) The *R* component (b) The *G* component (c) The *B* component

(d) Plaintext Peppers_color (e) Ciphertext of Peppers_color (f) Decryption of Peppers_color

(g) Ciphertext of R component (h) Ciphertext of G componentr (i) Ciphertext of B component

FIGURE 9. Encryption and decryption of Color Peppers.

encryption effect, through the above comparative experimental analysis, this paper has a better encryption effect.

The second point of view is from the encryption time, in the case of almost the same encryption effect, the faster the encryption time, the more popular it will be. We use matlab 2017 to do experimental simulation. The computer is configured as follows: Intel Core i5-7500 CPU, 8 GB memory and Windows 10 operation system. The time test results are shown in Table 10. And compare it with Ref. [34]–[36] which are mentioned in Ref. [15]. As you can see from Table 10,

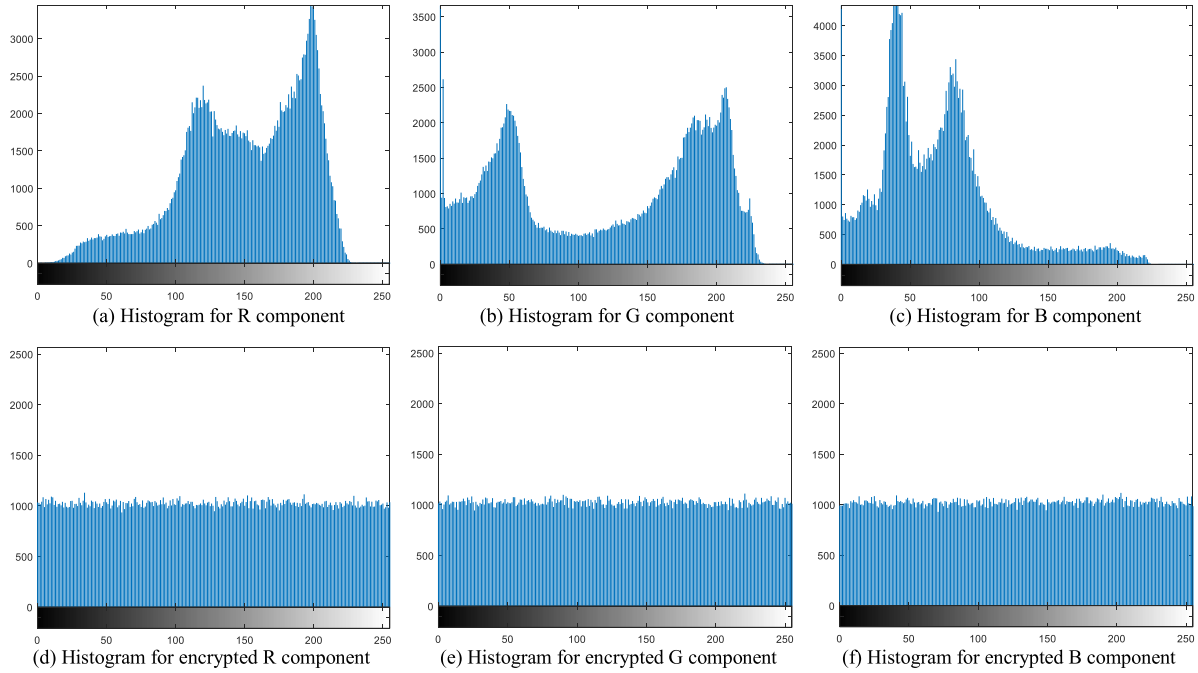


FIGURE 10. Encryption and decryption histogram of Peppers_color.

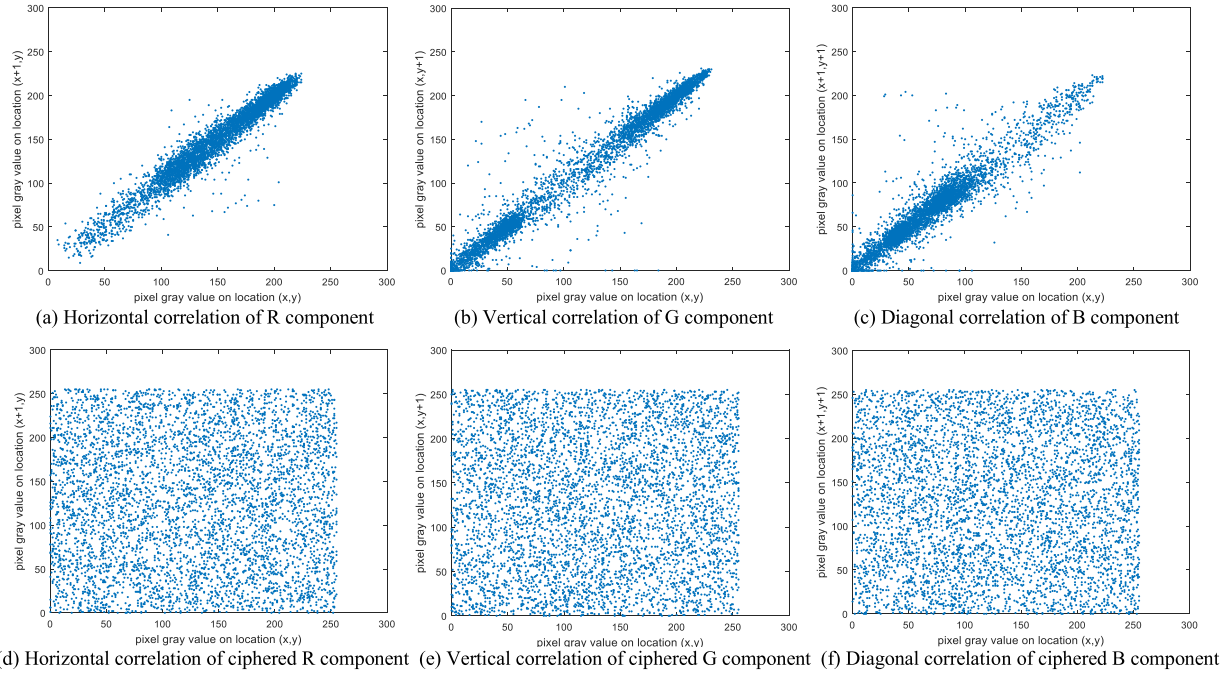


FIGURE 11. Correlation coefficients of Peppers_color.

the encryption time required in this paper is shorter, so the encryption algorithm proposed in this paper is easier to be extended.

V. PERFORMANCE ANALYSIS OF COLOR IMAGE

In this chapter, the color image encryption algorithm is introduced, and some simple security analysis is carried out, including statistical analysis, information entropy detection, differential attack and so on.

A. COLOR IMAGE SIMULATION

For color image encryption, the color image is decomposed into three gray images which are R, G and B. The grayscale image encryption process of R, G, B is carried out, and then

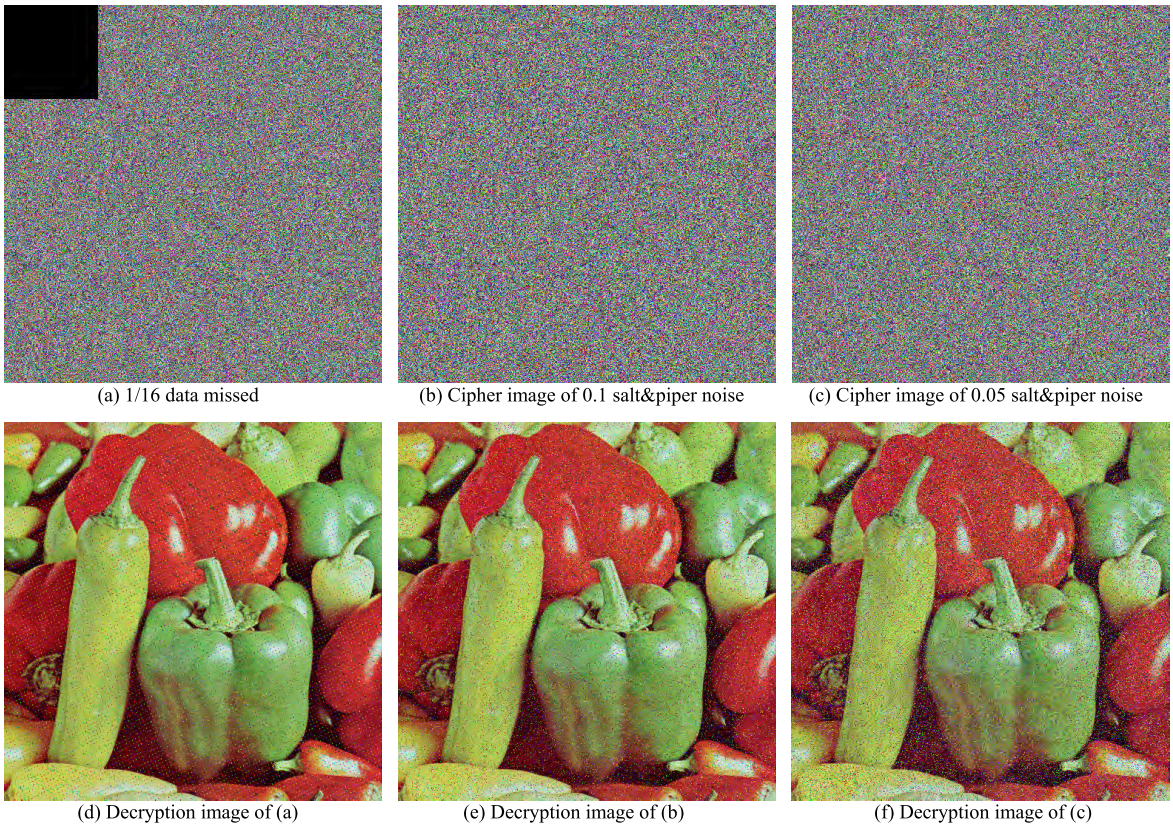


FIGURE 12. Different noise attacks of Peppers_color.

TABLE 10. Encryption time.

Image size	Proposed	CCB [34]	HZ [35]	XLLH [36]
128×128	0.105587	0.2757	0.1531	0.0247
256×256	0.354781	0.9810	0.6347	0.1164
512×512	1.219680	3.8539	2.4919	0.4924
1024×1024	6.889220	15.4565	9.9185	20.144
2048×2048	37.975845	-	-	-

the color image is synthesized. In this paper, color Peppers is selected as an example to encrypt. The size of the image is 512×512. The encryption process and decryption process are shown in Fig. 9.

B. HISTOGRAM ANALYSIS

In this section, the distribution of Plaintext and ciphertext histogram on the three components of color image R, G, and B is given which are shown in Fig. 10. Through the encryption algorithm in this paper, the ciphertext histogram becomes very uniform, so the algorithm in this paper is suitable for color image.

C. CORRELATION ANALYSIS

In this section, the horizontal pixel correlation of R channel, the vertical pixel correlation of G channel and the vertical pixel correlation of B channel are given respectively between plaintext and ciphertext which are shown in Fig. 11, the experimental results show that the adjacent pixel values of the encrypted image have a very low correlation, so the encryption algorithm proposed in this paper is also suitable for color image encryption.

D. COMMON TESTS

This section provides common tests, including NPCR, UACI, information entropy and χ^2 tests. The results are displayed in Table 11 and Table 12.

TABLE 11. Common test results of peppers_color change P (1, 1).

Image	Entropy of information	NPCR (%)	UACI (%)	χ^2
R	7.9993	99.6181	33.4448	255.3477
G	7.9993	99.6273	33.4829	260.3906
B	7.9993	99.5949	33.3948	239.6035

Through the test results, it can be found that the values are close to the theoretical values. Compared with the methods

TABLE 12. Common test results of peppers_color change *P* (256,256).

Image	Entropy of information	NPCR (%)	UACI (%)	χ^2
R	7.9994	99.5975	33.4133	234.2588
G	7.9994	99.6223	33.3950	219.2578
B	7.9993	99.6166	33.4214	241.0703

TABLE 13. Comparison with other algorithms.

Test name	Proposed	Ref. [37]	Ref. [38]	Ref. [39]
Entropy of information	7.9993	7.9906	7.9995	7.9971
NPCR (%)	99.6128	99.6075	99.6448	99.6000
UACI (%)	33.4254	33.4625	33.5319	33.5000

mentioned in Ref. [37]–[39] and the comparative experimental results are shown in Table 13. It can be proved that the encryption algorithm proposed in this paper can be applied not only to gray image encryption, but also to color image encryption.

E. ROBUSTNESS ANALYSIS

In this section, the feasibility of the algorithm in color image encryption is tested by robustness analysis. Fig. 12 shows the effect of clipping attack and noise attack on Peppers_color image, respectively. The experimental results show that the algorithm proposed in this paper has good robustness in color image encryption, so the algorithm proposed in this paper is also suitable for color image encryption.

VI. CONCLUSION

In this paper, based on multiple chaotic systems, a dynamic diffusion image encryption algorithm is proposed, which is a process from scrambling to diffusion. Generate different secret keys for different plaintext. The parameters of Arnold mapping and the number of encrypted wheels are determined by this secret key. In this way, the periodicity problem of Arnold mapping is solved. For differential attack, a dynamic diffusion encryption method is designed. If the size of plaintext image is $M \times M$. Theoretically, there are $M \times M$ encryption methods. This makes it very difficult to crack. The experimental results show that this method can not only encrypt gray images, but also has good results in black images, white images and color image encryption. The experimental results show that the algorithm has better security and can resist common attacks.

At present, our algorithm is still in the theoretical stage. However, the experimental results show that the algorithm proposed in this paper is more secure and the encryption time is shorter. Therefore, the algorithm proposed in this paper can be provided to users, in the future work, we will extend this encryption algorithm to practical applications. Because this method has good security and encryption effect, we want to extend this method to the field of audio encryption or video encryption.

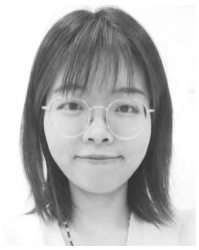
REFERENCES

[1] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[2] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[3] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.
[4] 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.
[5] J. Zhao, S. Wang, Y. Chang, and X. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dyn.*, vol. 80, no. 4, pp. 1721–1729, 2015.
[6] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.
[7] X. Wang, L. Feng, S. Wang, Z. Chuan, and Y. Zhang, "Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption," *IEEE Access*, vol. 6, pp. 39705–39724, 2018.
[8] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.
[9] Q. Ran, L. Yuan, and T. Zhao, "Image encryption based on nonseparable fractional Fourier transform and chaotic map," *Opt. Commun.*, vol. 348, pp. 43–49, Aug. 2015.
[10] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," *Int. J. Bifurcation Chaos*, vol. 28, no. 11, Oct. 2018, Art. no. 1850132.
[11] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Opt. Lasers Eng.*, vol. 115, no. 3, pp. 131–140, Apr. 2019.
[12] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.
[13] Y. Zhang, "The image encryption algorithm based on chaos and DNA computing," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21589–21615, 2018.
[14] R. Bansal, S. Gupta, and G. Sharma, "An innovative image encryption scheme based on chaotic map and Vigenère scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16529–16562, Aug. 2017.
[15] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.
[16] M. K. Mandal, M. Kar, S. K. Singh, and V. K. Barnwal, "Symmetric key image encryption using chaotic Rossler system," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 2145–2152, Nov. 2014.
[17] X.-Y. Wang, T. Wang, D. H. Xu, and F. Chen, "A selective image encryption based on couple spatial chaotic systems," *Int. J. Mod. Phys. B*, vol. 28, no. 6, Mar. 2014, Art. no. 1450023.
[18] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, Oct. 2014.
[19] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8911–8938, Apr. 2018.
[20] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2017.
[21] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014.
[22] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.
[23] Q. Zhang and X. Wei, "RGB color image encryption method based on Lorenz chaotic system and DNA computation," *IETE Tech. Rev.*, vol. 30, no. 5, pp. 404–409, Sep. 2013.
[24] 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.

[25] X. Wang, H. Zhao, and M. Wang, "A new image encryption algorithm with nonlinear-diffusion based on multiple coupled map lattices," *Opt. Laser Technol.*, vol. 115, pp. 42–57, Jul. 2019.
[26] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
[27] Z. Liu, H. Chen, T. Liu, P. Li, L. Xu, J. Dai, and S. Liu, "Image encryption by using gyrator transform and Arnold transform," *Proc. SPIE*, vol. 20, no. 1, Jan. 2011, Art. no. 013020.
[28] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.
[29] X. Wang and K. Guo, "A new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn.*, vol. 76, no. 4, pp. 1943–1950, 2014.
[30] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.
[31] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, 2016.
[32] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wireless Pers. Commun.*, vol. 77, no. 4, pp. 2771–2791, Aug. 2014.
[33] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[34] 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.
[35] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.
[36] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.
[37] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci.*, vol. 349, pp. 137–153, Jul. 2016.
[38] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, 2015.
[39] 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.

XINGYUAN WANG received the Ph.D. degree in computer software and theory from Northeast University, China, in 1999. From 1999 to 2001, he was a Postdoctoral Researcher with Northeast University. He is currently a Professor of information science and technology with Dalian Maritime University, China. He has published three books and over 460 scientific papers in refereed journals and proceedings. His research interests include nonlinear dynamics and control, image processing, chaos cryptography, systems biology, and complex networks.

SUO GAO received the B.S. degree from Shenyang Aerospace University, China. He is currently pursuing the master's degree in computer science and technology with Dalian Maritime University, China. His research interests include image processing, chaos cryptography, and complex networks.



LONGJIAO YU received the bachelor's degree in computer science and technology from the Shenyang University of Technology. She is currently pursuing the master's degree in computer science and technology with Dalian Maritime University, China. Her main research interests include recognition and tracking of multiple objects.

YUMING SUN received the bachelor's degree in software engineering from the School of Computer Science and Technology, Beihua University. He is currently pursuing the master's degree in software engineering with the School of Information Science and Technology, Dalian Maritime University, China. The main research interest includes data cleaning.

HUAIHUAI SUN received the bachelor's degree from the College of Computer, Liaocheng University, China. He is currently pursuing the master's degree in computer science and technology with Dalian Maritime University, China. His main research interests include chaotic encryption and image processing.