Eng Int Syst (2022) 3: 175–183

Engineering
Intelligent Systems

An Efficient Image Encryption Scheme Based on Four Directional Diffusion and Regular Key Selections

Jianzhong Yang[1], Shili Xuan[2,*], Huirong Chen[3] and Xianyang Li[1]

[1] *School of Electronic and Information Engineering, Beibu Gulf University, Qinzhou 535011, China*
[2] *School of Mathematics and Satistics, Yulin Normal University, Yulin 537000, China*
[3] *College of Resources and Environment, Beibu Gulf University, Qinzhou 535011, China*

At present, many existing chaos-based scrambling-diffusion encryption techniques already have a relatively high level of security. However, most of them leverage fixed keys to change the pixel positions and complete encryption from a single direction, resulting in poor randomness of the ciphertext. To solve this problem, this paper proposes an image encryption scheme based on four directional diffusion and regular key selections. Firstly, the initial values of four logistic maps are generated with a 128-bit external key, and an iterative process is performed to obtain a group of secret keys as candidates for the subsequent key selections. Then, during the pixel scrambling process, the plaintext pixels from different positions are scrambled with different keys according to the predefined rules. Finally, a four-directional continuous diffusion method is designed to encrypt the scrambled image. The experiment results confirm that the proposed scheme has a high level of security and feasibility. The ciphertext correlation test, maximum deviation analysis, irregular deviation analysis and sensitivity test show that the proposed scheme is superior to the state-of-the-art methods in many respects.

Keywords: scrambling-diffusion, chaotic encryption technique, image encryption, logistic map, ciphertext correlation, sensitivity

1. INTRODUCTION

Due to technological innovations and developments, rapid social and economic changes are occurring worldwide. In this environment, cybersecurity has become one of the major international scientific issues and an important factor affecting social economy and national security (Wen and You, 2014). Meanwhile, attacks on network are becoming more frequent, and the means of attack are constantly evolving, posing serious challenges to network security. In everyday life, most of the data such as file, video and image information are transferred through the Internet (Zhang and Gao, 2016). The digital images, which contain a lot of user information and have intuitive expression capabilities, play an important role in the fields of education, medicine and economics, and make many aspects of day-to-day life more convenient (Ma et al., 2016). The image encryption technique is an effective means of guaranteeing the integrity and security of the transferred images. The high redundancy of image data, the strong correlation between pixels, and the huge amount of data make image encryption technology inefficient in terms of time, causing a bottleneck in the safe transmission of the image data. How to ensure the security of the image transmission in the network, so that it can effectively resist network attacks, has attracted widespread attention from researchers in various countries (Janakiraman et al., 2018; Sun et al., 2013).

*Corresponding Author Email: ylsyxsl1985@126.com

In this paper, an image encryption algorithm based on dynamic key selection and multi-directional diffusion is proposed, in which the initial values of four logistic maps are generated with a 128-bit external key, then an iterative process is performed to obtain a set of keys. Meanwhile, during the pixel scrambling, the encryption keys are dynamically selected based on values from the engine functions, and different keys are used to scramble the plaintext pixels in different positions. This significantly improves the scrambling degree of the pixels, making the ciphertext closely related to the plaintext, thereby enhancing the resilience of the ciphertext to plaintext attacks. Finally, based on the plaintext pixels, a four-directional continuous diffusion method is designed to diffuse the image pixels from multiple directions to complete the encryption of the scrambled image. Finally, the security and anti-attack capabilities of the proposed encryption algorithm are tested and the results are provided (Peng et al., 2020).

2. RELATED WORK

In recent years, the development and improvement of the chaos theory has provided a new direction for digital image encryption. Among the existing chaos-based encryption techniques, the scrambling-diffusion structure is a popular encryption structure in which a double encryption of images can be achieved through multiple rounds of encryption (Sun et al., 2013; Hasan et al., 2019). The chaotic sequences generated by chaotic encryption systems are highly unpredictable; therefore, the chaos-based encryption systems have been widely used in the field of image encryption.

One study has proposed an image encryption algorithm combining chaotic and super-chaotic mappings, in which a master key is used to determine the parameters of the discrete improved Henon maps, then random sequences are generated by scrambling the auto-regression encoding and logistic chaotic maps, in order to realize the ciphertext images with forward and backward diffusion encryption. This algorithm achieves ideal security effectively and can resist some common attacks (Zhao and Wu, 2016).

An encryption algorithm is proposed based on tent mapping and modified Logistic, Cubic, Chebychev mappings. The algorithm has a large key space and a complex mapping relationship between plaintext and ciphertext. It can resist exhaustive, plaintext, differential and statistical attacks (Yaermaimaiti, 2020). By utilizing logistic mapping, an ideal encryption security can be achieved. The logistic chaotic sequences-based algorithms have the advantages of easy implementation, good randomness and sensitivity to initial values. However, the limited accuracy of the chaotic sequence generator causes the chaotic sequence to have a certain periodicity, which reduces the security of the logistic sequence. Several researchers have improved traditional logistic mapping in order to improve its security (Zhao and Wu, 2016; Khan and Rasheed, 2019). However, these algorithms have introduced complex calculation and transformation processes, which reduces the efficiency of encryption systems. Such systems include two-dimensional sine mapping combined with logistic (Hua et al., 2015), bimodal mapping combined with logistic (Ismail et al., 2017), three-dimensional Brownian movement combined with logistic, etc. (Chai et al., 2017).

Ye and Huang propose an image encryption technique based on intertwining logistic mapping in order to enhance the security of ciphertext and strengthen its defence plaintext attack, in which the initial values of the intertwined. Logistic maps are generated with plaintext pixels and, through an iterative process, the plaintexts are scrambled and diffused with the output sequences of the intertwined logistic mapping (Ye and Huang, 2017). Experiment results show that the algorithm has good encryption efficiency and can resist plaintext attack. To improve the security of ciphertext, one study proposed an image encryption technique based on dynamic harmony searching mechanism and chaotic system. By introducing the dynamic harmony searching mechanism, the maximum information entropy is obtained as the fitness function to diffuse the images and output the optimal ciphertext (Talarposhti and Jamei, 2016; Jain and Kumar, 2019). Then based on chaotic mapping combined with dynamic harmony searching mechanism, the minimum correlation coefficient is used as the fitness function to scramble the optimal ciphertext both horizontally and vertically. The experiment results prove the soundness and superiority of this technique. An image encryption technique based on hyperchaotic system is used to improve the security level. Through an iterative process, the 5D hyperchaotic system outputs a group of keys to scramble the plaintext image, and a corresponding diffusion strategy is designed to encrypt the scrambled image and change the pixel values. Experiment results show that the algorithm has a large key space and can resist many known attacks (Li et al., 2017).

The existing scrambling-diffusion double chaotic encryption techniques have a relatively high level of security and can protect the image transmission in the network to some extent. However, during the image scrambling, these encryption algorithms use fixed keys to change pixel positions. And during the whole diffusion process, the encryption is performed from a single direction, leading to a poor randomness of the ciphertext. In order to solve the aforementioned problems, this paper proposes an image encryption algorithm based on dynamic key selections and multi-directional diffusion.

3. THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The flowchart of the proposed dynamic key selections and multi-directional diffusion-based image encryption algorithm is shown in Figure 1. The proposed method uses different encryption keys to scramble and diffuse the plaintext from different directions. In doing so, the periodicity of the encryption has been significantly reduced and the randomness and security of the ciphertext have been improved. The proposed method has two main stages: (1) plaintext scrambling based on the dynamic key selection mechanism; (2) pixel encryption based on the four-directional continuous diffusion mechanism.

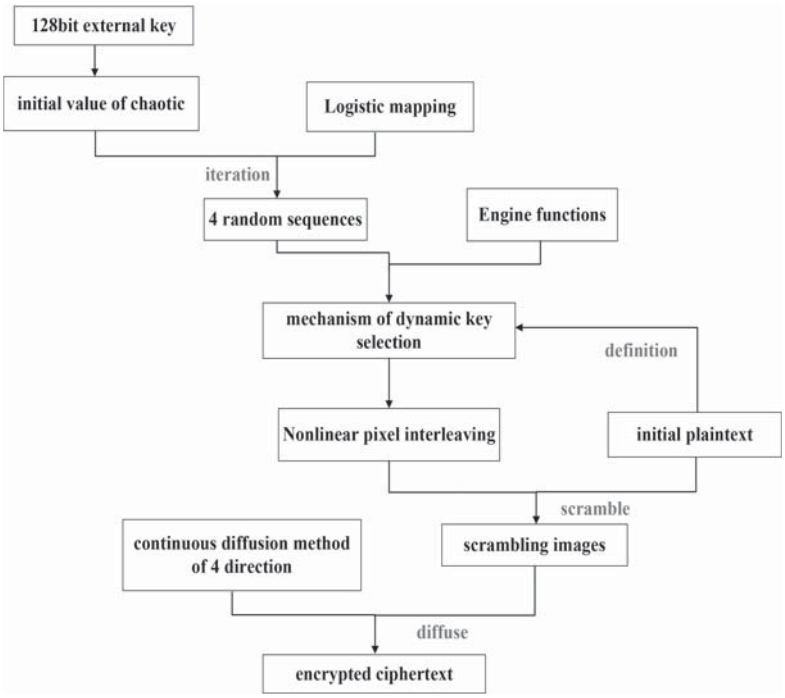

Figure 1 The flowchart of the proposed image encryption algorithm.

3.1 Plaintext Scrambling Based on The Dynamic Key Selection Mechanism

This paper proposes a dynamic key selection mechanism to increase the scrambling degree of the plaintext pixels, avoid the periodicity of the scrambling, and strengthen the connections between ciphertext and plaintext. Let P_0 be the initial plaintext of size $M \times N$, and transform the pixels in P_0 to a 1D array by *Zigzag* scan:

$$\mathbf{P} = \{P(1), P(2), \ldots P(M \times N)\}$$

Firstly, split the 128-bit external key K into 16 8-bit subkeys k_i:

$$K = k_1 k_2 k_3 \ldots k_{16} \tag{1}$$

Where the subkeys k_i are used to generate the initial values x_0, y_0, z_0, w_0 of four Logistic maps:

$$x_0 = \left(\left((k_1 \oplus k_2 \oplus k_3 \oplus k_4) + \sum_{i=1}^{16} k_i \right) / 2^8 \right) \bmod 1 \tag{2}$$

$$y_0 = \left(\left((k_5 \oplus k_6 \oplus k_7 \oplus k_8) + \sum_{i=1}^{16} k_i \right) / 2^8 \right) \bmod 1 \tag{3}$$

$$z_0 = \left(\left((k_9 \oplus k_{10} \oplus k_{11} \oplus k_{12}) + \sum_{i=1}^{16} k_i \right) / 2^8 \right) \bmod 1 \tag{4}$$

$$w_0 = \left(\left((k_{13} \oplus k_{14} \oplus k_{15} \oplus k_{16}) + \sum_{i=1}^{16} k_i \right) / 2^8 \right) \bmod 1 \tag{5}$$

Where $\oplus$ denotes XOR operation, and mod is the complementation function.

Thereafter, use x_0, y_0, z_0, w_0 to perform iterations of Logistic mapping and output four random sequences $\mathbf{X} = (x_1, x_2, x_3 \ldots x_{M\times N})$, $\mathbf{Y} = (y_1, y_2, y_3 \ldots y_{M\times N})$, $\mathbf{Z} = (z_1, z_2, z_3 \ldots z_{M\times N})$, $\mathbf{W} = (w_1, w_2, w_3 \ldots w_{M\times N})$ where the Logistic mapping can be written as (Budimir et al., 2015):

$$x_{i+1} = \lambda x_i (1 - x_i) \tag{6}$$

Combining the random sequences **X, Y, Z, W** to obtain six random matrices:

$$\begin{aligned} \boldsymbol{A}_0 &= \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix}, \boldsymbol{A}_1 = \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Z} \end{bmatrix}, \boldsymbol{A}_2 = \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{W} \end{bmatrix}, \\ \boldsymbol{A}_3 &= \begin{bmatrix} \boldsymbol{Y} \\ \boldsymbol{Z} \end{bmatrix}, \boldsymbol{A}_4 = \begin{bmatrix} \boldsymbol{Y} \\ \boldsymbol{W} \end{bmatrix}, \boldsymbol{A}_5 = \begin{bmatrix} \boldsymbol{Z} \\ \boldsymbol{W} \end{bmatrix} \end{aligned} \tag{7}$$

To fully exploit the five matrices $\boldsymbol{A}_0, \boldsymbol{A}_1, \boldsymbol{A}_2, \boldsymbol{A}_3, \boldsymbol{A}_4, \boldsymbol{A}_5$ in Equation (7), plaintext pixels are used to define an engine index computation function:

$$\begin{cases} \text{index} = T1\%6 \\ T1 = \quad \bmod \left(floor \left(y_0 \times 10^8 \right), M \times N \right) \end{cases} \tag{8}$$

$$y_0 = \begin{cases} 0 & if \ \max (a_i = 0) \\ \frac{\sum_1^{M\times N} a_i}{M \times N \max(a_i)} else & \end{cases} \tag{9}$$

where a_i is the i-th element value in the 1D array P, $\max(a_i)$ is the biggest element in the array P, *floor* denotes the round down operation, % denotes the complementation operation. The engine *index* output from Equation (8) is used as the initial value, and the matrices $\boldsymbol{A}_0, \boldsymbol{A}_1, \boldsymbol{A}_2, \boldsymbol{A}_3, \boldsymbol{A}_4, \boldsymbol{A}_5$ are combined to achieve dynamic key selection mechanism. If $index = 0$, then is used to generate a scrambling key; If $index = 1$, then is used to generate a scrambling key, and so on. Based on $T1_0$ corresponding to the plaintext image, the first pixel is

Table 1 Dynamic key selections.

Plaintext Pixel	$P(1)$	$P(2)$	$P(3)$	$P(4)$	$P(5)$	...	$P(n-2)$	$P(n-1)$	$P(n)$
scrambling pixels	$P'(1)$	$P'(2)$	$P'(3)$	$P'(4)$	$P'(5)$	.....	$P'(n-2)$	$P'(n-1)$	$P'(n)$
$T2$	$T1_0$	$P'(1)$	$P'(2)$	$P'(3)$	$P'(4)$	.....	$P'(n-3)$	$P'(n-2)$	$P'(n-1)$
X	x_1	x_2	x_3	x_4	x_5	.....	x_{n-2}	x_{n-1}	x_{n-1}
Y	y_1	y_2	y_3	y_4	y_5	.....	y_{n-2}	y_{n-1}	y_n
index-new	0	1	1	0	1	.....	1	0	0
scrambling keys	x_1	y_2	y_3	x_4	y_5	.....	y_{n-2}	x_{n-1}	x_{n-1}

scrambled with the initial *index*. After that, the first scrambled pixel value is used to replace $T1$ in Equation (8) and get a new *index* as $index\_new = T2\%2$. Then select the key again and perform the scrambling of the next plaintext pixel. As a further explanation, assume $index = 0$ corresponding to the initial plaintext, then use matrix $A_0 \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix}$ to select secret keys and complete the scrambling of the plaintext pixels. The dynamic key selection mechanism is shown in Table 1. In the table, $P'(i)$ is the pixel scrambled with the selected key; $T1_0$ is the initial value of the plaintext calculated with Equations (8) and (9). Use $index = 0$ corresponding to the initial plaintext to select matrix $\boldsymbol{A}_0$, then use $index\_new = T2\%2$ to define the encryption key. If $index\_new = 0$, then the i-th element in the first row of matrix $\boldsymbol{A}_0$ should be selected to scramble the i-th pixel of the initial image. If $index\_new = 1$, then the i-th element in the second row of matrix should be selected as the encryption key.

It can be observed from Table 1 that, compared with the state-of-the-art dynamic key techniques, the proposed dynamic key selection mechanism has two advantages:

(1) Based on $index\_new = T2\%2$, $T2$ utilizes the previous scrambled pixel to continuously update itself, so that the current encryption key is also constantly updated. Moreover, each key is associated with a plaintext pixel, which makes the proposed method better for defending plaintext against attack, and produces a larger key space.

(2) Even a minor change from the initial image would alter the value of the corresponding Index-new from 0 to 1 or from 1 to 0, resulting in a huge difference in the choice of the encryption key. Hence, the proposed algorithm has a strong sensitivity.

After determining the keys for scrambling each pixel according to the above process, a nonlinear pixel crossover strategy is proposed to complete the scrambling of all plaintext pixels. Let x be the current position of the plaintext pixel, and let x be the position of the scrambled pixel. Firstly, the encryption key $K(x)$ corresponding to x is determined according to the dynamic key selection mechanism. Then x can be calculated as:

$$X' = X + \mathrm{mod}(K(x) + P'(X-1), (M \times N - X + 1)) \quad (10)$$

Where $P'(X-1)$ is the previously scrambled pixel.

According to Equation (10), the pixel value of $P(X')$ is:

$$P(X') = P[X + \mathrm{mod}(K(x) + P'(X-1), (M \times N - X + 1))] \quad (11)$$

Then, exchange the positions between $P(X')$ and $P(X)$. After the first pixel in the plaintext pixel array $\boldsymbol{P} = \{P(1), P(2) \ldots P(M \times N)\}$ is scrambled by the X'-th pixel (here $X' = 3$), the first scrambling ends. After that, it moves forward to $X + 1$ position to realize the second scrambling. Perform the above operations on all pixels in the plaintext until all pixels are scrambled, so as to obtain a final scrambled image.

3.2 Image Diffusion Based on Four-Directional Continuous Diffusion

After the scrambling process, the content information of the plaintext is fully scrambled, but the pixel values still remain unchanged, which makes it a potential security hazard (Fukami et al., 2002; Suartini et al., 2019). In the proposed method, the pixel values are changed from multiple directions to further improve the security level of the ciphertext. Select the previously described random sequence $\boldsymbol{X} = (x_1, x_2, x_3 \ldots x_{M \times N})$ as a secret key and process it with quantification function to get a key stream $\{k_i\}$:

$$k_i = \mathrm{mod}\ (floor(x_i \times 10^{14}), 256) \quad (12)$$

Then, based on the key stream $\{k_i\}$, a four-directional continuous diffusion method is proposed:

Stage 1: Let the scrambled image be I', then use the pixels in I' to from a matrix $\boldsymbol{R}$. The key stream $\{k_i\}$ is randomly sorted to form a matrix Q. The pixel diffusion from the first direction is shown in Figure 2(a), and the diffusion function is as follows:

$$\begin{cases} B'_h(i,j) = B_h(i,j) \oplus Q_{bh}(i,j) \\ T'_h(N-i+1,j) = T_h(N-i+1,j) \oplus B'_h(i,j) \end{cases} \quad (13)$$

Where $B_h(i,j)$ and $T_h(i,j)$ are the pixel values of the upper and lower parts of the ciphertext I', respectively. $Q_{bh}(i,j)$ is the key stream of the lower part of matrix $\boldsymbol{Q}$. $B'_h(i,j)$ and $T'_h(i,j)$ are the encrypted pixel values of $B_h(i,j)$ and $T_h(i,j)$, respectively.

Stage 2: After Stage 1, the encrypted ciphertext I'_1 from the first direction is obtained. Then perform the pixel diffusion of I'_1 from the second direction, as shown in Figure 2(b).

State 3: After the foregoing, the encrypted ciphertext I'_2 from two directions is obtained. After that, perform the pixel diffusion of I'_2 from the third direction (Figure 2(c)):

$$\begin{cases} L'_h(i,j) = L_h(i,j) \oplus Q_{lh}(i,j) \\ R'_h(i,N-j+1) = R_h(i,j) \oplus L_h{}'(i,N-j+1) \end{cases} \quad (14)$$

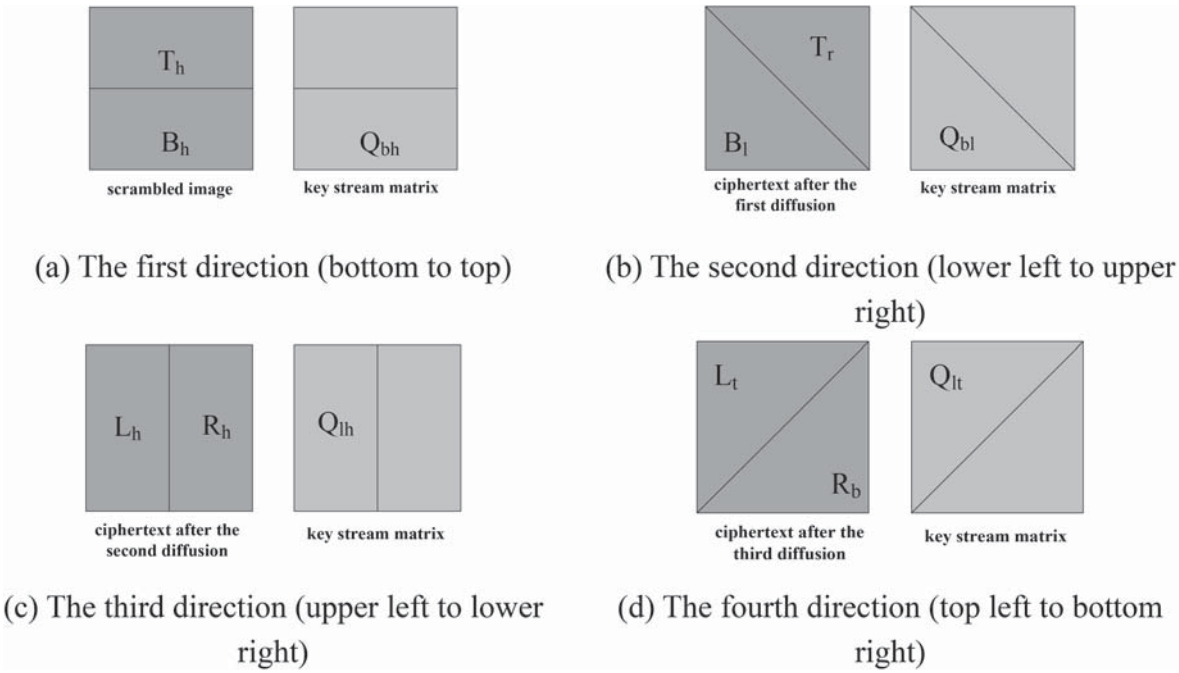

Figure 2 Four-directional continuous diffusion mechanism.

Where $L_h(i, j)$ and $R_h(i, j)$ are the pixel values of the left and right parts of the ciphertext I'_6, respectively. $Q_{lh}(i, j)$ is the key stream of the left part of matrix Q. $L'_h(i, j)$ and $R'_h(i, j)$ are the encrypted pixel values of $L_h(i, j)$ and $R_h(i, j)$, respectively.

State 4: After Stage 3, the encrypted ciphertext I'_3 from three directions is obtained. After that, perform the pixel encryption from the fourth direction based on the ciphertext I'_3, as shown in Figure 2(d).

After the encryption of the scrambled image with the above-mentioned diffusion functions of four directions, the ciphertext can be obtained. Take Figure 2(b) as an example, and encrypt it with 4-directional continuous diffusion. The result is shown in Figure 3. It can be seen from Figure 3 that with the increase of the number of encryption directions, the output ciphertexts are completely different, and the security of image content is significantly improved. In order to quantify the influence of the number of diffusion directions on the security level of ciphertext, this paper introduces the ciphertext entropy to quantify the security level of Figure 3(a)–3(d). The results are 7.8254, 7.8906, 7.9417 and 7.9932, respectively, which indicates that the entropy value of ciphertext increases significantly with the increasing number of diffusion directions. The result proves that, compared with single direction diffusion, the security level of multi-directional diffusion has been improved (De Santis et al., 2001).

According to the encryption procedure of the proposed algorithm, the encryption key of each pixel is obtained by using the dynamic key selection mechanism, and based on the non-linear pixel crossover strategy, the scrambling degree of pixels is significantly improved, the restoration of pixel positions caused by periodicity is avoided, and the security of scrambled image is enhanced. Based on the highly scrambled image, the key stream closely related to plaintext is used to alter the pixel values from four different directions, which effectively improves the randomness and anti-attack ability of the diffused ciphertext, significantly expanding the key space of the algorithm. Therefore, a highly-secured double encryption of the image is achieved.

4. RESULTS AND ANALYSIS

In order to verify the security level of the proposed encryption technique, the experiments are carried out with the Matlab2011b software package. A personal computer with Intel I7-2670 and 8.0 GB RAM is used as the test platform. Meanwhile, the results from a recent study are used as control groups to demonstrate the superiority of the proposed technique. The proposed method uses a hyperchaotic system to encrypt plaintext. The hyperchaotic system is a popular and highly-secure encryption technology whereby the scrambling is performed at pixel-level and the encryption is realized at bit-level. Similar to a recent study, with the proposed technique, the image scrambling is performed at pixel level by low dimensional chaotic mapping, then the scrambled image is diffused at bit level (Khan and Rasheed, 2019; Ye and Huang, 2017). Both encryption techniques use the hyperchaotic system and adopt a scrambling-diffusion encryption structure. Therefore, they are used as control groups. The critical parameters are: $\lambda_1 = 3.35$, $\lambda_2 = 3.08$, $\lambda_3 = 3.52$, $\lambda_4 = 3.61$, the external key $K =$ 26abn17dzxuy84vn.

4.1 Comparison and Analysis of The Encryption Performance

Take Figure 4(a) as an example and encrypt it with the proposed algorithm and the techniques proposed in the research, respectively. The results are shown in Figure 4(b)–4(d). The encryption results show that the output ciphertexts

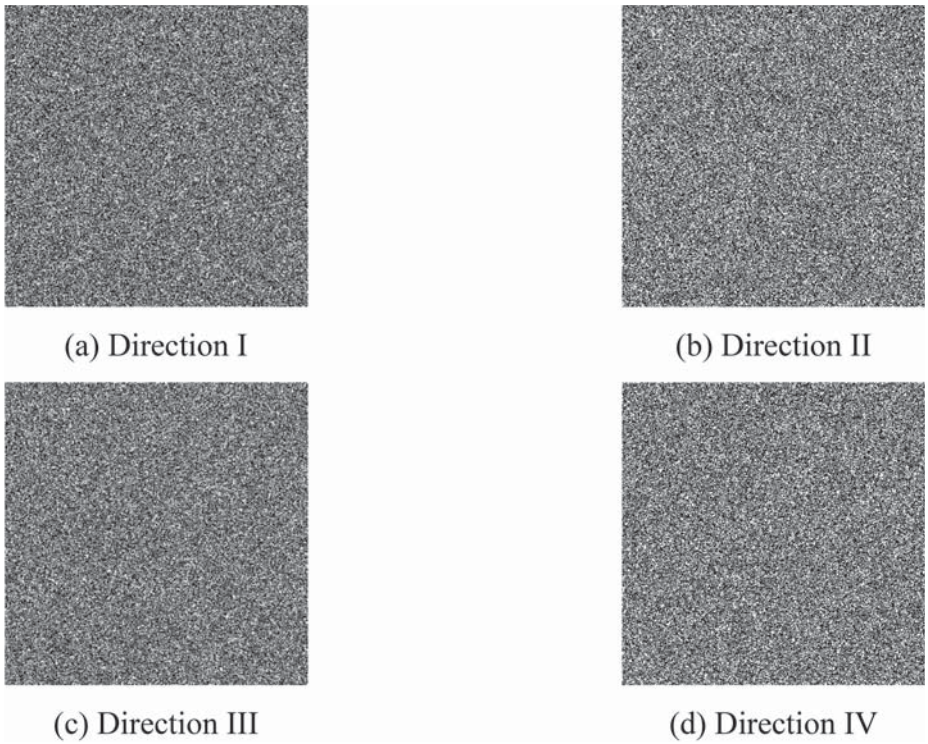

Figure 3 Encryption results of the four-directional continuous diffusion mechanism.

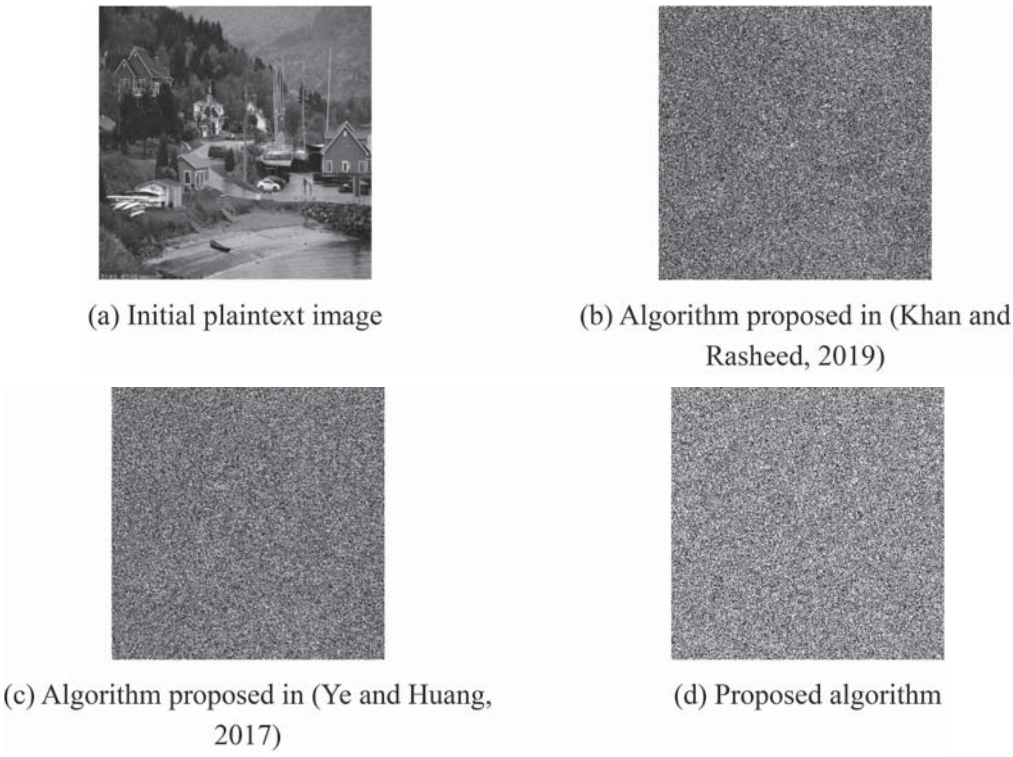

Figure 4 Comparison of the encryption performance of different algorithms.

of the three techniques all have a high level of visual invisibility, and the plaintext content is fully concealed without any visual information leakage. In addition, in order to determine the differences in the security levels of the three algorithms, ciphertext entropy is used to quantify Figure 4(b)–Figure 4(d) and the ciphertext entropy values of the three algorithms are 7.9946, 7.9861 and 7.9829, respectively. It can be seen that the ciphertext obtained by the proposed algorithm has the highest security level, and the entropy values of other algorithms are lower than those of the proposed algorithm (Khan and Rasheed, 2019; Ye and Huang, 2017). The reason is that the proposed algorithm utilizes plaintext pixels to define an engine function, and then designs a dynamic key selection mechanism and

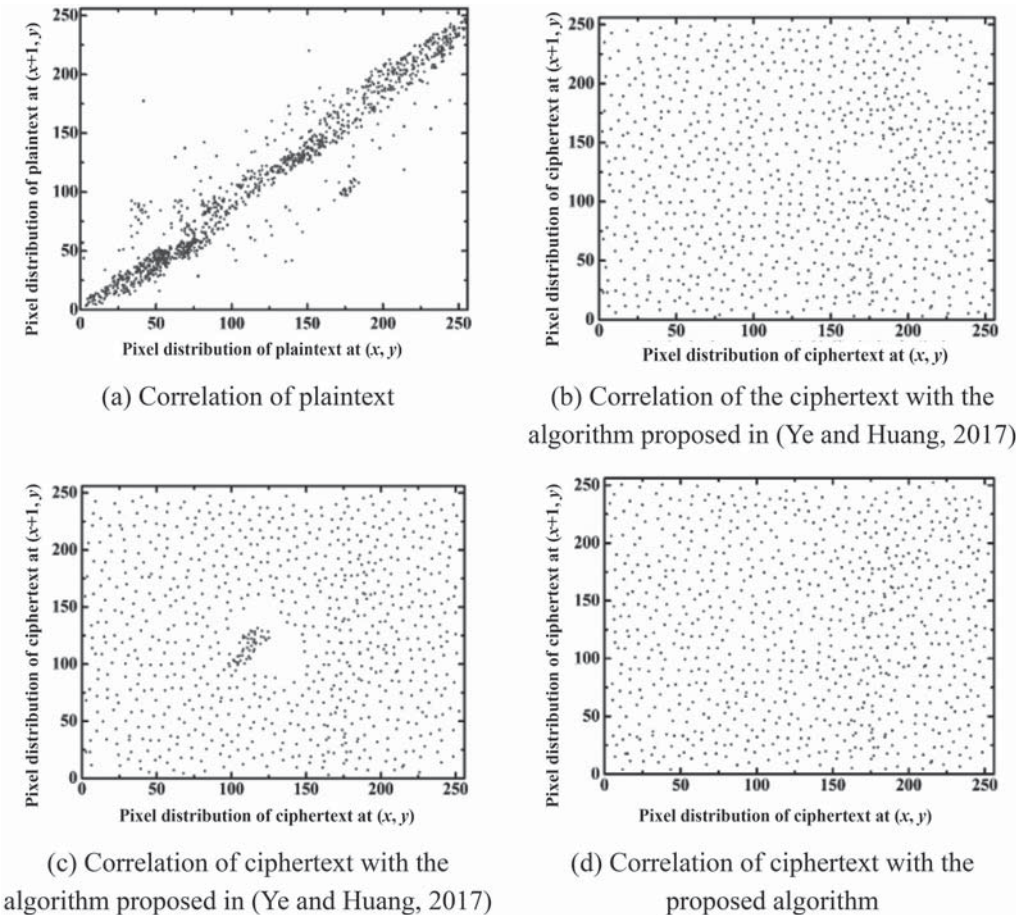

Figure 5 Correlation test results of the three algorithms.

its updating strategy. During image scrambling, different keys are selected based on the difference of each pixel value, and a crossover strategy is used to scramble the pixels, which significantly improves the scrambling degree of pixels and effectively avoids the scrambling periodicity. Meanwhile, a four-directional diffusion function is used to encrypt the scrambled ciphertext from multiple directions, which significantly increases the randomness and dynamics of ciphertext, makes ciphertext closely related to plaintext, and improves the security level and anti-attack ability of the ciphertext. On the other hand, the algorithms proposed in the previous study use a high-dimensional chaotic system to perform pixel scrambling and diffusion, which increases the complexity of the algorithms and increases the difficulty of decoding. However, the reliance on only the chaotic system to complete the encryption will make it have obvious periodicity. And both algorithms adopt fixed keys during the scrambling process, so the pixel diffusion is realized only from a single direction, which leads to a the ciphertext having poor security.

4.2 Correlation Test of Ciphertext

There is a high correlation between two adjacent pixels in an image, which is a great threat to the security of ciphertext. A highly secured encryption algorithm should be able to significantly reduce this disadvantage (Enayatifara et al., 2017). To test the ciphertext correlation of the three algorithms, 2,500 pairs of adjacent pixels are randomly selected from Figure 4(b), 4(c) and 4(d). The calculation function of the correlation coefficient C_{xy} between adjacent pixels is (Kamali et al., 2020):

$$C_{xy} = \frac{1/n \sum_{i=1}^{n} (x_i - E(x_i))(y_i - E(y_i))}{\sqrt{\left(1/n \sum_{i=1}^{n} (x_i - E(x_i))^2\right)\left(1/n \sum_{i=1}^{n} (y_i - E(y_i))^2\right)}} \quad (15)$$

The pixel distribution of plaintext and ciphertext in the horizontal direction is shown in Figure 6. According to Figure 5(a), the correlation of the initial plaintext is extremely strong, and the pixel distribution is extremely uneven. All pixels are stacked into diagonal lines, with a C_{xy} value of 0.9418. However, after using the proposed algorithm and the algorithms proposed in a recent study, this correlation is significantly reduced, and the pixel distribution of the three output ciphertexts becomes uniform, with the C_{xy} values of 0.0011, 0.0034 and 0.0056, respectively. It can be observed from Figure 5(b)–Figure 5(d) that compared with other algorithms, the pixel distribution of the output ciphertext obtained from the proposed algorithm achieves the best uniformity, without any accumulation or blankness (Khan and Rasheed, 2019; Ye and Huang, 2017).

The results of C_{xy} from other directions are shown in Table 2. It can be observed from the table that for the three image diffusion directions, the C_{xy} value of the initial plaintext is always the largest. However, after the encryption process using the proposed algorithm or other algorithms (Khan

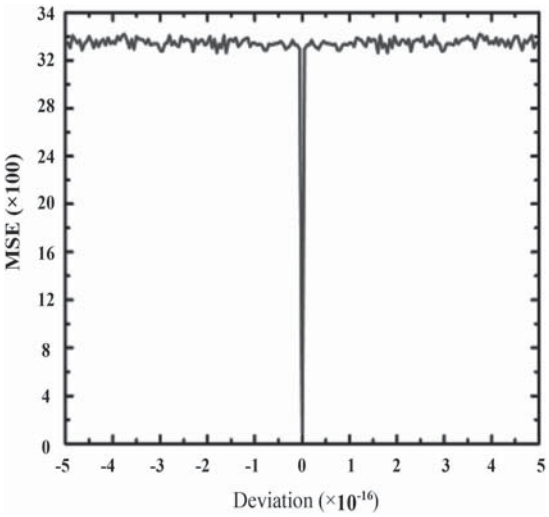

Figure 6 Test results for key sensitivity of the proposed algorithm.

Table 2 Test results of the correlation coefficients from different directions.

Selected Direction	Figure 5(a)	Figure 5(b)	Figure 5(c)	Figure 5(d)
horizontal	0.9418	0.0034	0.0056	0.0011
vertical	0.9575	0.0061	0.0067	0.0034
diagonal	0.9187	0.0019	0.0036	−0.0017

and Rasheed, 2019; Ye and Huang, 2017), the correlation coefficient C_{xy} is significant reduced, and the value of the correlation coefficient C_{xy} of the output ciphertext obtained by the proposed algorithm is the smallest.

4.3 Irregular Deviation Analysis

Irregular deviation measures the statistical distribution of deviation between plaintext image and ciphertext image (Chai et al., 2017). Irregular deviation is defined as follows:

$$I_D = \sum_{i=0}^{N-1} H_{D_i} \tag{16}$$

Where $H_{D_i} = |h_i - A_H|$, h_i is the amplitude of index i of the histogram, which can be calculated based on the absolute difference between plaintext image and ciphertext image, A_H is the mean value of the histogram. A low I_D value indicates that the pixels are uniformly distributed, so the quality of the image encryption is high. The irregular deviation values of the proposed algorithm and other algorithms are given in Table 3. It is obvious that the results obtained by the proposed algorithm are within the acceptable range, which is roughly equivalent to the results of other algorithms. Therefore, the low irregular deviation value proves the encryption strength of the proposed algorithm.

4.4 Sensitivity Test

Sensitivity level is a common index used to measure an algorithm (Min et al., 2016). Therefore, this paper tests the sensitivity of $\lambda_1 = 3.35$, by using the changing factor $\eta = 10^{-15}$ to tamper with the keys to obtain two wrong keys, $\lambda_1' = 3.35 + 10^{-15}$ and $\lambda_1'' = 3.35 + 10^{-15}$, and the rest of the keys remain unchanged. Then, perform decryption on Figure 4(d) to obtain the corresponding MSE curve. The result is shown in Figure 6.

It can be seen from Figure 6 that the MSE curve undergoes dramatic changes. This indicates that the proposed encryption technique meets the "avalanche effect" and has a strong sensitivity.

5. CONCLUSIONS

This paper proposed an image encryption algorithm based on dynamic key selections and multi-directional diffusion to improve the security of ciphertext. During the scrambling of the plaintext, the plaintext is used as a starting point to design a dynamic key selection mechanism. In the pixel crossover process, the encryption keys are selected based on the defined engine value, and the plaintext is scrambled based on the non-linear pixel crossover technique. Meanwhile, the plaintext pixel characteristics are used to design a four-directional continuous diffusion method, so that the pixel values of an image can be encrypted from multiple directions. The whole scrambling-diffusion process is closely related to the plaintext itself, which enhances the connection between output ciphertext and plaintext, and significantly improves its ability to resist plaintext attack. The experimental results show that the proposed encryption technique has good security and sensitivity and can resist plaintext attacks. The proposed method is suitable for high-speed communication applications such as optical fiber communication and 5G networks.

Table 3 Comparison of irregular deviations of different algorithms.

Images from the Standard Image Library	Irregular Deviation		
	Proposed Algorithm	(Khan and Rasheed, 2019)	(Ye and Huang, 2017)
Airport	17 106	16 780	16 586
Plane	40 306	40 434	40 358
Boat	42 708	42 674	43 014
Cameraman	36 226	36 098	36 220
Room	39 244	38 900	39 414
Lena	44 762	45 096	45 438
Man	27 442	27 210	27 230
Moon Surface	50 470	50 406	50 578
Pepper	45 674	46 126	45 854
Tank	43 016	42 996	42 938
Mean	40 739	40 751	40 776

ACKNOWLEDGEMENT

The research is supported by 2019 funding project for improving the basic scientific research ability of young and middle-aged teachers in Guangxi Universities: Research and application of improved distributed clustering algorithm based on Hadoop cloud computing platform (No. 2019KY0609); Qinzhou Science and Technology Development Project (No. 20198503).

REFERENCES

1. Budimir, M.E.A., Atkinson, P.M., Lewis, H.G. 2015. A systematic review of landslide probability mapping using logistic regression. *Landslides, 12*(3), 419–436.
2. Chai, X.L., Gan, Z.H., Yuan, K., et al. 2017. An image encryption scheme based on three-dimensional Brownian motion and chaotic system. *Chinese Physics B, 26*(2), 99–113.
3. De Santis, A., Gaggia, A.G., Vaccaro, U. 2001. Bounds on entropy in a guessing game. *IEEE Transactions on Information Theory, 47*(1), 468–473.
4. Enayatifara, R., Abdullahb, A.H., Isninb, I.F. 2017. Image encryption using a synchronous permutation-diffusion technique. *Optics and Lasers in Engineering, 90*(6), 146–154.
5. Fukami, Y., Nakahara, T., Matsuo, T., et al. 2002. Broadcast apparatus and reception apparatus for providing a storage service by which scrambled content is stored and descrambled using scrambling key list: US 2002.
6. Hasan S.M., Tushar S.H.K., Rahman M.H., Shimu A.R. 2019. An Optimized Design of Electromagnet and Float for A Magnetic Suspension System. *Acta Electronica Malaysia, 3*(1), 14–18.
7. Hua, Z.Y., Zhou, Y.C., Pun, C.M., et al. 2015. 2D sine logistic modulation map for image encryption. *Information Sciences*, 297, 80–94.
8. Ismail, S.M., Said, L.A., Rezk, A.A., et al. 2017. Biomedical image encryption based on double-humped and fractional logistic maps. 2017 *6th International Conference on Modern Circuits and Systems Technologies* (MOCAST). IEEE, 102–111.
9. Jain T., Kumar R. 2019. A Study of Vein Recognition System. *Acta Informatica Malaysia, 3*(1), 13–15
10. Janakiraman, S., Thenmozhi, K., Rayappan, J.B.B., et al. 2018. Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. *Microprocessors and Microsystems*, 56, 1–12.
11. Kamali, S.H., Shakerian, R., Hedayati, M., et al. 2010. A new modified version of advanced encryption standard based algorithm for image encryption. *Electronics and Information Engineering* (ICEIE), 141–145.
12. Khan, M., Rasheed, A. 2019. Permutation-based special linear transforms with application in quantum image encryption algorithm. *Quantum Information Processing, 18*(10), 298–311.
13. Li, Y.P., Wang, C.H., Chen, H. 2017. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering, 90*(10), 238–246.
14. Ma, J.M., Gao, Z.P., Ren, X.D. 2016. Image encryption based on chaotic switching system and cosine number transforms. *Computer Engineering and Design, 37*(9), 2490–2496.
15. Min, F.H., Wang, Z.L., Wang, E.R. 2016. A novel memristor chaotic circuit and its application in image encryption. *Journal of Electronics and Information Science, 38*(10), 2681–2688.
16. Peng, H., Yang, S., Liu, Q., et al. 2020. Intelligent indexing algorithm for the association rules of a multi-layer distributed database. *Engineering Intelligent Systems, 28*(4), 229–239.
17. Suartini S., Nurdiansyah D.H., Haryati S. 2018. The Influence of Costs and Sales Volume Towards the Profit of Cipta Gra fika Printing. *Information Management and Computer, 41*(3), 08–13.
18. Sun, L., Huang, Z.Q., Fu, W.M. 2013. Research on image encryption algorithm based on time delay and hyper-chaos Chen system. *Science and Technology and Engineering, 13*(35), 10523–10530
19. Talarposhti, K.M., Jamei, M.K. 2016. A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map. *Optics and Lasers in Engineering, 81*(7), 21–34.
20. Wen, W.L., You, L. 2014. A parallel image encryption algorithm based on chaotic and bit level permutation. *Netinfo Security*, (4), 40–45.
21. Yaermaimaiti, Y. 2020. An improved facial expression recognition algorithm. *Engineering Intelligent Systems, 28*(2), 25–130.
22. Ye, G.D., Huang, X.L. 2017. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing, 251(19), 45–53.
23. Zhang, S., Gao, T.G. 2016. An image encryption scheme based on DNA coding and permutation of hyper-image. *Multimedia Tools and Applications, 75*(24), 17157–17170.
24. Zhao, F., Wu, C.M. 2016. Image encryption algorithm combined self-encoded theory with super-chaotic mapping. *Journal of Computer-Aided Design & Computer Graphics, 28*(1), 119–128.