International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I5P109

Volume 68 Issue 5, 37-44, May 2020
© 2020 Seventh Sense Research Group®

Original Article

An Image Encryption Algorithm Based on Scrambling with Reversible Matrix Transformation and Chaotic Diffusion

Zikang Wu[1], Jietao Liang[2], Rui Deng[3], Ruisong Ye[4]

[1,2,3,4] Department of mathematics, Shantou University, Guangdong, 515063, China

Received Date: 05 April 2020
Revised Date: 20 May 2020
Accepted Date: 21 May 2020

Abstract *- In view of the poor resistance against statistical analysis and weak security of simple two-dimensional scrambling based image encryption algorithms, this paper proposes an image encryption algorithm combining image pixel scrambling and diffusion controlled by Chebyshev chaotic sequences. Firstly, two-dimensional and three-dimensional reversible scrambling matrices are generated and used to scramble the pixels positions and RGB colour component vector so as to weaken the correlation of adjacent pixels, the correlation of colour components and greatly change the statistical characteristics of plain images histogram. Then, the classical Chebyshev sequences are uniformized and used to diffuse the pixels components values. The security of the proposed encryption algorithm is simulated and analyzed from the histogram, correlation coefficient, information entropy, key sensitivity and differential attack. Experimental results show that the proposed image encryption algorithm is strongly sensitive to key and plaintext and can effectively resist exhaustive analysis, differential analysis, statistical analysis, etc. It is an encryption algorithm with high security and good encryption performance.*

Keywords *- Reversible scrambling matrix, chaotic sequence, diffusion, image encryption.*

I. INTRODUCTION

Image is one of the main carriers of information in the current era. With the fast development of Internet technology and image processing, more and more information is spread widely on the network in the form of the digital image. In an environment where the public gradually pays attention to information security and personal privacy, it is of great significance to ensure the security and confidentiality of images in the transmission process. Image information itself has its inherent attributes, such as a large amount of data, high correlation between adjacent pixels, a large degree of redundancy, etc. These inherent natures make the traditional encryption systems, such as IDEA, DES, AES, which are mainly oriented to text data, no longer adapt to the application of image information encryption. It is necessary to find more effective encryption algorithms for image data [1]. In the world, some unconventional methods are being studied and developed to encrypt and hide image information, among which image encryption algorithms based on chaos theory are adopted and intensively investigated. Chaos is a deterministic and random process in a nonlinear dynamical system. This process is not only aperiodic but also non-convergent, and it is very sensitive to the initial value and system parameters. Because a chaotic system has ergodicity, pseudo-randomness and sensitivity to initial value and system parameters, which are very similar to the confusion and diffusion properties of cryptography, it is particularly suitable for image information encryption applications [2-6].

Generally, the image encryption process based on a chaotic dynamical system consists of two processes: permutation (confusion) and substitution (diffusion). Through chaotic systems, the permutation process can disrupt the distribution of grey pixel values so as to show a good shuffling effect. It fully disorders the spatial positions of the plain-image pixels and achieves the effect of encryption. In the substitution process, the pseudorandom gray value sequences generated by chaotic systems are used to change the gray values of the image. Usually, the gray values of the pixels are changed one by one through the addition modular operation and bitwise XOR operation, and the change of the gray values will have the cumulative avalanche effect. It implies that one changes a certain pixel’s gray value in the plain image will make the gray value of the pixel processed subsequently change fundamentally as well. Consequently, it can effectively resist the attack of statistical analysis and differential analysis. A good substitution process should use a keystream that is closely related to the plain image. When encrypting different plain images, even if the same key is utilized, the encryption algorithm can generate different key streams. In this way, the encryption algorithm can resist the attacks of chosen plaintext and known plaintext.

There are a variety of transformations in the permutation process to achieve the scrambling effect of image encryption algorithm based on chaos, such as Arnold transform, Baker transform, standard transform and so on [2-5,7]. Generally speaking, these classical position scrambling transformation forms are relatively fixed, the keyspace is relatively small, and the security performance is not good enough. In order to overcome these shortcomings, this paper designs a novel image encryption algorithm to generate an invertible matrix on Z_n which is composed of the integers between 0 and $n-1$, and uses the invertible matrix generated as a transformation to realize pixel position scrambling or colour component value change of colour image. The generated matrix has random characteristics, and the range of matrix elements is widened, making the keyspace enlarge [7]. By constructing a reversible permutation matrix, the pixel coordinate set of the image is transformed to get a scrambled image. This algorithm can not only destroy the correlation between pixels but also quickly decrypt the restored image by constructing an inverse permutation matrix. However, it still retains the frequency distribution of the plain image, leaving a hidden danger to the confidentiality of the image. In fact, the pure spatial position scrambling encryption algorithms are vulnerable to plaintext attacks [8, 9]. Therefore, this paper will propose a diffusion process to enhance security and performance. The continuous signals generated by Chebyshev mapping are discretized to form chaotic sequences, which are unpredictable and aperiodic. Combining the method of pixel position and colour component scrambling with the method of diffusion using chaotic sequences, the resistance of simple scrambling algorithms to exhaustive analysis, statistical analysis and differential analysis can be greatly improved [10].

In this paper, reversible position scrambling transformation matrix and colour component transformation matrix are randomly generated Z_n, which are used for pixel position scrambling and colour component change at the same time. The encryption algorithm includes three steps: pixel position scrambling, pixel colour component scrambling and diffusion. In pixel scrambling, 2D pixel coordinates and 3D RGB colour component vectors are scrambled by using 2D and 3D reversible matrices based on modular N operation, where N denotes the size of the processed $N \times N$ image or the grayscale level of colour components, respectively. This method can not only destroy the correlation between adjacent pixels but also change the frequency distribution of the grey value of pixels and can effectively resist statistical analysis, including correlation analysis, histogram analysis, entropy analysis, etc. In order to improve the encryption performance of the image encryption algorithm, which only uses the scrambling method, the algorithm further diffuses the colour component value of the image. In the diffusion operation, the chaotic sequence generated by Chebyshev chaotic mapping is used as the keystream in the diffusion process, which makes the information of pixel colour component fully mixed and diffused, and destroys the gray value frequency distribution and correlation of plain-image. Chebyshev chaotic sequence is sensitive to the initial value, but its distribution is uneven, so it needs uniformization [11]. After homogenization, the Chebyshev sequence has more excellent chaotic characteristics, such as strong sensitivity of initial value and system parameters, good ergodicity and pseudorandomness. When the difference between the two initial values is greater 10^{-15}, the correlation between the two sequences is extremely weak, which greatly improves the keyspace of the image encryption algorithm. Therefore, the hybrid image encryption algorithm can effectively improve the information entropy of cypher-image and enhance the ability to resist differential attacks. Experiment results show that the proposed image encryption algorithm can effectively resist attacks such as exhaustive analysis, statistical analysis differential analysis, etc.

The remainder of this paper is organized as follow. The chaotic sequences used to control the scrambling and diffusion process in the proposed image encryption scheme are introduced in Section II. The proposed image encryption scheme is presented in Section III. Section IV shows the experimental results and performance analysis. Finally, some conclusions are drawn in Section V.

II. THE CHAOTIC SEQUENCES

The image encryption algorithm based on chaotic sequences is usually to make the original image information change into a cypher-image similar to random noise by bitwise XOR, cyclic shift and other operations between the chaotic sequence and the plain-image so as to achieve the good encryption effect. The chaotic sequences used in this paper will be generated by Chebyshev mapping.

The sequence-based on Chebyshev mapping has the characteristics of high complexity and strong initial value sensitivity. If the initial value changes with perturbation 10^{-15}, two weakly related sequences can be generated by Chebyshev mapping. Therefore, the chaotic sequences meet the cryptographic requirements of confusion and diffusion and therefore can be used for image encryption. The Chebyshev mapping equation is defined by

$$x_{n+1} = T_k(x_n) = \cos(k\cos^{-1} x_n) \qquad (1)$$

where $x_i \in [-1,1], i = 0,1,2,3,...$ k is the order of Chebyshev mapping? When k it is greater than 2, it has a positive Lyapunov exponent, and the system is in a chaotic state [11]. However, the sequence values generated by Chebyshev mapping are not uniformly distributed. It is difficult to guarantee the security of image encryption directly and needs homogenizing.

How to transform the chaotic sequence generated by Chebyshev mapping into a chaotic sequence with uniform distribution? In this paper, sequence mapping is used for such homogenizing. By substituting the Chebyshev chaotic sequence x_i generated by Eq. (1) into Eq. (2), it can be transformed into a uniformly distributed chaotic sequence T:

$$T_i = \text{floor}(\frac{2}{\pi}\arcsin\sqrt{\frac{x_i+1}{2}} \times 255), \qquad (2)$$

Where function “floor(x)” returns an integer not greater than x. After transformation, the chaotic sequence T basically obeys the discrete uniform distribution in the interval [0, 255]. The distribution histogram of Chebyshev sequence T generated by $k=3$, $x_0=0.96$ and Eq. (1) is shown in Fig. 1, and the statistical histogram of Chebyshev sequence subject to uniform distribution after the conversion by Eq. (2) is shown in Fig. 2. As can be seen from the histogram in Fig. 2, the transformed sequence is evenly distributed.

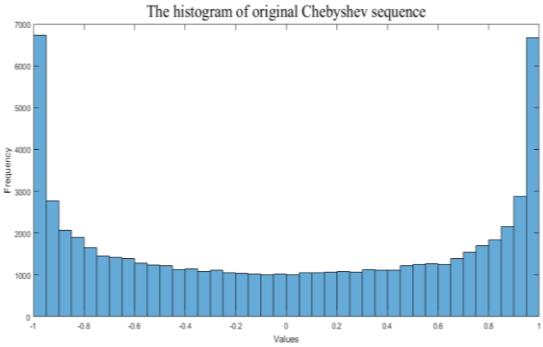


Fig.1 The histogram of the Chebyshev sequence.

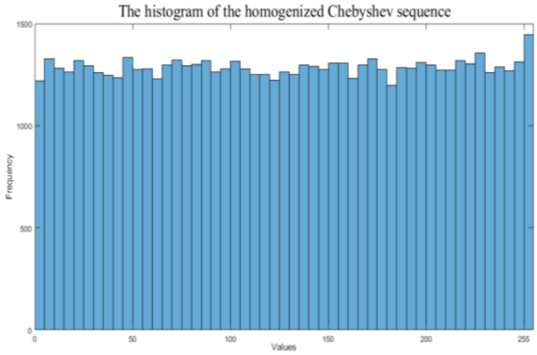


Fig.2 The histogram of the homogenized Chebyshev sequence.

III. THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The pixel scrambling based process encrypts the pixel positions of the plain image to get a disordered image so that people cannot read any information from it through vision or computer system. The image scrambling based on matrix transformation is realized by constructing a reversible permutation matrix based on the modular operation in the equivalent residue ring Z_n. Although the pixel position scrambling and colour component scrambling based on the reversible matrix can change the pixel position and its colour intensity and can hide the original image content from vision, histogram and correlation, its security needs to be strengthened due to the risks caused by the lower security of fixed reversible transformations matrix. Especially if we want to well resist the differential attack, we must have the mechanism of grey value diffusion. A good diffusion operation function can achieve the effect that a slight change only in one pixel of the plain image can greatly alter the whole image. Through diffusion, the correlations of colour components and pixels can be highly weakened, which can further enhance the encryption effect and security performance.

A. The construction of reversible transformation matrix

Set the size of the plain image to be $N \times N$, and the 2D pixel position transformation matrix A in Z_N is generated by the following steps:

Step 1. Generate 2D lower triangular matrix L, such that the determinant of L and N are mutual prime.

Step 2. Generate 2D upper triangular matrix U, such that the determinant of U and N are mutual prime.

Step 3. Multiply L and U to get the pixel position transformation matrix A by Eq. (3):

$$A = LU = \begin{pmatrix} l_{11} & \\ l_{21} & l_{22} \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ & u_{22} \end{pmatrix}. \qquad (3)$$

In fact, if the diagonal elements l_{11} l_{22} are both coprime to N, then the determinant of L and N are mutual primes. Similarly, if u_{11}, u_{22} are both coprime to N, then the determinant of U and N are mutual primes. As a result, l_{21} and u_{12} are arbitrary and can be chosen $\{0,...,N-1\}$.

The invertible transformation matrix B of 3D colour component vectors can be generated by Eq. (4):

$$B = WV = \begin{pmatrix} w_{11} & & \\ w_{21} & w_{22} & \\ w_{31} & w_{32} & w_{33} \end{pmatrix} \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ & v_{22} & v_{23} \\ & & v_{33} \end{pmatrix}, \qquad (4)$$

Where the lower triangular matrix W and the upper triangular matrix V are reversible matrices in Z_K, K is the grayscale level, for example, if the processed image is of 256 grayscale level, then $K=256$. Therefore the diagonal elements $w_{11}, w_{22}, w_{33}, v_{11}, v_{22}, v_{33}$ are all coprime to K, and the other elements of W and V are arbitrary and can be chosen in $\{0,...,K-1\}$.

The two-dimensional transformation changes the position correlation by scrambling the position space, and the three-dimensional transformation changes the gray values by scrambling the colour component space. It is known from the properties of number theory that if the determinant of the transformation matrix A and N are mutual primes, then the transformation matrix A is invertible in Z_n, and its inverse matrix A^{-1} can be obtained by multiplying the inverse matrix of U and L, that is,

$$A^{-1} = U^{-1} L^{-1} \ mod \ N .$$

The inverse matrices L^{-1}, U^{-1} of the lower triangular matrix L and the upper triangular matrix U Z_n are easy to obtain by fast algorithms [7]. The same operation can be handled for the inverse matrix B^{-1} by

$$B^{-1} = V^{-1}W^{-1} \; mod \; K \, .$$

As for the generation of elements in upper and lower triangular matrices, we perform the following implementation. Chebyshev mapping is used to generate the chaotic sequence. After quantization, the elements of L , U , W , V are generated. Among them, the diagonal elements of L , U should be coprime to N ; the elements of W , V should be coprime to K . Other elements can be selected at $\{0,...,N-1\}$ or $\{0,...,K-1\}$ arbitrarily. In order to make the encryption algorithm related to the content of plain-image and achieve the effect of one-time pad encryption, the elements of the pixel position scrambling encryption transformation matrix in this paper will be designed to be related to the plain-image. We sum all elements of the pixel colour component matrix of the plain image to obtain the image feature and standardize the processing to make the feature value belong to [0,1]. Then, the normalized feature is used to be the initial value of the Chebyshev chaotic sequence. The chaotic sequence is generated iteratively from the generated invertible transformation matrix, and the generated elements L U are quantized. It is related to the content of the plain image. Different plain images will yield different features, so the position scrambling transformation matrix is also different, and the adaptive encryption is realized. Moreover, this feature can be obtained through the content of the processed image in the decryption process and does not need to be transmitted as an additional key. Regarding the elements of the invertible transformation matrix and the pseudorandom chaotic sequence for diffusion, we use the original key, i.e. the initial value x_0 of the Chebyshev mapping and the system parameter k , to generate them accordingly.

B. The scrambling of pixel positions and colour components

Image scrambling changes the spatial distribution of pixels of the whole image by scrambling the spatial position of pixels so as to remove the strong correlation between adjacent pixels of the plain image. It can make the whole image look disordered, and the information of the original plain image cannot be seen visually. The pixel position scrambling is implemented by using some reversible chaotic mapping to transform the coordinate vectors of the image pixel positions. Assuming the size of the image is $N \times N$, the scrambling transformation matrix can be generated by Eq. (3). By Eq. (5), one can realize the scrambling of pixel positions.

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} l_{11} & \\ l_{21} & l_{22} \end{pmatrix} \begin{pmatrix} u_{11} & u_{12} \\ & u_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N, \qquad (5)$$

where $(x,y), x,y = 0,1,...,N-1$ represent the position coordinates of the plain-image pixels, and $(s,t), s,t = 0,1,...,N-1$ represent the position coordinates of the scrambled image pixels. The invertible transformation matrix transforms the pixel from position (x,y) to position (s,t) . When the positions of the whole image are all transformed, a round of scrambling is realized. One can disorder the image several rounds so as to increase the level of disorder.

The colour components of a colour image constitute a three-dimensional matrix, and the confusion of colour components can be realized by reversible transforming the R, G and B component values of the corresponding positions of image pixels. The specific transformation is realized by Eq. (6).

$$\begin{pmatrix} r' \\ g' \\ b' \end{pmatrix} = \begin{pmatrix} w_{11} & & \\ w_{21} & w_{22} & \\ w_{31} & w_{32} & w_{33} \end{pmatrix} \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ & v_{22} & v_{23} \\ & & v_{33} \end{pmatrix} \begin{pmatrix} r \\ g \\ b \end{pmatrix} \bmod K \, , \quad (6)$$

where $(r,g,b), (r',g',b')$ represent the colour components of the original image and the scrambled image.

C. Diffusion based on chaotic sequence and two-way cyclic bitwise XOR operation

Two Chebyshev chaotic sequences after homogenization are used as the diffusion key streams, which are recorded as S and M . After the key streams are generated, the scrambled pixels are processed by a two-way bitwise XOR operation to spread the scrambled pixel information to the whole encrypted image. For the convenience of writing, we will record $N \times N \times 3$ as n in the sequel.

The encryption process of pixel diffusion. The R, G and B colour component matrices are spliced, and then the spliced matrix is vectorized so that it becomes a one-dimensional vector P of length n . The bi-directional diffusion strategy is applied to achieve good encryption performance [10]. We first perform the forward diffusion by using the chaotic keystream S , and the primary cypher-image T is obtained. And then, the primary cypher-image and the chaotic sequence M are correspondingly reversely diffused to get the final cypher-image Q . The forward diffusion is shown in Eq. (7).

$$T_1 = P_1 \, , \; T_i = T_{i-1} \oplus S_i \oplus P_i \, , \; i = 2,3,\cdots,n \, . \qquad (7)$$

It can be seen from Eq. (7) that in the process of forwarding diffusion, only the pixel information of P_1 can be diffused to all cypher-image pixels, while P_2 can only be diffused to $T_2 \sim T_n$, that is to say, in the process of forwarding diffusion, the later the pixel to be diffused, the worse the effect will be. It is necessary to carry out another reverse diffusion to improve the diffusion effect. The corresponding encryption formula is shown in Eq. (8). The initial value of this formula is the last element of the vector:

$$Q_n = T_n \, , \; Q_i = Q_{i+1} \oplus M_i \oplus T_i \, , \; i = n-1,\cdots,2,1. \quad (8)$$

D. The encryption algorithm

The encryption process includes pixel position scrambling, colour component scrambling and colour component value bidirectional diffusion. Suppose the plain-image is I , its mathematical model is expressed as three-dimensional matrix sized $N \times N \times 3$. The specific algorithm is described as follows:

Step 1. Set the initial value x_0 x_0' and system parameter k of the Chebyshev mapping. Read the image data and get the three-dimensional matrix I. The sum of all element values of the matrix is calculated to get the features t_0, t_1 of the image by Eq. (9).

$$t_0 = (\sum_{k=0}^{2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j,k)) / (3 \times N \times N \times 255),$$

$$t_1 = \sum_{k=0}^{2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j,k) \bmod 30. \quad (9)$$

Step 2. Change x_0 to $y_0 = (x_0 + t_0) \bmod 1$, use y_0 and k iterate the Chebyshev mapping $t_1 + 20$ times, discard the transition points so that the values of the subsequent iteration points have better chaotic characteristics. Take the following iterative points $y_1, y_2, ..., y_m$, where m is some appropriate positive integer. $y_1, y_2, ..., y_m$ Are quantized by Eq. (10) to obtain an integer sequence $Y_1, ..., Y_m$ whose values are in $\{0, ..., N-1\}$, from which the elements l_{11}, l_{22}, l_{21}, u_{11}, u_{22}, u_{12} satisfying the required conditions are selected.

$$Y_i = floor(y_i \times 10^{10}) \bmod N, \ i = 1, ..., m. \quad (10)$$

Step 3. Use Eq. (5) to scramble the pixels positions of the colour image. If the pixel positions (x, y) of the plain-image are transformed into the position (s, t), but the R, G, B components at the position (x, y) of the plain-image to the R, G, B components at the position (s, t) of the scrambled image respectively to get the scrambled colour image J.

Step 4. Use the initial value x_0' and system parameter k to iterate Chebyshev mapping, and discard the first 30 transition points. Take the following points and quantize them by Eq. (11) to get the pseudorandom integer sequence $S_1, ..., S_n$ in $\{0, ..., K-1\}$. The elements W V satisfying the required conditions are selected orderly.

$$S_i = floor(x_i \times 10^{10}) \times 255 \bmod K, \ i = 1, ..., n. \ (11)$$

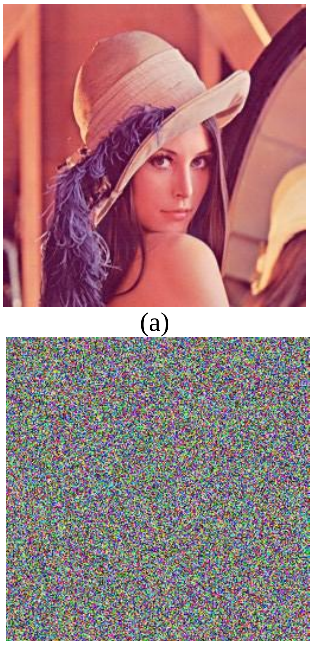
Step 5. Use Eq. (6) to scramble the colour components of the scrambled colour image J. It will change the colour component values at any pixel of the colour image J. The yielded colour image matrix is transformed into a one-dimensional vector P with a length of n.

Step 6. Use Eqs. (7) and (8) to perform two-way bitwise XOR diffusion on the vector P to get another vector Q. The final colour cypher-image C is obtained by converting the vector Q to one 3D matrix with size $N \times N \times 3$.

The decryption algorithm is the inverse process of the encryption algorithm. The decryption key is consistent with the encryption key, and we will not be described it in detail here.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

Lena is selected as the test image for encryption and decryption experiments. In the experiment, the Chebyshev map is used as the chaotic map to generate chaotic sequences. The initial values of forwarding diffusion, back diffusion and system parameter are set to be $x_0 = 0.96$, $x_0' = 0.583$, k = 3 respectively. A Chebyshev sequence with better pseudo-randomness is obtained by homogenizing the original chaotic sequence, which is used to generate the reversible transformation and pseudorandom colour component value sequences required by the encryption algorithm. The encrypted cypher image is shown in Fig. 3.


(a)

(b)

Fig. 3 Plain-image Lena and its cypher-image.

A. Histogram analysis

One can see the distribution of the gray values of one image intuitively through its histogram. If the histogram of the cypher-image is closer to the uniform distribution, it indicates that the encryption effect is better, and the opponents are difficult to obtain useful information related to plain-image. After scrambling and diffusion, the colour vectors composed of R, G, and B colour components have changed greatly. The histograms of R, G and B colour components for the plain-image and the cypher-image are demonstrated in Fig. 4.

According to Fig. 4, one can see that the histograms corresponding to the R, G, B colour components for the cypher image are significantly different from those for the plain image, and the histograms become flat and even indicating that the histograms are very close to the uniform distribution. The proposed image encryption algorithm can efficiently resist histogram analysis.

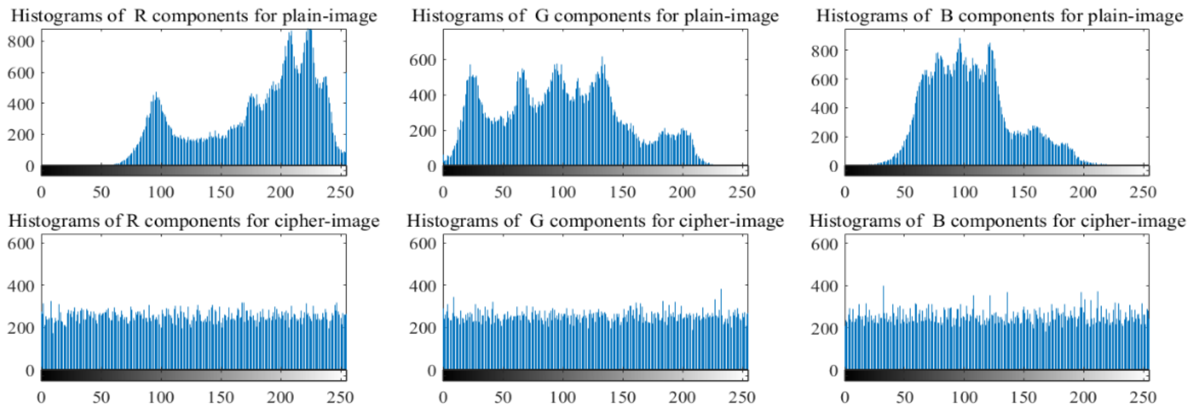


Fig. 4 Histograms of R, G, B colour components for plain-image and cypher-image.

B. Correlation analysis

The correlation of adjacent pixels reflects the correlation degree of pixel values in adjacent positions of the image. A good image encryption algorithm can effectively reduce the correlation of adjacent pixels. Generally, T pairs of adjacent pixels are selected from the vertical, horizontal and diagonal directions of the image, and then the correlation coefficients of the adjacent pixels are calculated from vertical, horizontal and diagonal directions. The formula for the calculation of the correlation coefficient is defined by Eq. (12).

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad (12)$$

$$\operatorname{cov}(x,y) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y)),$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2, \; E(x) = \frac{1}{T}\sum_{i=1}^{T}x_i,$$

Where x_i and y_i represent the pixel values of a pair of adjacent pixels. The large correlation coefficient implies that the correlation between adjacent pixels is strong, and the small correlation coefficient implies that the correlation between adjacent pixels is weak.

It follows from the results in Table 1 that the correlation coefficients in all directions of plain-image are greater than 0.9, implying significantly correlated. The absolute value of the correlation coefficient in all directions of cypher-image is less than 0.026, which is close to 0. Therefore the correlation analysis shows that the proposed image encryption algorithm greatly deduces the relationship between adjacent pixels. The correlation of adjacent pixels can be visualized in Fig. 5 as well. From Fig.5, one can see that the pixels in the three directions of vertical, horizontal and diagonal in the plain-image are concentrated in the diagonal direction, indicating that the correlation between pixels is strong. However, the pixels in the three directions of the cypher-image cover the whole region more evenly, which shows that the correlation between the pixels of the cypher-image is very weak, which is close to randomness.

Table 1. The correlation coefficients between adjacent pixels

	Vertical	Horizontal	Diagonal
Plain-image	0.9561	0.9768	0.9320
Cypher-image	0.0122	-0.0106	-0.0119

C. Information entropy analysis

The information entropy of the image is a kind of statistic to test the uncertainty, reflecting the average information in the image, and also can be used to describe the degree of the histogram of the image close to the uniform distribution. When the amount of information in the image is larger, the entropy value is larger, and the image is more noise-like. When the amount of information in the image is smaller, the entropy value is smaller, and the image is smoother. Since the range of grey values is [0, 255] and the total number of gray levels is 256, the value range of entropy is [0, 8]. The calculation of information entropy is shown in Eq. (13).

$$H(X) = -\sum_{i=0}^{L-1} P(X_i)\log_2 P(X_i) \qquad (13)$$

where L is the grayscale level (for example, 256) and $P(X_i)$ denotes the frequency of information X_i. The entropy values of plain-image and its cypher-image are calculated using Eq. (13). The entropy of the cypher-image is 7.9991, which is very close to 8, implying the cypher-image is very close to randomness. The possibility of being attacked is very slight, and it is difficult to disclose the information.

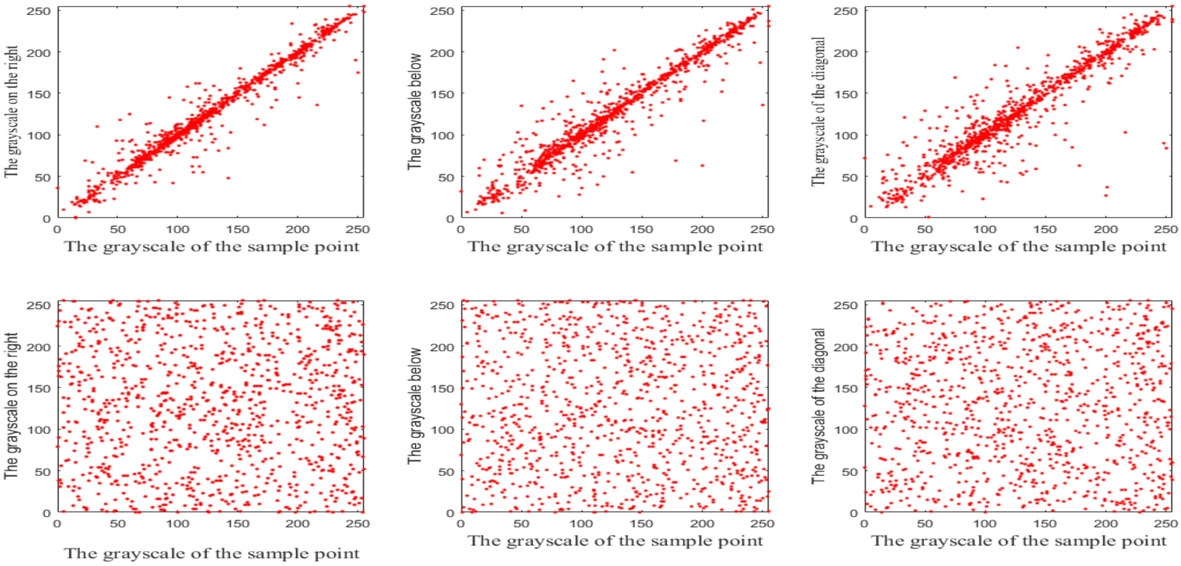


Fig. 5 The correlation distribution of horizontal, vertical and diagonal directions

D. Key sensitivity and differential attack

The key sensitivity refers to how many differences can be generated when the key is changed slightly in the encryption process. If a minor perturbation of the cypher key will make the ciphertext greatly change, the corresponding key is strongly sensitive; otherwise, it is weakly sensitive. An ideal cryptosystem requires that the key should be as strong as possible. The differential attack is a kind of chosen-plaintext attack. By making a small change to the plaintext, one can analyze the difference between two ciphertexts to find some useful links between the ciphertext and the plaintext. An ideal cryptosystem should be robust enough against differential attacks. In order to test the sensitivity of the key, the change rate of the corresponding cypher-image obtained by the image encryption algorithm with the change of the key and the ability to resist differential attack is calculated. Here, the unified average change intensity UACI and the pixel number change rate NPCR are two common indices to measure both the key sensitivity and the resistance ability against differential attack. The calculation formulae are shown in Eq. (14) –Eq. (16).

$$NPCR = \frac{1}{N \times N} \sum_{i,j=1}^{N} D(C_1(i,j), C_2(i,j)) \times 100\% \, , \quad (14)$$

$$UACI = \frac{1}{N \times N} [\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100\% \, , \quad (15)$$

$$D(C_1(i,j), C_2(i,j)) = \begin{cases} 0 & , \; C_1(i,j) = C_2(i,j) \\ 1 & , \; C_1(i,j) \neq C_2(i,j) \end{cases} \quad (16)$$

where C_1 C_2 denote the two cypher images encrypted by the original key and the slightly changed key.

Key sensitivity

The theoretical expectation of the encrypted image is NPCR = 99.5804, UACI = 33.5692 [12]. In the simulation, the key parameters are slightly perturbed to get the corresponding cypher image. The perturbation for the initial values x_0, x_0' and the system parameter k of the chaotic system are shown in Table 2. The NPCR and UACI values are calculated and shown in Table 2 as well. The NPCR value and UACI values in Table 2 are close to the ideal expected values, respectively. It shows that when the key changes slightly, more than 99.5% of the pixels in the cypher image will change. That is, the key sensitivity is strong enough to resist brute-force attacks.

Table 2. The calculated NPCR and UACI

	NPCR	*UACI*
$x_0 + \Delta\mu$	99.5967	33.4852
$x_0 - \Delta\mu$	99.5931	33.4487
$k + \Delta\mu$	99.6048	33.4431
$k - \Delta\mu$	99.6292	33.4229
$x_0' + \Delta\mu$	99.6195	33.5224
$x_0' - \Delta\mu$	99.6012	33.3782

Differential attack.

For a pixel whose gray value is between 0 and 254, we change its gray value by adding 1. For one pixel with a gray value of 255, we change its value to be 254. After the last change, we encrypt the two plain images with the same key. Compare the cypher images and calculate the NPCR and UACI of the two cypher images. We perform 100 times of tests. The average NPCR is 99.4862%, the minimum is 99.0987%, and the maximum is 99.8698%. The average UACI is 33.4743%, the minimum value is 33.3355%, and the maximum value is 33.6026%. The results show that the encryption algorithm has a good effect on differential attacks.

V. CONCLUSION

In this paper, one novel image encryption algorithm using the image pixel position scrambling, colour component value scrambling and diffusion is proposed. The main characteristics of the method are as follows: 1) In the process of scrambling of pixel positions and colour component values, we utilize reversible transformation matrices to realize the scrambling. Both the pixel position and colour component scrambling eliminate the correlation of adjacent pixels to a large extent, making it difficult for people to peep at the information of the plain image from the cypher image even with the help of vision and computer system. The reversible matrix used in the position scrambling process is related to plain-image, so the encryption algorithm is more effective to resist the attack of chosen-plaintext and known-plaintext. 2) In pixel value diffusion, Chebyshev chaotic sequences with uniformization make the cypher-image more random and disordered, further enhance the encryption effect, and make the encryption algorithm more effective against various attacks such as statistical analysis, differential analysis, chosen-plaintext attack, etc.

ACKNOWLEDGMENT

This research is supported by Innovation and Entrepreneurship Training Program for College Students in Guangdong Province.

REFERENCES

[1] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley and Sons, New York, (1996).

[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998) 1259–1284.

[3] G. Chen, Y. Mao, C. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons and Fractals, 21(2004) 749–761.

[4] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011) 5290-5298.

[5] Patidar Vinod, N. K. Pareek, K. K. Sud, A new substitution–diffusion-based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulations, 14 (2009) 3056-3075.

[6] R. Ye, M. Ge, P. Huang, H. Li, A Novel Self-adaptive Colour Image Encryption Scheme, International Journal of Computer Trends and Technology, 2016 40(1) 39-44.

[7] L. Shao, Z. Qin, X. Heng, H. Gao, Solution for the inverse problem of matrix transform-based image scrambling. Acta Electronica Sinica, 7(2008) 1355-1363.

[8] S. Li, C. Li, G. Chen, N. G. Bourbakis, K. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication, 23(2009)212-223.

[9] X. Zhao, G. Chen, D. Zhang, et al., Decryption of pure-position permutation algorithms. Journal of Zhejiang University (Science Version), 5(7) (2004) 803-809.

[10] X. Zhang, J. Chen, J. Peng, M. Xi, Image encryption algorithm based on complex, chaotic sequences, Application Research of Computers, 36(2019) 3396-3400.

[11] L. Lei, G. Ma, X. Cai, H. Shi, Study of chaotic sequence based on Chebyshev mapping, Computer Engineering, 35(2009), 4-6.

[12] H. Kwok, W. Tang, A fast image encryption system based on chaotic maps with finite-precision representation, Chaos, Solitons and Fractals, 32(2007) 1518-1529.