Research and Improvement of Image Encryption Algorithms Based on Chaos

Ruoyu Wang, Sanxing Cao
Collaborative Innovation Center, Communication University of China, Beijing 100024, China
1741940195@qq.com

Abstract. Due to user privacy protection and other demands, image encryption is always a hot spot in the research field. In view of these problems, this article proposes a chaotic image encryption algorithm, which is named permutation-diffusion algorithm. Specifically, the image of the pixels is permuted, so that the pixel position changes, and then spreads, to change the pixel value. It can be observed from the test results that the algorithm is better in terms of efficiency and safety, compared with the state of the art.

1. Introduction
In recent years, due to the development of communication technology, image encryption technology has become a hot research topic. The traditional encryption technology has many drawbacks. A permutation-diffusion algorithm based on chaotic image proposed by Fridrich has attracted people's attention. The algorithm can be divided into two parts: permutating first and then diffusing. This algorithm is quickly adopted by many studies. For example, a set of encryption algorithm proposed by Chen et al. in the literature has high security. In this paper, an algorithm is proposed, which is further improved on the basis of security, and the advantages of this algorithm are verified by experiments.

2. Algorithm Introduction

2.1. Algorithm elicited
At present, a large number of literature show that many image encryption methods only use chaotic sequence to produce permutating address matrix, only permutating the location of the pixels, the gray histogram of the image has not changed, and the distribution of the pixels is the same as the original image, so it is easy to be deciphered by attackers, and the security is not high. To improve these schemes, diffusion function is introduced. The specific expression of the diffusion function is as follows:

\[
\begin{align*}
    c(k) &= f(x_k, u) \\
    q(k) &= c(k) \oplus \left[\Phi(k) + q(k-1) + c(k)\right] \mod N
\end{align*}
\]

Among them, \(c(k)\) is a natural chaotic sequence generated by chaotic mapping \(f(x_k, u)\) which is sampled and amplified in an appropriate proportion. \(\Phi(k)\) is the pixel to be encrypted, \(q(k)\) is the encrypted pixel, \(q(k-1)\) is the former encrypted pixel, and \(N\) is the gray level of the image.
The introduction of diffusion function in encryption scheme can spread the influence of each bit of plain image to the whole cipher image, and change the statistical characteristics of plain image to a great extent, so as to make up for the shortcomings of simple pixel permutating encryption algorithm and effectively resist statistical attacks.

It is found that the histogram distribution of the image can also be changed when the gray value is substituted, and the algorithm is relatively simple, but it can achieve the same effect as the diffusion function. If the pixel value substitution is introduced into the pixel position transformation, it can make up for the shortcoming that the pixel position transformation does not change the histogram distribution of cipher image, so a new chaotic image encryption algorithm proposed in this paper is introduced.

2.2. Algorithmic thought

This paper first encrypts the gray-scale image by chaos. First, the pixel value of the image is converted to eight-bit binary, and only the first four bits are selected for permutating. Then, the permutated image will be diffused by XOR at bit-level. That is, the plain image signal and the chaotic signal are operated by XOR at bit-level. The result will be a cipher image with good effect, which can resist a certain degree of attacks. For the color image, it can be divided into three basic colors: red, green and blue. Each layer can be encrypted by gray image encryption method. Finally, the results are superimposed.

A set of algorithms presented in this paper can be presented simply with the block diagram of Fig.1. Such a set of algorithms can be roughly divided into four steps to decompose and describe, as follows:

The first step is to split the color image into three parts: R, G and B. For any part of them, the pixel value is converted from decimal to octal binary, and only the first four bits are taken out of reserve.

The second step is to adopt the characteristics of Chaotic Circuit System. First, a set of numerical values are generated by differential function, and then a certain number of values can be obtained from the starting position specified by the key by using the results of differential equation. Then, these values are reordered to generate the corresponding permutating relationship. Then, the first four bits of the permutated pixel values are permutated by using the array.

The third step: Using Logistic chaotic mapping, the algorithm is first diffused by taking a set of keys, and then the mapped value is combined with the plain image by XOR at bit-level, which can change the pixel value.

The last Step: Finally, we can rearrange the pixel values that have experienced the permutation-diffusion operation to form the matrix arrangement necessary for image generation. At the same time, we need to superimpose the R, G and B layers together, so that we can get an encrypted image.
For decryption, it is actually the inverse process of encryption. The reader can decrypt the information of plain image only by returning to the opposite path. Because of the limitation of space, it will not be repeated here.

3. Performance Analysis and Testing

3.1. Key space and key sensitivity analysis

The Chen's chaotic system and Logistic mapping used in this paper use the corresponding keys respectively. Combining these secret keys, we can realize the system's confidentiality. Next, we verify the sensitivity of the secret keys through experimental comparison.

In order to see the contrast effect conveniently, this experiment adopts five groups of key values to encrypt the same image. The images encrypted by the first group of keys were taken as blank control group, and the images encrypted by the other four groups of keys were subtracted from the control group in turn to observe the difference of encryption effect between different keys. The results are as follows:

![Fig.2 Differences between different keys](image)

From the above results, we can see that there are great differences between encrypted images due to the different secret keys, which shows that the system has a high sensitivity to key.

In addition, we can also introduce the concepts of NPCR (number of pixels change rate) and UACI (unified average change intensity). The two measurements are mainly used to evaluate the effect of the change of one pixel in the original image on the whole encrypted image. The calculation methods of NPCR and UACI are as follows:

\[ D(i,j) = \begin{cases} 0 & \text{if } P_1(i,j) = P_2(i,j), \\ 1 & \text{if } P_1(i,j) \neq P_2(i,j), \end{cases} \]

\[ \text{NPCR} = \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\%. \]

\[ \text{UACI} = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{|P_1(i,j) - P_2(i,j)|}{L - 1} \times 100\%. \]

Among them, \( P_1(i, j) \) and \( P_2(i, j) \) are the first (i, j) pixel values of two images \( P_1 \) and \( P_2 \) respectively. \( W \) and \( H \) are the rows and columns of the image pixels, and \( L \) is the maximum of the pixels (i.e. 256). Lena's chart is still used for testing. The calculated NPCR and UACI values are listed in Table 1.

| Keys          | NPCR    | UACI    |
|---------------|---------|---------|
| The first set of keys | 99.56%  | 33.47%  |
| The second set of keys | 99.53%  | 33.44%  |
| The third set of keys  | 99.67%  | 33.40%  |
| The forth set of keys  | 99.60%  | 33.46%  |
| The fifth set of keys   | 99.65%  | 33.41%  |

Table 1 NPCR and UACI after image encryption
From Table 1, it can be seen that the effect of encrypting the same picture with different keys is different, and the NPCR and UACI values obtained are obviously different, which shows that the algorithm has high key sensitivity again.

### 3.2. Histogram analysis

Write the above program into MATLAB. While the encrypted and decrypted image is simulated, the distribution of each pixel of RGB tricolor can also be displayed. The result is presented in the form of histogram.

As shown in Fig.3, it can be seen that the plain color image with uneven RGB distribution can be changed by Logistic mapping after encryption algorithm. After a new round of permutating, the distribution of the pixel values of each point will become very uniform, so it will become even in the histogram. Similarly, when the decryption program is executed, it is the inverse process of the encryption algorithm, and the RGB tricolor will be disturbed again, so the distribution of the tricolor will become uneven, that is to say, the tricolor distribution of the plain image will be restored.

![Fig.3 Histogram of RGB components of plain-cipher-decipher images](image)

### 3.3. Pixel correlation analysis

In the process of encrypted transmission, pictures are often attacked by malicious external attacks. When the correlation between adjacent two pixels is strong, the attacker can easily break the encrypted image. Therefore, we need to do an operation to reduce the correlation between them. For this reason, we give the following set of formulas.

\[
\text{cov}(x,y) = E((x - E(x))(y - E(y)))
\]

\[
R_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x) \cdot D(y)}}
\]

Among them, x and y are the pixel values of two adjacent pixels in the image, E(x) is the mathematical expectation of x, D(x) is the variance of x, and \(\text{cov}(x, y)\) is the covariance of x and y.

We choose three directions of Lena image: horizontal, vertical and diagonal to calculate the correlation between pixels. For the convenience of calculation, only one row/column/diagonal line is selected to calculate the correlation. The numerical results are shown in Table 2, and the results of point chart are shown in Fig.4.
Table 2 Correlation of adjacent pixels

| Direction  | Plain image | Cipher image |
|------------|-------------|--------------|
|            | R  | G  | B  | R  | G  | B  |
| Horizontal | 0.9361 | 0.9593 | 0.9340 | -0.0369 | 0.0251 | -0.0197 |
| Vertical   | 0.9607 | 0.9481 | 0.9235 | -0.0086 | 0.0319 | 0.0294 |
| Diagonal   | 0.8945 | 0.9307 | 0.9035 | -0.0158 | 0.0147 | 0.0200 |

Fig. 4 Comparisons of inter-pixel correlation before and after encryption

From Table 2 and Fig. 4, it can be seen intuitively that before the image is not encrypted, there is a strong correlation between the pixels, but after the encryption, the correlation between the pixels of cipher image decreases significantly, which shows that the algorithm can reduce the correlation of the pixels very well, and then can effectively resist the attack.

3.4. Information entropy

In order to further illustrate the advantages of encryption algorithm, we introduce the concept of information entropy, which is used to describe the degree of pixel confusion. The specific formula is as follows.

\[ H(s) = - \sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i) \]

The above formula is the formula for calculating information entropy, where \( s \) is the information source, \( N \) is the number of bits representing the symbol \( s_i \), and \( P(s_i) \) is the probability of the symbol \( s_i \).
For a true random source consisting of $2^N$ symbols, the entropy is $N$. Therefore, for a secure encryption system, the theoretical value of the entropy of the encrypted image with 256 gray levels should be 8. When the value is 8, the pixels are cluttered to the point where there is no correlation. Therefore, the closer the pixel value of the picture is to 8, the better the encryption effect.

In order to test the encryption effect, we test Lena's image and calculate its entropy values before and after encryption, respectively. The results are listed in Table 3.

| Test image | Plain image | Cipher image |
|------------|-------------|--------------|
| Lena       | 6.833787    | 7.999264     |

From the data in the table, it can be seen that the entropy value of the original graph is low, and when the algorithm is used for encryption, the entropy value reaches a satisfactory level, which shows that the proposed algorithm greatly reduces the possibility of outside attacks.

4. Conclusion
In this paper, the image encryption algorithm is studied and a chaotic image encryption algorithm, which is named permutation-diffusion algorithm, is proposed. Specifically, the pixels of the image are permuted to change the position of the pixels, and then diffused to change the value of the pixels. From the experimental analysis, it can be concluded that the performance of the algorithm is very good in terms of encryption effect and security.

Because the image encryption algorithm is a developmental subject, this paper only simulates the existing technical requirements. However, with the development of modern technology, many of the existing security algorithms which are considered to be excellent may be cracked in the future. Therefore, such algorithms must be constantly improved.

Acknowledgments
The work of this paper was funded by the Interdisciplinary Team Project of the "Double First-Class" Construction Project of the Communication University of China, which is named "Virtual Reality of New Media Independent Innovation Capability Improvement and Application Promotion" (No. YLTS180522).

References
[1] Li Shujun, Chen Guanrong, et al. Chaos-based encryption for digital images and videos[M]. Multimedia security handbook. CRC Press, 2005, Chap.4.
[2] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps[J]. Int. J. Bifurcation Chaos, 1998,8(6):1259–1284.
[3] Omid Mirzaei, Mahdi Yaghoobi, et al. A new image encryption method: parallel sub-image encryption with hyper chaos[J]. Nonlinear Dyn 2012;67(1):557–566.
[4] Ye Guodong, Wong Kwok-Wo. An efficient chaotic image encryption algorithm based on a generalized Arnold map[J]. Nonlinear Dyn 2012;69(4):2079–2087.
[5] Ye Guodong, Wong Kwok-Wo. An image encryption scheme based on time-delay and hyperchaotic system[J]. Nonlinear Dyn 2013;71(1–2):259–267.
[6] Zhang Xuaping, Zhao Zhongmeng. Chaos-based image encryption with total shuffling and bidirectional diffusion[J]. Nonlinear Dyn 2014;75(1–2):319–330.
[7] Wang Xingyuan, Guo Kang. A new image alternate encryption algorithm based on chaotic map[J]. Nonlinear Dyn 2014;76(4):1943–1950.
[8] Hua Zhongyun, Zhou Yicong, et al. 2D sine logistic modulation map for image encryption[J]. Information Sciences, 2015, 297(C):80-94.
[9] Li Chunhua, Luo Guangchun, et al. Chaotic image encryption schemes: a review[C]. International Conference on Electrical, Automation and Mechanical Engineering, 2017, 86:261-263.
[10] Chen Junxin, Zhu Zhiliang, et al. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach[J]. Commun Nonlinear Sci Numer Simulat, 2015, 23(1-3):294–310.