Research on Image Scrambling Method Based on Combination of Arnold Transform and Exclusive-or Operation

Hanmin Ye[1] ,Shiming Huang[1] ,Wenjie Liu[1]
1. School of Information Science and Engineering, Guilin University of Technology
Guilin, China
yehanmin@163.com, 1573930865@qq.com, 2929502268@qq.com

Abstract*—Aiming at the encryption problem in digital image information hiding process, an image scrambling algorithm based on combination of Arnold transform and exclusive-or operation is proposed. The algorithm first uses the Arnold transform to change the pixel position of the original image to obtain the initial scrambled image A, and then performs a bitwise exclusive-or operation on each pixel in the image A with its prior pixel. Finally, the gray value of the image is changed again by the high and low bit transposition operation to improve the image scrambling effect, and the final scrambled image S is obtained. The experimental results show that compared with Arnold's existing scrambling methods, the scrambled image is not only more difficult to recognize subjectively, but also has a significant change in its histogram, which is more suitable for the encryption of digital images and subsequent experiments.

***Keywords*—image scrambling; Arnold transform; exclusive-or operation**

I. Introduction

With the rapid development of multimedia technology and storage technology in the digital age and the increasing network bandwidth, more and more digital images are transmitted on the network every day, and gradually become one of the main means for people to obtain information, which also makes images the security of transmission is becoming more and more prominent. The digital images transmitted on the network involve personal privacy, corporate interests, and some even military secrets, which involve national security. Therefore, reliable digital encryption of digital images transmitted in the network has attracted more and more scholars' attention[1~4]. It is a research topic worthy of further study.

How to encrypt the image to ensure that the image is completely and safely arrived at the receiver has become an important research direction. Digital image scrambling is to transform a digital image into a chaotic image, which is a chaotic image. It processes the image from pixel position, gray value, etc., disturbs the components of the image, and destroys the image. Correlation. Even if an illegal interceptor obtains an image, the true face cannot be recognized from the perspective of the "human eye", and the receiver can restore the original image from the chaotic image even if the scrambling algorithm is known. The image scrambling technology can be directly used to protect images on the one hand, and can also be used as pre-processing before information hiding, and the gray distribution of secret information is disturbed, so that it is more like noise into the image file. Such an encryption method improves the security of image transmission to a certain extent.

Therefore, a new method based on traditional Arnold transform image scrambling and XOR operation is proposed. The method first performs Arnold transform scrambling on the original image to change the position of the pixels in the image. Then, the bitwise XOR operation is performed to make the image. The position of the pixel is rearranged again, and the corresponding pixel gray value also changes. The simulation results show that compared with the traditional image scrambling algorithm, the image of the proposed algorithm has changed greatly. The histogram distribution is better than the histogram of the traditional scrambled image, and it is evaluated according to the scrambling effect. The method proves the feasibility of the algorithm.

II. The Reversible Operation of Scrambling Images Based on Arnold Transform and XOR Operation

A. Arnold Transform Scrambling

Arnold transform is an important technique[5~6] for image scrambling, which achieves image scrambling by changing the pixel position. The definition of the Arnold transformation is:

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod(N) \tag{1}$$

Convert to polynomial is:

$$\begin{cases} X=(x+ay)\bmod(N) \\ Y=(bx+(ab+1)y)\bmod(N) \end{cases} \tag{2}$$

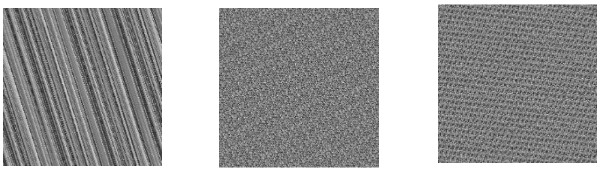
The inverse transformation formula and transformation polynomial are:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} ab+1 & -a \\ -b & 1 \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \operatorname{mod}(N) \tag{3}$$

$$\begin{cases} x = \left(\left(ab+1\right)X - aY\right)\operatorname{mod}(N) \\ y = \left(-bX + y\right)\operatorname{mod}(N) \end{cases} \tag{4}$$

Where (x,y) is the pixel coordinates of the original image,(X,Y) is the transformed coordinates of the pixel (x, y), mod() is the modulo operation, and N is the side length of the original image, a, b are given parameters. Given a=3; b=5, the number of iterations is 10, which can achieve better scrambling effect.

We experimented with 256×256 grayscale image Lena and simulated it in the environment of MATLAB R2016b. The Arnold transform scrambled image after different iterations[7] is shown in Fig.1.



(a)iterations 1 (b)iterations 5 (c)iterations 10

Fig. 1. The Arnold transform scrambling images with different iterations

B. Introduction of XOR Operation

XOR is a binary-based mathematical operator that is mainly used for logical operations. The mathematical symbol is represented as "$\oplus$" and the computer symbol is "xor". Its algorithm is:

$$a \oplus b = \left(\neg a \wedge b\right) \vee \left(a \wedge \neg b\right) \tag{5}$$

If the two values a and b are not the same, the XOR result is 1. If the two values a and b are the same, the XOR result is 0. The XOR operator is characterized by the fact that the number a is twice XOR the same number b ($a = a \oplus b \oplus b$) is still the original value a.

By analyzing the above-mentioned XOR operation[8], the XOR operation is reversible, and in the image scrambling, the original image is restored accurately, and the scrambling transformation must be reversible, and the XOR operation is simple. Flexible, it provides a good theoretical basis for the application of image scrambling methods, and can achieve better scrambling effects.

C. The Scrambling Algorithm Combine Arnold Transform and XOR Operation

The algorithm block diagram of this paper is shown in Fig.2.

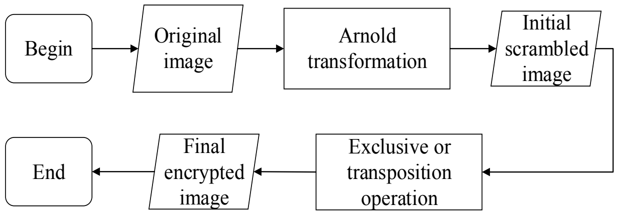


Fig. 2. The scrambling algorithm implementation process based on Arnold transform and XOR operation

Let the size of the original standard Lena image I be M×N (the image used in the MATLAB simulation experiment is a 256×256 grayscale image).

The steps of the scrambling algorithm are as follows:

Step 1: Perform an Arnold transformation on the original standard image I to obtain an initial scrambled image A, and A(i, j) represents the gradation value of the i-th row and the j-th column of the initial scrambled image.

Step 2: XOR the gray value A(1,1) of the first pixel of the initial scrambled image with 255 to obtain A'(1,1); perform high and low transposition on A'(1,1), the operation is the higher 8 bit of A'(1,1) is interchanged with the lower 1 bit; the higher 7 bit is interchanged with the lower 2 bit; the higher 6 bit is interchanged with the lower 3 bit; the higher 5 bit is interchanged with the lower 4 bit, get S(1,1).

Step 3: XOR A(1,2) with its previous S(1,1) to get A'(1,2); then perform high-low transposition on A'(1,2) to get S (1, 2).

Step 4: XOR each element A(i,j) and S(i,j-1) in turn to obtain A'(i,j), and transpose it according to the high and low transposition rules to obtain S(i, j), until S (M, N) is obtained, then S is the scrambled image.

The steps of the restoration algorithm are as follows:

Step 1: First, S (M, N) is subjected to high and low transposition operations. The rules of the transposition operation are the same as above, that is, the higher 8 bit is interchanged with the lower 1 bit; the higher 7 bit is interchanged with the lower 2 bit; the higher 6 bit is interchange with the lower 3 bit; the higher 5 bit is interchanged with the lower 4 bit; after the transposition, A'(M,N) is obtained, and then it is XOR with S(M,N-1) to obtain A(M, N).

Step 2: Perform the same operation on S(M, N-1) in sequence, that is, first perform high and low transposition, and then XOR the gray value of the previous pixel to obtain A(M, N-1).

Step 3: Finally, S(1,1) is subjected to high and low transposition to obtain A'(1,1), and then XOR with 255 to obtain A(1,1).Then A is the initial scrambled image.

Step 4: Perform an Arnold inverse transform on the initial scrambled image A to obtain the restored image.

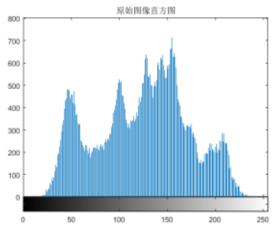
III. The Simulation Experiments and Performance Analysis

A. Experimental Simulation Analysis

In this paper, MATLAB R2016b simulation software is used as the development environment to verify the effectiveness of the scrambling algorithm. The following experiments are mainly carried out.

Experiment 1: Give the original standard Lena image and its histogram, as shown in Fig.3.

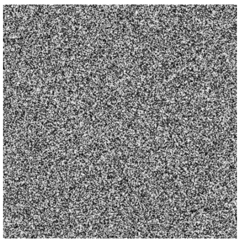
(a)The original image



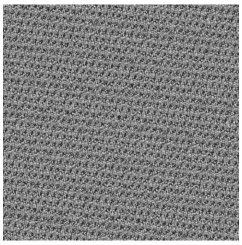
(b) Histogram of Lena

Fig. 3. The original standard image and its histogram

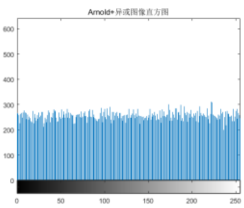
Experiment 2: Give the scrambled image and its histogram obtained by the traditional Arnold transform and the scrambled image and its histogram obtained by the Arnold transform combined with XOR operation, as shown in Fig.4.



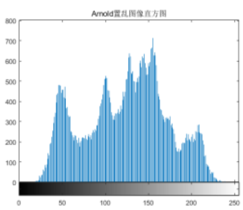
(a)The scramble image of the method of this paper



(b)The scramble image of Arnold transform



(c)The histogram of the method of this paper

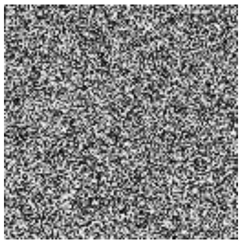


(d)The histogram of the Arnold transform

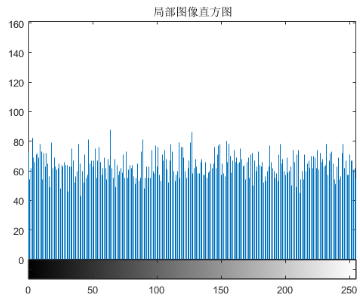
Fig. 4. The scrambling images and histogram comparisons obtained by different methods

According to the results shown in Fig. 4, we can clearly see that compared with the traditional Arnold transform scrambling algorithm, the scrambled image particles obtained by this algorithm are finer and more average, and no information of the original image can be seen from the scrambled image. And features from the perspective of histogram, the traditional Arnold transform is exactly the same as the histogram of the original image. The histogram contains a lot of information of the original image. The attacker can easily get some information of the image by using the histogram feature, which increases the image transmission process. Insecurity. These grayscale values based on the algorithm itself that change the image pixel position do not change, so the histogram does not change. In this paper, the XOR operation of changing the gray value of the image is combined, so that the histogram of the image after scrambling changes significantly, and the gray value distribution of the local image is evenly filled with the entire gray space, as shown in Fig. 5. This also shows that the proposed algorithm is more suitable for the encryption operation of digital images in network transmission and the subsequent information hiding.

(a)The partial original image



(b)The partial scramble image



(c)The histogram of partial scramble image

Fig. 5. The partial scrambled image and its histogram

Experiment 3: Give the final restored image as shown in Fig.6.

Fig. 6. Last restored image

B. *The Scramble Methods Performance Analysis*

According to the similarity definition of the histogram in the literature [9], the scrambling effect of the image is evaluated from the other direction, and the histograms of the two images are h(k) and H(k) respectively, and the similarity of the histogram is defined as :

$$a = 1 - \frac{\sum_{k=0}^{N-1} \left| h(k) - H(k) \right|}{\sum_{k=0}^{N-1} \left| h(k) + H(k) \right|} \tag{6}$$

The histogram of an ideal pure noise image has a uniform gray distribution, that is, h(i)=h(j), and any i,j belongs to {0,1,...,N-1}. According to the above formula, the similarity between the image before and after the scramble and the gray histogram of the white noise image are compared, as shown in Table 1.

TABLE I. THE SIMILARITY BETWEEN DIFFERENT ALGORITHMS AND GRAY HISTOGRAM OF WHITE NOISE

Different image	similarity
The original image	0.5199
The scramble image of Arnold transform	0.5199
The scramble image of the method of this paper	0.9801
The partial scramble image	0.8037

The histogram similarity between the original image and the white noise image is 0.5199, and the histogram similarity between the image after scrambling and the white noise is 0.9801, obviously better than the Arnold scrambling image. The similarity between the partial image and the white noise image is 0.8037, it shows that the scrambled image of the method of this paper is closer to white noise, and the scrambled effect is ideal.

Let the image size be M×N, the pixel value of the (i, j) point in the original image is f(i, j), and the pixel value of the (i, j) point in the scrambled image is F(i, j), then have:

$$SN = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} F^2(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} (F(i,j) - f(i,j))^2} \tag{7}$$

The above formula takes the original signal as a signal, and treats the difference between the original image and the scrambled image as noise. When the mean square signal-to-noise ratio (SN)[10] is larger, the scrambling effect is closer to the original image, which means that the scrambling effect is more terrible. The result is shown in the Table 2.

TABLE II. THE SN BETWEEN DIFFERENT ALGORITHMS

	Arnold transform	The method of this paper
SN	3.7594	2.2785

It is obvious that the method of this paper can achieve better results than the general Arnold algorithm.

IV. CONCLUSIONS

In this paper, after studying Arnold transform and exclusive-or operation, an algorithm combining Arnold transform and exclusive-or operation is proposed. The algorithm uses Arnold transform to change the position of the original image pixel, and then uses the exclusive-or operation to change the pixel gray value of the image. The algorithm changes the image simultaneously from the spatial domain and the transform domain. Experiments show that the new algorithm can change the information of the image and achieve the effect of encryption, which can be applied to the encryption in the image transmission process. In the future, we will study the reversibility of image hiding and the direction of robustness.

REFERENCES

[1] K. T. Lin, "Image Encryption Using Arnold Transform Technique and Hartley Transform Domain," 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, 2013.

[2] D. Nandur and V. H. R, "Visually Meaningful Encrypted Images using Arnold Transform and Other Transforms," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018.

[3] Zhu Xi'an, "A semi-fragile digital watermarking algorithm in wavelet transform domain based on Arnold transform," 2008 9th International Conference on Signal Processing, Beijing, 2008.

[4] Xianzhen Jin, "A digital watermarking algorithm based on wavelet transform and arnold," 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2011.

[5] M. Ding and F. Jing, "Digital Image Encryption Algorithm Based on Improved Arnold Transform," 2010 International Forum on Information Technology and Applications, Kunming, 2010.

[6] Z. Ni, X. Kang and L. Wang, "A novel image encryption algorithm based on bit-level improved Arnold transform and hyper chaotic map," 2016 IEEE International Conference on Signal and Image Processing (ICSIP), Beijing, 2016.

[7] Xu Caocao, Yang Qiming, Yin Fucheng. Image encryption technology based on digital watermarking [J]. Computer and Digital Engineering, 2019, 47 (09): 2273-2275 + 2305..

[8] Ma Miao, Tan Yongjie. Image scrambling algorithm based on bitwise XOR between adjacent pixels [J]. Computer Engineering and Applications, 2008 (09): 187-189.

[9] Tong Xinguang, Luo Hui. Digital image scrambling technology based on S box [J]. Journal of Image and Graphics, 2004 (10): 79-83.

[10] Y. Chen, Y. Ji, J. Zhou, X. Chen and W. Shen, "Computation of signal-to-noise ratio of airborne hyperspectral imaging spectrometer," 2012 International Conference on Systems and Informatics (ICSAI2012), Yantai, 2012.