Scrambling With Image Processing

[1]**Miss. Niharika Raman Satpute**, [2]**Mr. Hirendra Hajare**

[1]M.Tech. Scholar, [2]Assistant Professor Computer Science & Engineering, Ballarpur Institute of Technology, India

Abstract. In recent years, with the rapid development of the Internet, our life has undergone tremendous changes, and the Internet has become an indispensable part of us. With the popularity of the Internet, more and more people use the Internet to transmit multimedia information such as images [1]. Studies have shown that about 75% of human information from the outside world comes from the visual system, that is, from images. Image is not unfamiliar to us. However, in recent years, the security of image information in the transmission process has become increasingly prominent. Such image information as cases, design drawings and so on need to be encrypted when they are transmitted on the Internet. Scrambling technology is an image encryption technology. There are many commonly used image scrambling algorithms. This paper first introduces the image scrambling algorithm based on Arnold transform. Then, in order to improve the image scrambling performance, the application of Arnold transform matrix in image scrambling is analyzed. On this basis, a double scrambling image encryption algorithm based on two-dimensional Arnold transform is proposed. This algorithm uses two-dimensional Arnold transform at the same time.

Keyword : Gray scale, scrambling, The simulation, encryption.

1. Introduction

With the continuous improvement of network bandwidth, it is becoming more and more convenient and rapid for people to transmit data from the network. But some of these data must be encrypted if they are to be transmitted on the network, such as commercial secrets, military secrets, design documents, etc. In case these documents are stolen in the process of network transmission, it will bring huge losses to the country and individuals. Therefore, the related image data of some important industries must be effectively encrypted to ensure the security of the image in the transmission process.

Image scrambling technology is mainly to encrypt the image. By some transformation, the original image becomes chaotic, which makes the transformed image unable to display the original image information. In this way, even if the image is stolen, the stolen person cannot understand the specific content of the image. It can enhance the ability of digital image information to resist illegal attacks and improve security by adding images.

There are several commonly used image scrambling algorithms: the first type is called color space based scrambling algorithm. This kind of algorithm achieves image encryption by changing the pixel value. Although it changes the original basic information of the image to a great extent, the thieves can find out the scrambling rules by comparing the coefficients quantized in the plaintext and ciphertext transform domains to get the information they need. The second type is based on the location space scrambling algorithm. This kind of algorithm changes the pixels of the image. The position of points is used to realize

image encryption. The classical algorithms include Arnold transform, Fibonacci transform, IFS model, Gray code transform, magic square transform, affine transform, fractal Hilbert curve, Tangram algorithm, etc. [5], but these algorithms have a similarity, they do not change the pixel value of the image, so the pilfer may discover the scrambling rule directly by comparing the pixels of plaintext and cipher text, thus stealing the number. Word image information. The third kind of scrambling algorithm is based on position and color space. This algorithm combines the first two algorithms, that is, the fusion of pixel position scrambling and pixel value scrambling, which is a new direction of future image scrambling algorithm development and will be paid more and more attention.

Now I want to focus on Arnold transformation. Among many image scrambling algorithms, Arnold transform is simple, efficient and easy to understand, which makes it widely used in image encryption. Therefore, this paper mainly discusses the double scrambling image encryption algorithm based on Arnold transform. This algorithm applies Arnold transform to both gray level and position scrambling, which not only changes the basic statistical information of the image, but also changes the texture information of the image. The experiment shows that the algorithm is simple and safe, and can achieve better scrambling effect with a small number of iterations, which has a certain impact on the research of image encryption [3].

2. Arnold Transform

The current digital image can actually be regarded as a binary function Z = F (x, y), (x, y) E R, so that the image can be regarded as a two-dimensional pixel matrix, and the encryption of the image actually becomes the encryption of the matrix. Russian mathematician Vladimir Igorevich Arnold proposed Arnold transformation and applied it to ergodic theory. Because Vladimir Arnold first made this transformation in cat images, it is also known as Cat Mapping. Cat face transformation can replace the position of each pixel in the image to achieve the purpose of encryption [18].

2.1. Arnold Positive Transform

After the transformation matrix is transformed, the corresponding polynomials are obtained as follows:

$$\begin{cases} x' = (x + y) \bmod(N) \\ y' = (x + 2y) \bmod(N) \end{cases}$$

A. Arnold Inverse Transform

After the transformation matrix is transformed, the corresponding polynomials are obtained as follows:

$$\begin{cases} x = 2x' - y' \bmod(N) \\ y = -x' + y' \bmod(N) \end{cases}$$

Table 1 shows the Arnold transform period TN of digital image in different order N.

Table 1. Cycle of Arnold transformation

N	2	3	4	5	6	7	8	9	10	11	12
T_N	3	4	3	10	12	8	6	12	30	5	12
N	25	32	48	50	56	64	100	128	256	480	512
T_N	50	24	12	150	24	48	150	96	192	120	384

A large number of studies have shown that Arnold transform can interfere with image in position or gray space, but there are still some shortcomings. For example, Arnold transform scrambling in position space needs several iterations, which only destroys the order without changing the statistical characteristics of the image; Arnold transform scrambling in gray space needs to use high-order transformation matrix and calculate its phase. For complex. Therefore, this paper proposes a double scrambling encryption algorithm based on Arnold transform, and uses the improved Arnold image scrambling algorithm to better encrypt the image [5].

3. Double scrambling encryption algorithm based on Arnold transform

3.1. Arnold Pixel Position Transform

Definition 1 Arnold transformation of an N×N digital image is defined as:

$$F = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{1}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} (\bmod N) \tag{2}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n \cdot \begin{bmatrix} x \\ y \end{bmatrix} (\bmod N) \tag{3}$$

In it, x, y, x ', y 'are in time for {1, 2..., N-1}, N is the order of image matrix, mod is the modular operation. (X, y) is the pixel position of the original image, and (x ', y ') is the pixel position of the scrambled image. A digital image can be regarded as a two-dimensional matrix. Arnold transform moves the pixel value of the original point (x, y) to the position of the transformed point (x ',y '), and the image will change from clear to fuzzy, and the pixel bits of the image will be rearranged after Arnold transform, so that the image will be scrambled, thus realizing the scrambling encryption effect of the image. One Arnold transformation of the image is equivalent to one scrambling, as shown in equation (3). Usually, n times are needed for this transformation process to achieve the desired effect [8].

3.2. Arnold Pixel Value Transform

Definition 2 the arbitrary gray value H denotes the hexadecimal of the pixel value, and the gray scrambling of each pixel value H denotes:

$$\begin{bmatrix} h_1' \\ h_2' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} (\bmod 16) \tag{4}$$

$$\begin{bmatrix} h_1' \\ h_2' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^n \cdot \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} (\bmod 16) \tag{5}$$

In it, h= (h1, h2,) h, h '= (h1', h2 ') h, hl, h2, hi ', h2 ', h2 'in two hours (1, 2..., n), h '= (h1', h2 ') h is the pixel value corresponding to h scrambling. One Arnold pixel value transformation of the image is equivalent to one scrambling, as shown in equation (5). Usually, n times are needed for this transformation process to achieve the desired effect [3].

4. Experimental simulation

The improved Arnold image scrambling algorithm studied in this paper firstly generates the sequence key of scrambling times (k1, K2) randomly, then scrambles the image according to formula (3), and finally scrambles the pixel value according to formula (5). After these steps, the disordered image can be obtained and the encryption effect can be achieved. The image encryption process is shown in Figure 1:
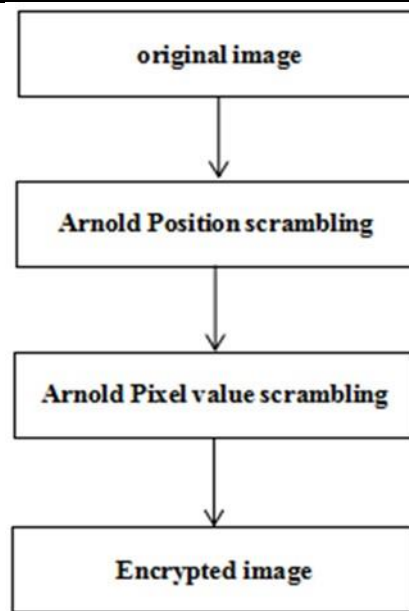
```
┌─────────────────────────────┐
│        original image       │
└─────────────────────────────┘
               │
               ▼
┌─────────────────────────────┐
│   Arnold Position scrambling │
└─────────────────────────────┘
               │
               ▼
┌─────────────────────────────┐
│  Arnold Pixel value scrambling │
└─────────────────────────────┘
               │
               ▼
┌─────────────────────────────┐
│       Encrypted image       │
└─────────────────────────────┘
```

Figure 1. Encryption flow chart

4.1. Scrambling Experiment

In this experiment, the gray scale image of the original image with 256 x 256 pixel size is selected as the experimental image (a). From Figure 2, we can clearly see that the effect of different scrambling experiments is completely different. Figure 2 (b) is the image effect obtained under the position scrambling with fewer iterations, and it can be seen that the image is still relatively clear and does not reach the desired state; Figure 2 (c) is the image effect obtained under the pixel scrambling with fewer iterations, and it can be seen that the image still does not reach the chaotic state; Figure 2 (d) is obtained under the mixed situation of position scrambling and pixel scrambling. The image effect, we can see that the image has achieved a better scrambling effect, giving us a direct visual feeling is very blurred, to achieve the desired effect. Through experiments, we can clearly see the impact of different algorithms on the scrambling effect. By combining the two scrambling algorithms, the new scrambling algorithm not only makes the image scrambling effect more obvious, but also improves the efficiency and security. Traditional scrambling algorithm for image encryption effect has been reduced, in recent years, more and more improved algorithms have appeared and continue to innovate and develop, and there will be great prospects in the future. The following is part of the experimental results:
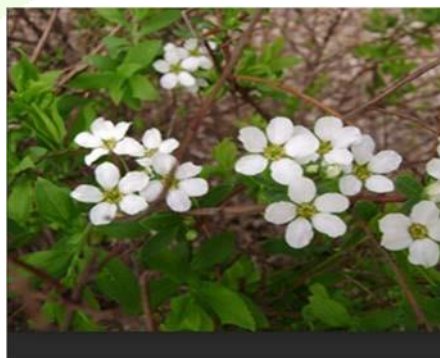
Original map
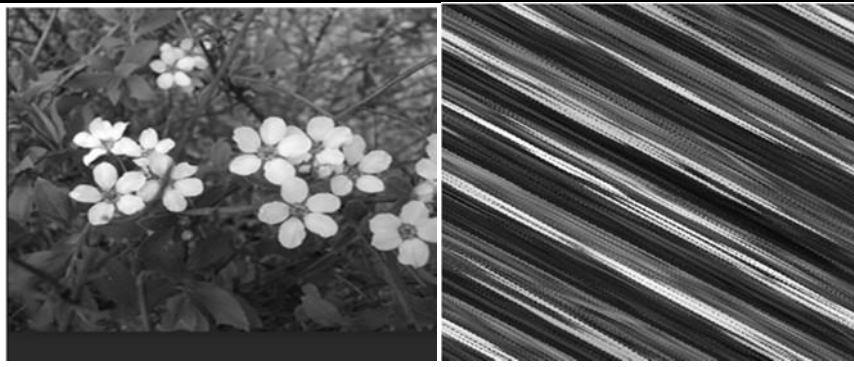
(a) Gray scale image (b) k (2, 0) scrambled graph
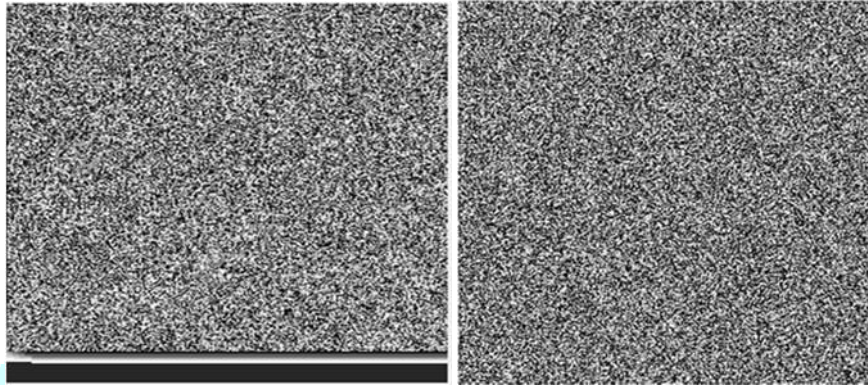
(c) K (0, 2) scrambled graph (d) K (8, 8) scrambled graph **Figure 2.** Experimental
results

4.2. *Gray Histogram Experiment*

Gray histogram describes the statistical information of the image drawing. Mathematically speaking, it is a function of gray level. Graphically speaking, it is a two-dimensional graph. The abscissa represents the gray level, and the ordinate represents the number or probability of the occurrence of the pixels with each gray level in the image. From Figure 2, we can see that the effect of image scrambling is different in different scrambling experiments. In order to see the effect of image scrambling more clearly and intuitively, we have done gray histogram experiments on the above images. From Figure 3, we can see that the gray histogram of the image processed by the double scrambling algorithm has changed more obviously, that is, the statistical information of the image is completely different before and after the experiment.
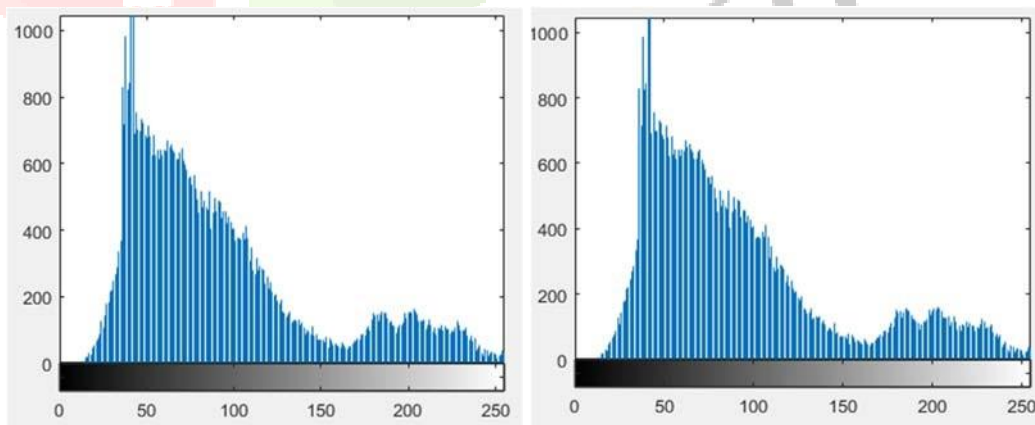
(a) Ginal histogram (b) k (3, 0) histogram
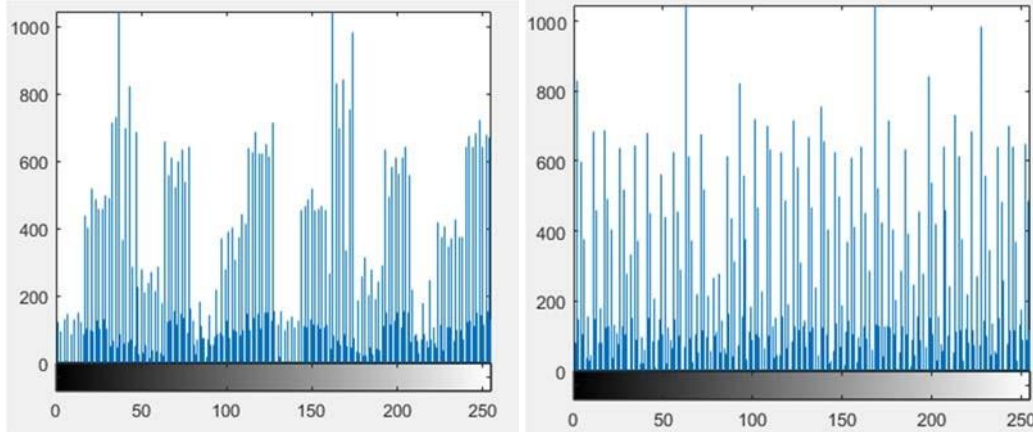
(c) K (0, 3) histogram   (d) k (5, 5) histogram **Figure 3.** Grayscale
                                                histogram

4.3. Algorithm Performance Analysis

Scrambling refers to moving a pixel of an image to the position of B pixel, and B pixel to the position of C pixel, so that it can be converted into a confused and difficult to recognize image. In fact, it is the encryption of the image. It hides the scrambled image as secret information, which can greatly improve the robustness of the hiding carrier. Therefore, image scrambling is a very common information hiding technology [16].

The evaluation criteria used to measure image scrambling include subjective criteria and objective criteria of the observer. Subjective judgment can be made based on the human eye's visual perception of the original image and the scrambled image. There is no unified mathematical model for objective standards. Bersen et al. proposed a mathematical model to measure the image scrambling degree by using the difference between the gray value of each pixel in the original image and the gray value of surrounding pixels [17]:

$$S = \frac{1}{(n \times m)^{3/2}} \sum_{i=1}^{n} \sum_{i=1}^{n} \sqrt{\left(i - t_{row}(i,j)^2\right) + \left(j - t_{col}(i,j)^2\right)}$$

The improved Arnold image scrambling algorithm in this paper can achieve the expected encryption effect with fewer scrambling times, and the scrambling times with double keys also greatly improve the security of the algorithm. The difference in keys means that the scrambling process of images is different, and only the correct key can restore the original image.

5. Conclusion

An improved Arnold image scrambling algorithm based on Arnold is proposed in this paper, and related experiments are carried out with MATLAB. Aiming at the shortcomings of traditional Arnold transform technology, the improved algorithm adopts Arnold transform double scrambling image encryption technology. The Arnold matrix is used not only for position scrambling, but also for pixel value scrambling, which enlarges the scope of application. At the same time, this improved algorithm can achieve the desired results with fewer scrambling times, improve the efficiency of the algorithm, and enhance the security and reliability of the algorithm by using double keys. Experiments show that the algorithm has high practicability, of course, with the continuous development of technology, there will be better algorithms, we need to continue to explore and learn.

References

[1]   Sun Xiao.Research on image restoration under bounded constraints and selection of regularization parameters [D]. China University of Petroleum, 2008.

[2]   Huang Fangyuan. Image scrambling algorithm and Implementation Based on Arnold transform [J]. Journal of Guizhou University (Natural Science Edition), 2008 (3): 276 - 279.

[3]   Guo Linqin, Zhang Xinrong. Image double scrambling algorithm based on two-dimensional Arnold transform [J]. Computer application and software, 2010 (4): 264 - 266.

[4]   Duan Huan, Zheng Ziwei. An improved Arnold scrambling transform algorithm based on bit plane [J]. Wireless communication technology, 2018 (02): 37 - 42.

[5]   Zhang Ying, Yang Yong. Arnold double scrambling image encryption algorithm [J]. Journal of Liaoning University of Engineering and Technology (Natural Science Edition), 2013 (10): 1429-1432.

[6]   Fang Yi.Arnold Scrambling Transform Image Encryption Algorithms [D]. Jiangxi University of Technology, 2018:58.

[7]   Li M, Xiao D,Peng Z,Nan H.A. ETRI Journal. Modified reversible data hiding in encrypted images using random diffusion and accurate prediction., 2014.

[8]   Chen Li. DCT domain digital watermarking technology based on HVS [J]. Information technology, 2013 (02): 170 - 173.

[9]   Qi DONGXU, ZOU J1ANCHUN,BAN XIAOYOU.A newelass of scrambling transformation and it's application in the image information covering [J]. Science in china Scrics, 2000(3):304 - 312.

[10] Wang Taiyue, Dai Yanqing. Research and comparison of digital image scrambling algorithms [J]. Journal of Hubei Institute of Technology, 2017 (04): 25 - 30.

[11] He Bing, Niu Huaigang, Xiao Linglu. A dual transform two-dimensional image encryption algorithm [J]. Optical Technology, 2015 (01): 52 - 58.

[12] Dou Huazhe. Tracking Research of Model Measurement Targets Based on Machine Vision [D]. Beijing Jiaotong University, 2016.

[13] Lai Qingming. Validation of image encryption algorithm based on Arnold transform [J]. Electronic quality, 2015 (06): 31 - 36.

[14] Wang Yi, Xu Liangliang, Zou Shengfu. A double scrambling image algorithm based on gray level and position [J]. Communication technology, 2017 (12): 2856 - 2866.

[15] Wen Xiaoshuang, Zhu Kaige. Colour image encryption algorithm based on scrambling and diffusion [J]. Software guide, 2018 (10): 81 - 84.

[16] Wang Wei, Jin Cong. An image encryption scheme based on Android platform [J]. Computer Science, 2014 (10): 100 - 102.

[17] Jin Yanhong. Digital Image Scrambling Algorithms [J]. Science and Technology Information, 2009 (26): 216.

[18] Guo Long. Research and Design of Secure Video Communication System Based on Chaos [D]. Guangdong University of Technology, 2015.