Image information hiding based on Arnold scrambling and chaotic fusion algorithm

Jubao Qu[a, *], Hongtao Liang[b]

School of Mathematics and Computer, Wuyi University, Wuyishan, Fujian 354300, China

[a]Qjbok@qq.com, [b]wyxyqjb@163.com

*Corresponding author

Keywords: Arnold scrambling, Logistic chaotic mapping, image, hiding.

Abstract: Arnold scrambling algorithm is used to scramble and encrypt secret information. Logistic chaotic mapping and discrete cosine transform are combined to hide secret information in the image, so that secret information can be hidden and transmitted safely. The simulation experiment under the environment of MATLAB shows that the method has good robustness and effectiveness.

1. Introduction

With the advent of the network era, information security has become more and more important. Information encryption and hiding can greatly improve the security of information. However, the security of traditional encryption methods cannot be guaranteed at present. If it can cooperate with information hiding, it will play a multiplier role with half the effort. Literature [1] points out that information hiding mainly uses redundant information in the carrier to embed the secret information to the carrier so that it is not easy to be found, so as to achieve the purpose of secret communication. Literature [2] points out that the encrypted information is first encrypted and then hidden in the carrier to ensure the security of communication. In this paper, we first scramble and encrypt the information, and then hide the information by combining Logistic chaotic map and discrete cosine transform

2. Arnold information scrambling algorithm

Information scrambling technology is to confuse the hidden information according to some algorithm to make it imperceptible and restore it when needed. Literature [3] points out that after scrambling operation, the information looks like randomly distributed white noise, and cannot extract any effective information from it, so when it is embedded into the carrier image, it will not cause too great changes in color and texture, and enhance the visual effect of the embedded image. Literature [4] points out that the process of scrambling is equivalent to encrypting information, and the interceptors who do not know the scrambling method and key need a great deal of computation to decrypt the acquired information. Therefore, it can effectively improve the security of transmission while improving the imperceptibility.

Arnold scrambling is a transformation proposed by Russian mathematician Vladimir I. Arnold. For a two-dimensional Arnold scrambling of an N*N digital image, the expression used is:

$$\begin{bmatrix} i_{k+1} \\ j_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} i_k \\ j_k \end{bmatrix} \bmod(N) \tag{1}$$

When restoring, the inverse matrix of the transformation matrix can be used:

$$\begin{bmatrix} i_{k+1} \\ j_{k+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} i_k \\ j_k \end{bmatrix} \bmod(N) \tag{2}$$

In the above formula, (i_k, j_k) is the pixel position of the image before transformation, (i_{k+1}, j_{k+1}) is the pixel position after transformation, a, B is the parameter, K is the number of current transformation, N is the length of the image, mod is the modular operation. In the process of scrambling, parameters a, B and scrambling times K can be used as key keys. When extracting information and decrypting, information can be extracted according to different scrambling cycles and key keys.

3. Information hiding

3.1 Logistic Chaotic Mapping Transform.

Information hiding technology mainly includes spatial hiding algorithm and transform domain hiding algorithm. Spatial hiding algorithm is the embedding of information in the spatial domain of an image. The main method is to hide secret information by directly modifying the pixel value of the image. Compared with the spatial information hiding algorithm, the advantage of the transform domain algorithm is that the embedded secret information energy can be distributed evenly on all the pixels, and the hiding effect is better. Moreover, if only the IF coefficients are modified, the transform domain algorithm has strong robustness to general noise attacks and compression attacks. Logistic chaotic mapping transformation is used to obtain arbitrary initial values, then DCT is used to transform the carrier image into frequency domain, and then the frequency domain coefficients are adjusted to achieve the purpose of embedding information.

$$\mathrm{L}_n(x_{k+1}) = \mu\, \mathrm{L}_n(x_k) \bullet [1 - \mathrm{L}_n(x_k)] \tag{3}$$

Among them, $\mathrm{L}_n(x_{k+1})$ is the value of Logistic mapping after n iterations of arbitrary initial value x0; n = 0, 1, 2, ... When $\mu \in (3.594536\ ,\ 4)$, the model enters into chaotic state, and the generated sequence $\{\mathrm{L}_n(x_k);\ k = 0,1,2,\cdots\}$ is non-periodic, non-convergent, sensitive to initial conditions, and has good security.

3.2 Discrete cosine transform.

Discrete cosine transform (DCT) is a separable transformation. Its transform core is cosine function. Besides the general orthogonal property, the base vector of the transform matrix has a characteristic vector similar to that of Toeplitz matrix. DCT is considered as a quasi-optimal transformation in the processing of image and speech signals. The transformation kernels of two-dimensional DCT transform are:

$$G(i, j, x, y) = \frac{2}{\sqrt{mn}} T(x) \bullet T(y) \bullet \cos\frac{(\pi x(1 + 2i))}{2m} \bullet \cos\frac{(\pi y(1 + 2j))}{2n} \tag{4}$$

In the formula, i, x = 0, 1, 2, ... m-1, J, y=0,1,2,... n-1.

The definition of two-dimensional DCT transformation is as follows. If f(i,j) is a digital image matrix of m*n, then:

$$F(x, y) = \frac{2}{\sqrt{mn}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} f(i, j) \bullet T(x) \bullet T(y) \bullet \cos\frac{(\pi x(1 + 2i))}{2m} \bullet \cos\frac{(\pi y(1 + 2j))}{2n} \tag{5}$$

In the formula, i, x = 0, 1, 2, ... m-1, J, y=0,1,2,... n-1.

Two-dimensional inverse DCT transform is defined as:

$$f(i, j) = \frac{2}{\sqrt{mn}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} F(x, y) \bullet T(x) \bullet T(y) \bullet \cos\frac{(\pi x(1 + 2i))}{2m} \bullet \cos\frac{(\pi y(1 + 2j))}{2n} \tag{6}$$

3.3 L-D fusion algorithm based on Logistic chaotic map and DCT.

$$x_{k+1} = \begin{cases} \alpha \times L(x_k) & x_k \le 0.5 \\ \beta \times F(x_k, y_k) & x_k > 0.5 \end{cases} \tag{7}$$

Among them, $x_k \in (0, 1)$ is the initial value of compound chaotic system, which is generated by random function RND (xk), L (xk) is the Logistic mapping model, F (xk, yk) is the DCT of discrete cosine transform, and α、β is the scaling factor of L-D fusion algorithm. By adjusting the scaling factor, different chaotic sequences can be obtained.

4. Algorithm implementation steps

The implementation of the algorithm mainly includes two parts: information embedding and extraction. The embedded information used in this paper can be a hybrid document of text and image. The carrier is a 512*512 gray image. The specific experimental design steps are as follows:

4.1 Secret information embedding process.

Step1: Record the carrier image size 512*512 and the information to be embedded as M and N, respectively.

Step2: N is encrypted by Arnold scrambling transformation, a n d the scrambled image is recorded as P. The scrambling matrix parameters a, b, c, d a n d scrambling number n are saved as key.

Step3: Divide M and P into 8*8 blocks. DCT transform is performed on each block to obtain its DCT coefficient matrix, which is recorded as M1 and P1, respectively.

Step4: According to the L-D fusion algorithm, the embedding information can be better hidden in the carrier by choosing the appropriate coefficients.

4.2 Secret Information Extraction Process.

Step1: The received secret information image S and the original carrier image M are transformed by block DCT, and their DCT coefficient matrices S2 and M 2 are obtained.

Step2: Using two-dimensional inverse DCT transform f (i, j), the fusion coefficients at the time of embedding are substituted, and the embedded secret information P2 can be obtained by IDCT transformation.

Step3: By decrypting P2 according to the key, the original secret information N to be embedded can be obtained.

5. Simulation experiment

Text and image can be regarded as a two-dimensional matrix. After Arnold transformation, the pixel positions of the image will be rearranged, so that the image will appear chaotic, thus achieving the scrambling encryption effect of the image. Fig. 1 is a part of the code for simulation by using MATLAB software. Figure 1(a) is a scrambling code for information, and Figure 1(b) is a recovery code after scrambling.

Figure 2 is a simulation experiment. Figure 2(a) is the embedded information after scrambling encryption, approximating white noise. Figure 2(b) is the encrypted image after embedding scrambling information. It cannot be seen from the naked eye that it is different from the carrier image. The encrypted image is transmitted in the channel, and useful information cannot be obtained without knowing the key used for encryption. Figure (c) is the peak signal-to-noise ratio (PSNR) of the proposed algorithm and other literature algorithms when dealing with image concealment. It can be seen that by choosing appropriate scrambling times and fusion coefficients, the peak signal-to-noise ratio (PSNR) of the encrypted image and the extracted image can basically reach more than 34 dB, thus ensuring good invisibility and extraction quality, and achieving the purpose of information

hiding and effective transmission.

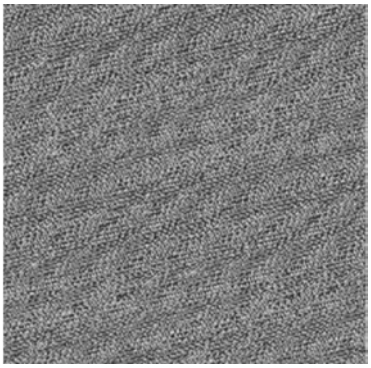
```
; Scrambling code
Function arnoldImg = arnold(img,a,b,n)
[h,w] = size(img);
N=h;
arnoldImg = zeros(h,w);
for i=1:n
    for y=1:h
        for x=1:w
            xx=mod((x-1)+b*(y-1),N)+1;
            yy=mod(a*(x-1)+(a*b+1)*(y-1),N)+1;
            arnoldImg(yy,xx)=img(y,x);
        end
    end
    img=arnoldImg;
end
arnoldImg =uint8(arnoldImg);
end
```

(a) Scrambling code

```
; Recovery code
function img = rearnold(arnoldImg,a,b,n)
[h,w] = size(arnoldImg);
img = zeros(h,w);
N = h;
for i=1:n
    for y=1:h
        for x=1:w
            xx=mod((a*b+1)*(x-1)-b*(y-1),N)+1;
            yy=mod(-a*(x-1)+(y-1),N)+1;
            img(yy,xx)=arnoldImg(y,x);
        end
    end
    arnoldImg=img;
end
img = uint8(img);
end
```

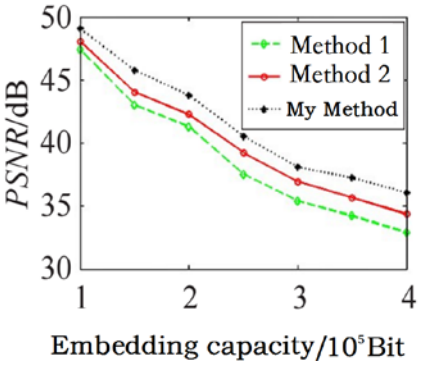
(b) Recovery code

Fig. 1 Part of Code for Simulation by Using MATLAB Software



(a)Scrambling Information

(b) Dense image



(c) PSNR comparison

Fig. 2 Experimental diagram of algorithm simulation

6. Summary

This paper integrates the traditional ideas of information hiding and encryption, and proposes to use Arnold scrambling algorithm to scramble and encrypt secret information. Then it integrates Logistic chaotic map and discrete cosine transform to hide secret information into images, so as to realize the secret information hiding and secure transmission. The simulation experiment under the environment of MATLAB shows that the method has good robustness and effectiveness, thus ensuring the security of communication.

Acknowledgments

This research was financially supported by The Key Laboratory of Cognitive computing and intelligent information processing of Fujian Education Innovation, Fujian Provincial Higher Education Innovation and Entrepreneurship Education Reform Project (sjzy2017002), Fujian Provincial University "Curriculum Thought" Education and Teaching Reform Project (KC18087), Fujian Provincial Natural Science Foundation Project (2017J01406).

References

[1] Yang Cuiling, Zhang Wei, Greenlin, Zhao Jiahui. A color image encryption algorithm based on Arnold and discrete fraction random transformation. Journal of Liaoning University of Petroleum and Chemical Technology. 38 (2018) 82-88.

[2] Hu Yunqin. Research and implementation of image-based information hiding technology. Information communication. 189 (2018) 38-39.

[3] Wang Linjuan, Zhang Xiaoying, Hao Zhengyi. Wavelet domain digital watermarking algorithm

based on Arnold scrambling and chaotic encryption. Information technology. 11 (2018) 49-58.

[4] Yang Cuiling, Zhang Wei, Greenlin, Zhao Jiahui. Reversible information hiding method for color image based on RGB correlation. Computer engineering and application. 54 (2018) 69-73.