International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Image Cryptography Technique based on FFT

Mudiyala. Akila Sowndarya[1], Damodara V V S Phani Kumar[2]

[1, 2]Computer Science Engineering, RISE Prakasam Group of Institutions, Ongole, India

Abstract: ***The author of this article makes studies and discussion on the image cryptography of transforming domains. In the image cryptographic algorithm, the sine chaotic mapping scrambling is applied to the original image and the scrambling matrix is generated by Logistic chaotic system. Fractional Fourier transform (FFT), respectively, is along the x-axis and y-axis that generates a function which is transformed random in the phase mask. The function of the phase mask uses the Logistic chaotic system. The simulation experiments verifies that this algorithm can effectively resist plaintext attack, differential attack and statistical analysis, and the large key space can be achieved to 1087, and has a higher security.***

Keywords: Fractional Fourier transform; scrambling; image encryption

1. Introduction

Image Encryption, as the core technology of the image security is a direct and effective means of protecting the image's security. At the same time, image encryption is an indispensable technology in information hiding and digital watermarking. Most image encryption adapts symmetric key crypto-system way. At present, the research of image encryption is mainly focused on the following aspects: spatial domain image encryption, transforming domain image encryption, image encryption based on the neural networks, image encryption based on chaotic, image encryption based on cellular automat and quantum code technology.

The advantage of transforming domain image encryption is that it can make the image encryption processing connecting with the image compression. Sun Xin, Yi Kaixiang et al proposed an image encryption algorithm based on the discrete cosine transform[1], which makes the image encryption connected with the image compression methods. However, due to the use of DCT transforming image, we often pretreat the blocks firstly. Therefore, the key space is not large and the security is not high when we use the chaotic system generating the scrambling matrix. In reference[2,3], the authors proposed an image encryption algorithm based on Fractional Fourier transform. From the perspective of optics information processing, the Fractional Fourier transform is achieved by the optical instruments in order to achieve the optical image encryption. This article makes research and discussion on transforming domain image encryption which is simulatively experimented in computer. As the image scrambling processing is added to the image encryption algorithm, thereby the security of the entire encryption system is improved. The algorithm thought is: Firstly, the original image is adapted with a sine scrambling chaotic mapping in which the scrambling matrix is generated by the Logistic chaotic system. Then, Fractional Fourier transform, respectively, is along the x-axis and y-axis that generates a function which is transformed random in the phase mask. The function of the phase mask uses the Logistic chaotic system. The simulation experiments verify that this algorithm can effectively resist plaintext attack, differential attack and statistical analysis, and the total key space can be achieved to 1087. Non-authorized users are difficult to successfully break the cipher in limited time with the brute-force method showing that the proposed algorithm in this article has higher security.

2. Principles of Algorithm

2.1. Logistic Mapping

Logistic mapping having the characteristics of simple structure, initial value sensitivity and noise statistics, is defined as

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

in which X_n is the initial value,and x0 is the iterative value after n iterations.$\mu \in [0,4]$ is called the Logistic controlling parameters, sometimes also known as the bifurcation parameter, the different μ value system presenting different characteristics. The sequence generated by this mapping is controlled by μ and the initial value x0, and when any one has tiny difference, the generated sequence will be distinct. The studies have shown that when $\mu \in$ (3.5699... 4], $x_n \in$ (0,1), the system is in a chaotic state. Figure1 shows the result when μ adopts different value iterations removed after 500 times in front of 100. The crossing axis represents the range of μ, and the vertical axis represents the range of X

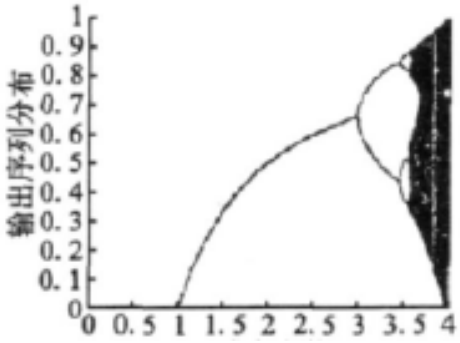

Figure 1: Logistic mapping iteration result

From Figre 1, we can see that when μ is closer to 4, X is closer to the average distribution in the entire region of to 1. So it is better when the selected logistic controlling Parameters are closer to 4[4]. That is to say, under the Logistic mapping, the sequence $\{X_k, k = 0, 1, 2 ...\}$ generated by the initial x0 is non-periodic and convergence and it is very sensitive to the initial value.

2.2. Fractional Fourier Transform

In 1980, V.Namias firstly proposed and studied an improved form of the Fourier transform [5] that is the Fractional Fourier transform (Fractional Fourier Transform on FRFT). Fractional Fourier transform is a promotion of the classic Fourier transform and it is to transform the study in to a higher dimension of the new object to be processed, belonging to the upgrading dimension method.

The definition of Fractional Fourier transform of the function (x, y) is

$$G(u,v) = F^{P_x,P_y}[g(x,y)] = \int_{-\infty}^{+\infty} g(x,y)K_{P_{x,P_y}}(x,y,u,v)dx,dy \quad (2)$$

In which the key function is

$$K_{P_{x,P_y}}(x,y,u,v) = K_{P_x}(x,u).K_{P_y}(y,v) \quad (3)$$

But the function of $K_{P_x}(x,u)$ and $K_{P_y}(y,v)$is respectively

$$\begin{cases} A_{P_x}\, exp[j\pi(x^2\cot\emptyset - 2xu\csc\emptyset + u^2\cot\emptyset)], 0 < |P_x| < 2 \\ \delta(x-u), P_x = 0 \\ \delta(x+u), P_x = \pm 2 \end{cases} \quad (4)$$

$$\begin{cases} A_{P_x}\, exp[j\pi(x^2\cot\emptyset - 2xu\csc\emptyset + u^2\cot\emptyset)], 0 < |P_y| < 2 \\ \delta(y-u), P_y = 0 \\ \delta(y+u), P_y = \pm 2 \end{cases} \quad (5)$$

Where in $P_x$and P_y are the orders of g(x, y) along the x axis and y-axis of a dimensional fractional Fourier transform, respectively. And the coefficient is

$$A_{P_x} = \frac{exp[-j\pi sgn(\sin\emptyset)/4 + /4 + j\emptyset/2]}{\sqrt{|\sin\emptyset|}}, \emptyset = \frac{P_x\pi}{2}$$

$$A_{P_y} = \frac{exp[-j\pi sgn(\sin\emptyset)/4 + +j\emptyset/2]}{\sqrt{|\sin\emptyset|}}, \emptyset = \frac{P_y\pi}{2} \quad (6)$$

When P_x=P_y =1, Fractional Fourier transform is degenerated as Fourier transform.

2.3. Sine chaotic mapping [7]

$$x_{n+1} = f(\mu, x_n) = \mu\, sin(\pi x_n), n = 0,1,2,\ldots \quad (7)$$

Formula (7) is iterated K+L times to get the chaotic Sequence of x_u,u=0,1,...K+L-1. In order to ensure The initial sensitivity and parameters' sensitivity of chaotic system, the iteration data of the former L times of chaotic system should be discarded. Therefore, the left chaotic sequence can be expressed with x_k, k=0, 1 ,... K-1. So the value of the element t(x,y) in the scrambling matrix T(x,y) can be achieved by formula(8).

$$T(x,y) = [x_k * (K-1)], K = x * M + y \quad (8)$$

3. Image Encryption Algorithm Based On Fractional Fourier Transform

Supposing f0(x, y) represents the original image, the steps of image encryption algorithm based on fractional Fourier transform as follow:

Step1 Chaotic transform (7) is used to scramble the original image f0(x, y) to get a real-valued function f1(x, y),in which the scrambling matrix of chaotic transform is generated by using Logistic chaotic system, and its system parameters and initial value are respectively x0 and u;

Step2$f_1(X,Y)$is transformed with one-dimensional Fractional Fourier transform of $P_X$along the x-axis to get the compositive valued function $f_2(X,Y)$.

Step3$f_2(X,Y)$is random phased mask to achieve $f_3(X,Y) = f_2(X,Y) * M_1(X,Y)$and phase mask function $M_1(X,Y)$ is$M_1(x,y)$ = e x p[j 2π φ (x , y)] , in which $\emptyset_{(x,y)}$ is generated by Logistic chaotic system, and the chaotic system parameters and the initial values are x01 and u1 respectively and its iteration value is random distributed in [0, 1];

Step4$f_3(X,Y)$) is transformed with one-dimensional Fractional Fourier transform ofP_Y along the x-axis to get $f_4(X,Y)$

Step5 $f_4(X,Y)$is random phased mask to get $f_5(X,Y) = f_4(X,Y) * M_2(X,Y)$ and the phase mask function $M_2(X,Y)$ is $M_2(x,y)$ = e x p [j 2π ϕ (x, y)], in which $\emptyset_{(x,y)}$ is also generated by Logistic chaotic system, and its chaotic parameters and initial values are x02 and u2 respectively, and the iteration value is random distributed in [0,l].So $f_5(X,Y)$is the encryption image which contains the amplitude spectrum abs[$f_5(X,Y)$and the phase spectrum angle[$f_5(X,Y)$]of encryption image.

Decryption algorithm is the inverse of the encryption algorithm, so the decryption steps are not discussed here.

4. Experiments Result and Analysis

4.1 Simulation experiment

This article adapts a Lena image with the size of 256 ×256, the gray-scale L = 256 as the encryption object, and an experiment platform with the memory of 1GB, CPU 1.90GHz PC. C language is used to achieved the programming, in which the two parameters of chaotic transform are x0 =0.6 and u = 1.99; the fractional of Fractional Fourier transform are P_X= 0.7 and P_Y= 0.8; two generated parameters of $\emptyset_{(x,y)}$re x01= 0.3 and u1= 1.991; but two generated parameters of $\emptyset_{(x,y)}$are x02= 0.4 and u2=1.992. The encryption result is shown in Figure 2((a) Original Image ;(b) Encryption Image;(c) Amplitude spectrum of Encryption Image; (d) Phase spectrum of Encryption Image; (e) Correct Encryption Image).

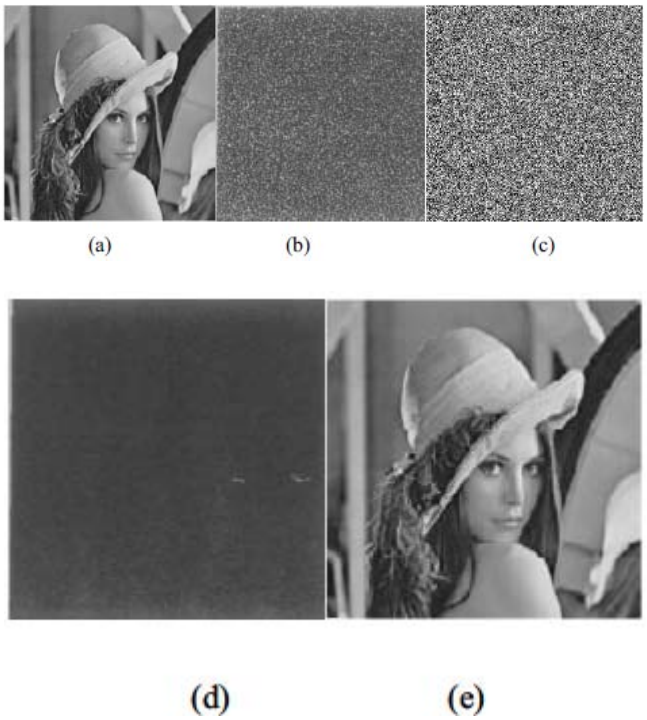

Figure 2: Image Encryption Result based on Fractional Fourier transform

Under the situation of all decryption keys being correct, the PSNR of the decrypted image is PSNR = 50.1438, almost the consistency of the original image and the subjective evaluation results. It shows that the image encryption algorithm proposed in this article is effective.

4.2 Analysis of Experiment Results

1) Analysis of the Key Space: The total key space of the image encryption algorithm proposed in this article is to10^{87}, wherein the magnitudes of key spaces of parameters x_0, x_1, x_2, all are10^{15}, the magnitudes of key spaces of u_0, u_1, u_2 all are 10^{13} (considering not all u can make the Logistic mapping to the chaotic state, the actual space cannot be to 10^{14}); the key space of$P_x$and P_y are smaller and the total magnitudes are 10^3 (the key space can be omitted).Therefore, non-authorized users are difficult to successfully break the cipher in limited time with the brute-force method showing that the proposed algorithm in this article has higher security.

2) Test of Sensitivity: According to the test result of Logistic chaotic system sensitivity, we can see that one must correctly enter all keys to decrypt the image correctly. These keys include: x_0 and u in chaotic transform; the parameter x_{01} in random phase mask 1 and the system parameter u_1; the parameter x_{02} in random phase mask 2 and the system parameter u_2;. Figure 3((a) Decrypted Image with Correct Key ;(b)Decrypted Image with Wrong Key(u_1=1.990))shows two encryption images of the correct key (u_1 1.991)and the wrong key (u1= 1.990), which illustrate that even if the key has a tiny difference, the original image cannot be decrypted. The enumeration search is difficult to decrypt the original image, so the algorithm proposed in this article has a better security. Figure 3.

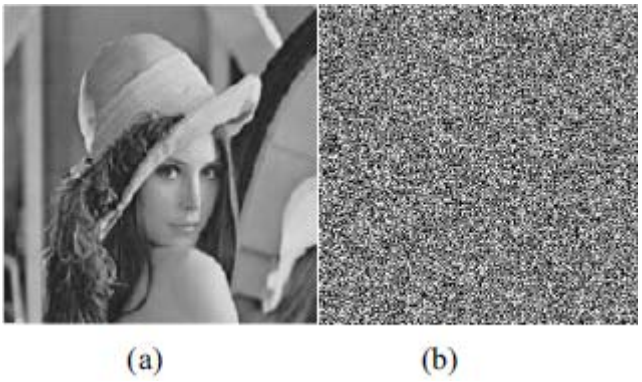

Figure 3: Test of Sensitivity

3) Histograms: A histogram shows the statistical characteristics of the gray level of each image and its frequency of occurrence. If the encrypted image histogram is shown with a uniform state distribution, it shows that the encryption algorithm can effectively hide the statistics of the original image, and the results of encryption works well. Figure 4(a) and Figure 4(c) are the component histograms of images before encrypting and after decrypting of Figure2 (a), respectively, and the distributions of the two graphs are substantially identical. Figure 4(b) is the component histogram of Figure 2(a) after encrypting, and the distribution is even. Therefore, Figure 4 shows that this algorithm has good effects of encryption and decryption((a)Gray-scale Histogram of Original Image(b)Gray-scale Histogram of Encryption Image(c) Gray-scale Histogram of Decryption Image).

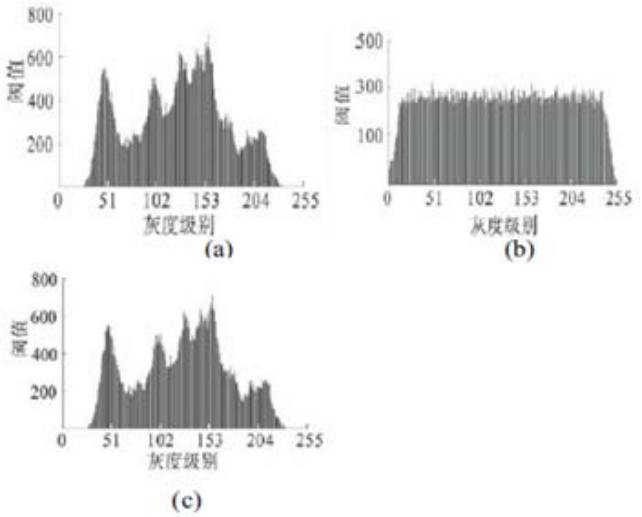

Figure 4: Gray-scale Histogram of Encrypting and Decrypting Image by the Algorithm Proposed in this Article

5. Conclusion

On the basis of the analysis of image encryption by domestic and foreign scholars, the author of this article proposes an image encryption algorithm based on Fractional Fourier transform. Owing to the use of Logistic mapping, Fractional Fourier transform and sine chaotic mapping in the process of encrypting, at the same time, the image scrambling processing is added to the image encryption algorithm so as to improve the security of the entire encryption system. The

simulation experiments verifies that this algorithm can effectively resist plaintext attack, differential attack and statistical analysis, and the large key space can be achieved to 10^{87},, and non-authorized users are difficult to successfully break the cipher in limited time with the brute-force method showing that the proposed algorithm in this article has higher security.

References

[1] Sun Xin, Yi Kaixiang and Sun You."Image Encryption Algorithm based on Chaotic System". Journal of Computer Graphics and Computer Aided Design Graphics, 2002, 14(2):136-139.
[2] Linfei Chen and Daomu Zhao."Optical image eneryption based onfractional wavelet transform". Optics Communications, 2005, 254(4-6):361-367.
[3] Xiaogang Wang and Daomu Zhao."Image encryption based onanamorphic fractional Fourier transform and three-step phase-shifting interferometry". Optics Communications, 2006, 268(2):240-244.
[4] Zhang Xiujun, Feng Qiaosheng and Luo Ke."Studies on Image Encryption Security Risk based on Logistic Mapping". Microcomputer and Application, 2010,29(5):24-26)
[5] NamiasV."The Fractional Fourier Transform and its Applieation inQuantum Meehanies". J.Inst.Math.Its APPl., 1980(25):241-265.
[6] N.Korabel and R.Klages."Fractality of deterministic diffusion in then on hyperbolic climbing sine map". Physica D: NonlinearPhenomena, 2004, 187(1-4):66-88.

Author Profile

Mudiyala. Akila Sowndarya Obtained the B.Tech. Degree in Information Technology (IT) from Prakasam Engineering College, Kandukur. At present persuing the M.Tech in Computer Science (CS) Department at Rise group of Institutions, Ongole.

Damodara V V S Phani Kumar obtained **M. C. A, M. Tech (Ph.d)**. At present working as Associate Professor in Computer Science and Engineering (CSE) Department at Rise Krishna Sai Prakasam Group of Institutions formerly known as RISE Prakasam Group of Institutions, Ongole.