



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

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

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

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

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

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

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

2.3. Sine chaotic mapping [7]

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

Formula (7) is iterated  $K+L$  times to get the chaotic Sequence of  $x_n, n=0, 1, \dots, K+L-1$ . 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  $x_k, k=0, 1, \dots, K-1$ . 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  $f_0(x, y)$  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  $f_0(x, y)$  to get a real-valued function  $f_1(x, y)$ , in which the scrambling matrix of chaotic transform is generated by using Logistic chaotic system, and its system parameters and initial value are respectively  $x_0$  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  $M_1(x, y) = e^{x p [j 2\pi \phi (x, y)]}$ , in which  $\phi_{(x, y)}$  is generated by Logistic chaotic system, and the chaotic system parameters and the initial values are  $x_{01}$  and  $u_1$  respectively and its iteration value is random distributed in  $[0, 1]$ ;

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

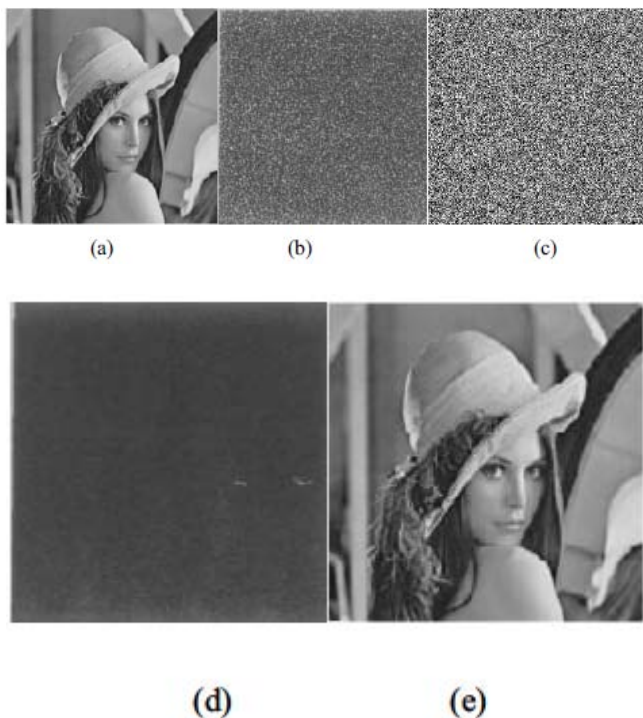
Step5  $f_4(X, Y)$  is random phased mask to get  $f_5(X, Y) = f_4(X, Y) * M_2(X, Y)$  and the phase mask function  $M_2(X, Y)$  is  $M_2(x, y) = e^{x p [j 2\pi \phi (x, y)]}$ , in which  $\phi_{(x, y)}$  is also generated by Logistic chaotic system, and its chaotic parameters and initial values are  $x_{02}$  and  $u_2$  respectively, and the iteration value is random distributed in  $[0, 1]$ . So  $f_5(X, Y)$  is the encryption image which contains the amplitude spectrum  $\text{abs}[f_5(X, Y)]$  and the phase spectrum  $\text{angle}[f_5(X, Y)]$  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  $256 \times 256$ , 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  $x_0 = 0.6$  and  $u = 1.99$ ; the fractional of Fractional Fourier transform are  $P_x = 0.7$  and  $P_y = 0.8$ ; two generated parameters of  $\phi_{(x, y)}$  are  $x_{01} = 0.3$  and  $u_1 = 1.991$ ; but two generated parameters of  $\phi_{(x, y)}$  are  $x_{02} = 0.4$  and  $u_2 = 1.992$ . 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).



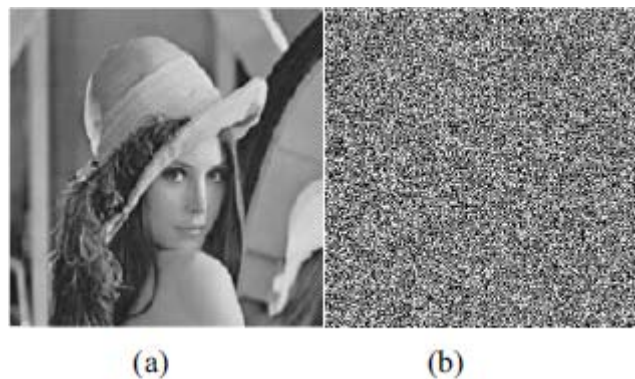
**Figure 2:** Image Encryption Result based on Fractional Fourier transform

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

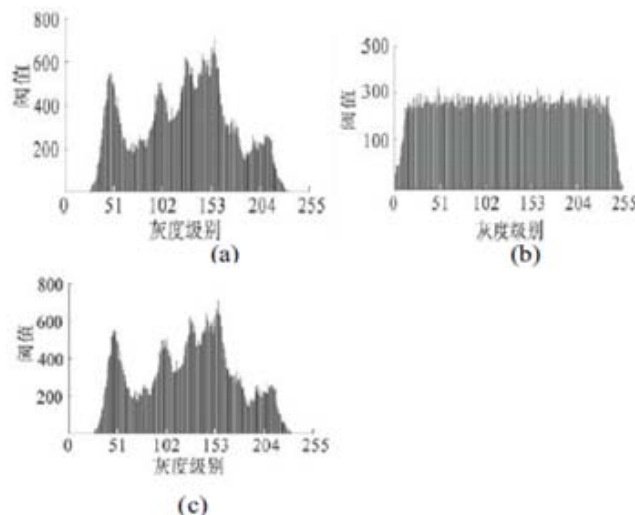
1) Analysis of the Key Space: The total key space of the image encryption algorithm proposed in this article is to  $10^{87}$ , wherein the magnitudes of key spaces of parameters  $x_0, x_1, x_2$  all are  $10^{15}$ , the magnitudes of key spaces of  $u_0, u_1, u_2$  all are  $10^{13}$  (considering 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 ( $u_1 = 1.990$ ), 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 Figure 2 (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 encryption based on fractional wavelet transform". Optics Communications, 2005, 254(4-6):361-367.
- [3] Xiaogang Wang and Daomu Zhao."Image encryption based on anamorphic 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] Namias V."The Fractional Fourier Transform and its Application in Quantum Mechanics". 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: Nonlinear Phenomena, 2004, 187(1-4):66-88.

## Author Profile



**Mudiyalak Akila Sowndarya** Obtained the B.Tech. Degree in Information Technology (IT) from Prakasam Engineering College, Kandukur. At present pursuing 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.