Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.650 – 655

IMAGE ENCRYPTION USING FRACTIONAL FOURIER TRANSFORM IN DRPE SCHEME

Preeti Yadav
Department of Electronics and Communication Engineering
The NorthCap University
preetiy280@gmail.com

ABSTRACT: Due to the fast evolution of digital data exchange, security of information becomes important. For industrial process images are used widely, therefore it is necessary to protect the confidential information. In the proposed work for encryption of image by the use of Fractional Fourier Transform(FRFT).This method enhances the security of data in comparison to DFT. In the proposed work we will be using an image as an input matrix and then multiplying it with the quadratic phase factor, this step will be the action performed by the first lens same action is performed by the second lens and image is encrypted, double random phase encoding is also used along with the transformation. This method offers a high resistance towards brute force attack.

Keywords- Discrete Fourier Transform(DFT), Fractional Fourier Transform(FRFT)

1. INTRODUCTION

Due to rapid development of internet and wide use of multimedia the digital information can be communicated among various people. The growing interest of optical system is due to the distinct advantage of processing in parallel manner. The need for security of information is increasing due to threats and interceptions from attackers. To overcome these threats we need new security methods. Optics field has revolutionalized the defence, medical and broadcasting system. For the distribution and storage of multimedia and data optical data storage has emerged as a good choice, in order to randomly access the stored data blue ray disk and compact disk can be used. Use of these devices made the optical technology popular. Government sector have spent money for the growth of "Cryptography technology". Refregier and Javidi proposed a new method for encoding of images " Double random phase encoding". We propose continuous FRFT using a scheme known as double random phase encoding(DRPE).Encryption and decryption of image is done using same transform order.

2. FRACTIONAL FOURIER TRANSFORM

This transform is generalized form of Fourier transform. It is a time frequency distribution and extension of classical Fourier transform. This transform is more flexible than conventional Fourier transform. Here transform order vary between 0 to 1.Keyspace is enlarged using this transform due to which FRFT based system are more secure.

This transform is more flexible than conventional Fourier transform due to extra parameter of transform order. Rotational angle is a multiple of $\pi/2$.

The α angle fractional fourier transform of a function f is denoted by F_α(u).

$$F_\alpha[f](u) = \sqrt{1 - i * \cot(\alpha)} e^{i*pi*\cot(\alpha)*u*u} \int_{-\infty}^{\infty} e^{-i*2*pi*(\csc(\alpha)*u*x - \frac{\cot(\alpha)*x*x}{2}} f(x)\,dx \quad (1)$$

Fractional kernel :

$$F_\alpha[f](u) = \int K_\alpha(u,x) f(x)\, dx \quad (2)$$

α angle kernel is

$$K_\alpha(u,x) = \sqrt{1 - \cot(\alpha)}\, \exp(i*pi*(\cot(\alpha)(x^2+u^2) - 2\csc(\alpha) u * x)) \quad (3)$$

If α is not a multiple of π above equation is used

$\delta(u-x)$ if α is a multiple of 2π

$\delta(u+x)$ if $\alpha+\pi$ is a multiple of 2π

3. DIGITAL IMPLEMENTATION

1. First lens action –
   - Multiplication of input matrix with quadratic phase factor.
   - QPF1= exp[-j*(pi/N)*tan(p*(pi/4))*(m*m)]
2. In order to accomplish free space propagation of step 1 following steps are used :
   - FFT
   - Result after FFT is multiplied with quadratic phase factor
     QPF2 =exp[-j*(pi/N)*sin(p*(pi/2))*(m'*m')]
   - Inverse FFT of the result after multiplication is taken
3. Second lens action –
   - Result generated from step2 is multiplied with QPF3
   - QPF3 =exp[-j*(pi/N)*tan(p*(pi/4))*(m''*m'')]

   Fair sampling condition –
   Sin(p*(pi/2)) < 1 (i)
   Tan(p*(pi/4)) <1 (ii)

   Condition (ii) is valid for p < 1
   Constant factor –

   Cp=(exp(-j*pi*sgn{sin[p(pi/2)]}/4 + j*p(pi/4))/sin $\left[p * \left(\frac{pi}{2}\right)\right]^{\frac{1}{2}}$

Input image is leena which is of size 256*256.Quadratic phase factor act as a random phase mask and it is multiplied with the input image. Fractional Fourier transform is applied on the image which is obtained after multiplication with the random phase mask. These mask act as a key during the encryption and decryption process. After transformation image is again multiplied with second random phase mask then again Fourier transform is taken, output obtained is the encrypted image.

During the decryption process encrypted image acts as a input, this input image is multiplied with conjugate of random phase mask2 then inverse fractional Fourier transform is taken. Again it is multiplied with random phase mask1 and then inverse fractional Fourier transform is taken, the resultant image we get is the decrypted image.

4. RESULTS OF DIGITAL IMPLEMENTATION

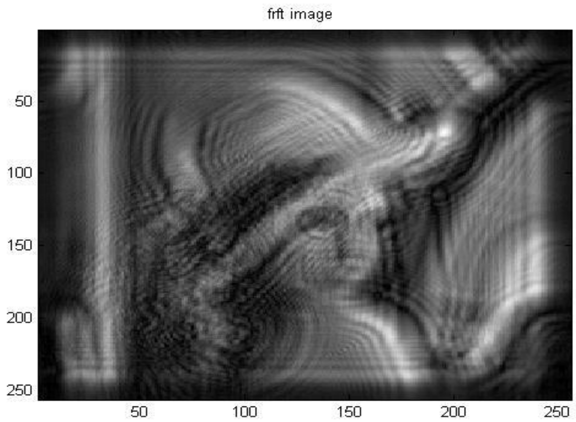


Figure 5.1 P=Q=0.25

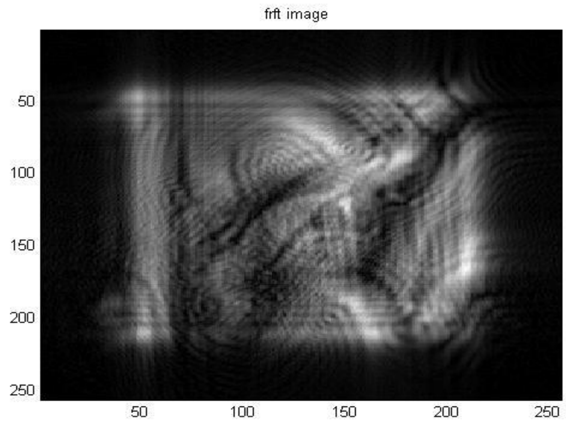


Figure 5.2 P=Q=0.50

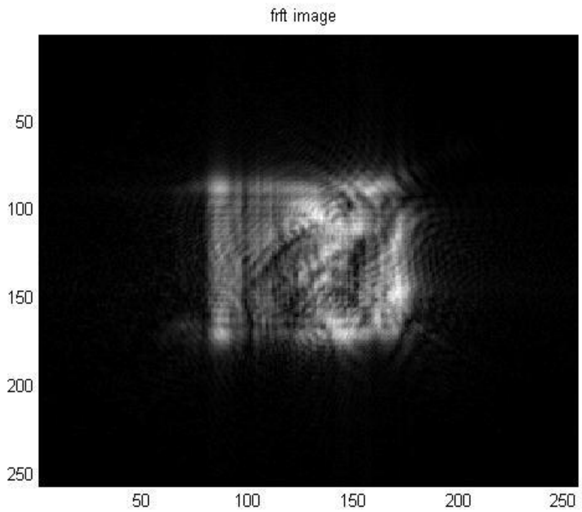


Figure 5.3 P=Q=0.75

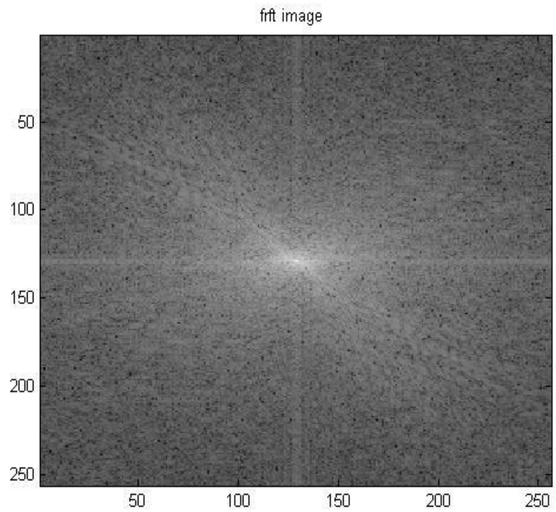


Figure5.4 P=Q=1

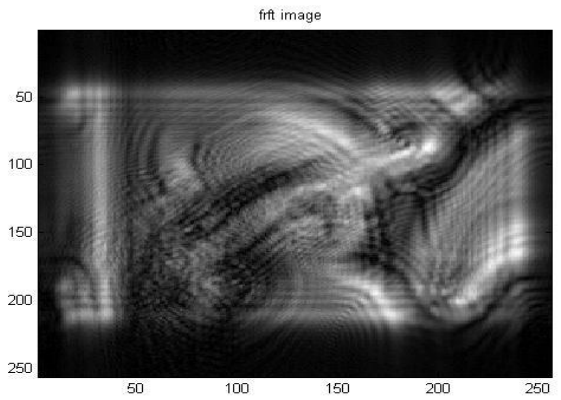


Figure 5.5 P= 0.25,Q= 0

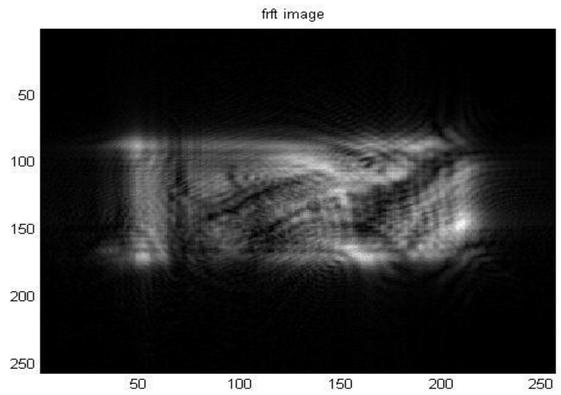


Figure 5.6 P= 0.50,Q= 0.75

5. EMPLOYING FRACTIONAL FOURIER TRANSFORM IN DRPE SCHEME

Steps for employing Fractional Fourier Transform in DRPE scheme:

Step1: The input image is multiplied with a random phase mask R1.

Step 2: The output is fractional Fourier transformed.

Step 3: Multiply with another random phase mask R2

Step 4: Take the Inverse fractional Fourier Transform of the output.

Step 5: Again apply fractional Fourier Transform.

Step 6: Multiply the output with the conjugate of random phase mask R2

Step 7: Take the inverse fractional Fourier Transform to retrieve the output image.

Figure 5.7 Input image of size 256*256

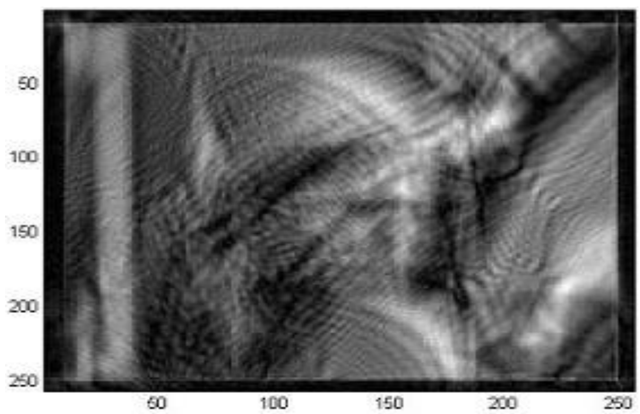
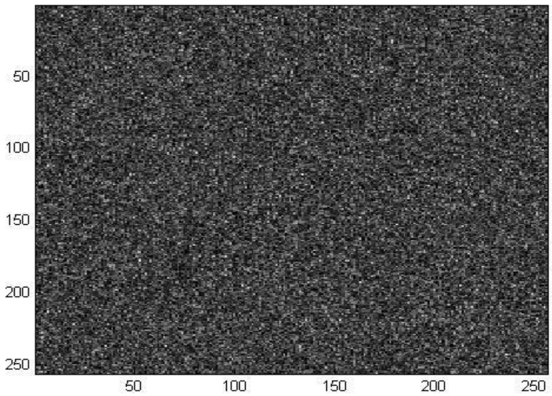


Figure 5.8 Transformed image



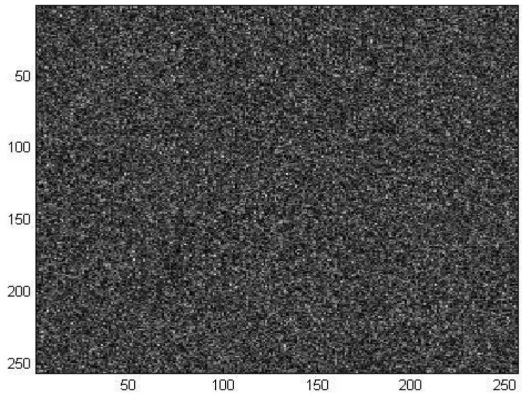


Fig 5.9Output after multiplying with RPM1 and taking FFT Fig5.10 Output after multiplying with RPM2 and taking IFFT

Figure 5.11 Decrypted image

6. CONCLUSION

For analyzing non stationary signals in time frequency plane, fractional Fourier transform proves to be a better tool. Numerical computation of FRFT is required in order to realize the FRFT based operators, filters etc. At different orders image is observed. We have used an algorithm for the digital implementation of fractional Fourier transform ,(FRFT)offers an extra degree of freedom in signal analysis. DRPE scheme is used for optical encryption, random phase masks act as key in this scheme during the encryption and decryption process

7. FUTURE SCOPE

(a)Faster algorithms for computation of 2-D FRT, 2-D inverse FRFT.DWT2,IDWT2 may result in further reduction in computation.

(b)To different format of images this work can be extended.

(c)This work may be extended using other transform methods.

REFERENCES

[1] Philippe Refregier and Bahram Javidi. Optical image encryption based on input plane and Fourier plane random encoding Vol. 20, No. 7 ,optics letters pp. 767-769 , April 1995.
[2] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain”, Optics letters, Vol. 25, No. 12 , pp. 887-889, June 15, 2003.
[3] Osamu Matoba, “Optical technique for information security”,Vol.97,IEEE June 2009.
[4] Javier Garcı´a, David Mas, and Rainer G. Dorsch, Fractional-Fourier-transform calculation through the fast-Fourier-transform algorithm,Vol 35,no. 35,January 1996.
[5] B. M. Hennelly, J. T. Sheridan, Image encryption and the fractional Fourier transform,Optik 114, No. 6 (2003) 251–265, 2003.
[6] Madan Singha, Arvind Kumar and Kehar Singh,” Encryption And Decryption Using A Phase Mask Set Consisting Of A Random Phase Mask And A Sinusoidal Phase Grating In The Fourier Plane”, ICOP 2009-International Conference on Optics and Photonics, CSIO,Chandigarh, India, 30 Oct.-1 Nov.2009.
[7] Madan Singh, Arvind Kumar and Kehar Singh, “Encryption And Decryption Using A Phase Mask Set Consisting Of A Random Phase Mask And A Sinusoidal Phase Grating In The Fourier Plane”, ICOP 2009-International Conference on Optics and Photonics, CSIO,Chandigarh, India, 30 Oct.-1 Nov.2009.
[8]M.A. Mohamed, A.S. Samarah, M.I. Fath Allah, “Optical Encryption Techniques: An Overview”, IJCSI International Journal of Computer Science Issues, Vol. 11, Issue 4, No 2, July 2014.
[9] Zhu B, Liu S, Ran Q: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. 25 (2000),pp 1159–1161.
[10] B. M. Hennelly and J. T. Sheridan, “Image encryption based on the fractional Fourier transform,” Proc. SPIE, vol. 5202, pp. 76–87, 2003.
[11]R. Tao, Y. Xin, and Y. Wang, “Double image encryption based on random phase encoding in the fractional Fourier domain,” Opt. Express, vol. 15, no. 24, pp. 16067–16079, 2007.
[12]R. Tao, X. M. Li, and Y.Wang, “Generalization of the fractional Hilbert transform,” IEEE Signal Process.Lett., vol. 15, pp. 365–368.
[13] M. T. Hanna, “Direct batch evaluation of optimal orthonormal eigenvectors of the DFT matrix,” IEEE Trans. Signal Process., vol. 56, no. 5, pp. 2138–2143, May 2008.
[14] M. T. Hanna, N. P. A. Seif, and W. A. E. M. Ahmed, “Hermite– Gaussian-Like eigenvectors of the discrete Fourier transform matrix based on the direct utilization of the orthogonal projection matrices on its eigenspaces,” IEEE Trans. Signal Process., vol. 54, no. 7, pp. 2815–2819, Jul. 2006.
[15] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett.20, pp767-769, (1995).
[16] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng. 36, pp992–998 (1997).
[17] N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” J. Opt. Soc. Am.A 16, 1915 (1999).
[18] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett.24, pp762-764 (1999).
[19]G.Unnikrishnan and K. Singh, “Optical encryption using quadratic Phasesystems,”Opt.Commun.193,pp51-67,(2001).
[20]Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng. 36, 1997:992-98.