Robust Technique for Image Encryption and Decryption Using Discrete Fractional Fourier Transform with Random Phase Masking

Ashutosh\textsuperscript{a}, Deepak Sharma\textsuperscript{b,1}

\textsuperscript{a} Modern Institute of Technology and Research Centre, Alwar, India
\textsuperscript{b} Jaypee University of Engineering & Technology, A.B.Road, Raghogarh, Guna 473226, India

Abstract

Encryption is one of the well known techniques to provide security in transmission of multimedia contents over the internet and wireless networks. There is use of image in all the area so its security is of great concern now a day. To focus on security aspect, in this paper we proposed a novel method of image encryption using discrete fractional Fourier transform (DFRFT) using exponential random phase mask. Encrypting with this technique makes it almost impossible to retrieve the image without using both the right keys. DFRFT is the generalization of the Discrete Fourier transform (DFT). This technique has been implemented and results are discussed in detail with analyzing parameters like Security, sensitivity and MSE.

© 2013 The Authors. Published by Elsevier Ltd. Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering

Keywords: Encryption; Fourier transform (FT); Discrete Fourier transform (DFT); fractional Fourier transform (FRFT); Discrete fractional Fourier transform (DFRFT).

1. Introduction

Fourier transform was first introduced by the French scientist Jean Baptiste Joseph Fourier, in 1807\cite{1}. After that FT was applied in all the field of science and engineering. Fractional Fourier Transform was introduced as the generalization of Fourier Transform, thus creating a scope of improvement where Fourier transform was applied. It has been applied to various areas like signal processing; optics and quantum mechanics \cite{1-4}. Discrete fractional Fourier transforms (DFRFT) was defined by Pei and Ozaktas \cite{5-6}. The discrete fractional Fourier transform (DFRFT) is a generalization of the DFT with additional free parameters \cite{5–7}. Pei and Yeh defined as the DFRFT.
based on the Eigen decomposition of the DFT matrix, a DFRFT with one fractional parameter was defined by taking fractional Eigen value powers of an Eigen decomposition of the DFT matrix [5]. The DFT Eigenvectors used in [16] are Hermit –Gaussian like. These Eigenvectors are computed from a DFT –comuting matrix proposed in [18]. Pei et al. first proposed the Eigen decomposition- based definition of the DFRFT [5], and then Candan et al. consolidated this definition [6].

In the recent year there is great concern over the information security. Various optical encryption methods have been proposed by the researchers in past two decades [8-17] [19-23]. We always look for more robust encryption schemes by which we protect the data for. This criterion may be fulfilled by proposing more robust transform and applying this transform in a model to achieve more unauthorized user protected scheme for encryption. We can apply two or more image using proposed method of encryption.

We propose Discrete FRFT with the double random phase encoding method to enhance its data security. We encrypted image using DFRFT and subsequently decrypted an image with same transform order. Security key is highly sensitivity to deviation in keys and it has been discussed in results.

The outline of this paper is as follows: In section II we discuss the FRFT and DFRFT in detail. In section III we discussed the proposed DFRFT based image encryption model for double random phase matrix. Section IV discussed the security and sensitivity. In section V we discussed the results.

2. Preliminaries

We know that Fourier transform is the rotation of a signal by angle of $\pi/2$ in time frequency plane. Fractional Fourier transform remove that constrain and allow rotation of angle ‘$\alpha$’ where it not a multiple of $\pi/2$. We can define the FRFT of signal $x(t)$ of order ‘$p$’ as

$$X_p(u) = \int_{-\infty}^{\infty} x(t)K_p(u,t)dt.$$  \hspace{1cm} (1)

There is a relation between the angle of rotation ‘$\alpha$’ and order given as $\alpha = p\pi/2$. The kernel $K_p$ is defined as

$$K_p(u,t) = \begin{cases} 
\sqrt{1 - j\cot \alpha} & \text{if } a \neq n\pi \\
\delta(t-u) & \text{if } a = 2n\pi \\
\delta(t+u) & \text{if } a = (2n \pm \pi) 
\end{cases} \hspace{1cm} (2)$$

As there was the development in the field of digital signal processing, there was a need of discrete fractional Fourier transform for all the application using fractional Fourier transform because all the signal are studied in discrete form. DFRFT is the generalization of the discrete Fourier transform (DFT). Some basic properties are

1) Unitary
2) Additive
3) Reduction to DFT when order is equal to unity.

The M×M DFT matrix can be expressed as
\[ X = \frac{1}{\sqrt{M}} e^{-\frac{j2\pi km}{M}}, \quad k \geq 0, \quad m \leq M - 1 \]  

(3)

Matrix X has only four distinct Eigen values 1, -1, j and -j. Now we define a \(M \times M\) matrix \(Z\) whose entries are

\[ Z_{m,m} = 2\cos\left(\frac{2\pi}{M} n\right), \quad 0 \leq n \leq M - 1 \]

\[ Z_{m,m+1} = Z_{m+1,m} = 1, \quad 0 \leq n \leq M - 2 \]

\[ Z_{M-1,0} = Z_{0,M-1} = 1 \]  

(4)

Now as \(ZX=XZ\), i.e. they commute with each other. They have same value of Eigen vector but different Eigen values. Now we can define \(M \times M\) DFRFT matrix as

\[ X^\alpha = VD^\alpha V^T \]

\[ = \begin{cases} 
\sum_{k=0}^{M-1} e^{-\frac{j2\pi k\alpha}{M} M} v_k v_k^T & \text{for } M=\text{odd} \\
\sum_{k=0}^{M-2} e^{-\frac{j2\pi (k+1)\alpha}{M} M} v_k v_k^T + e^{-\frac{j2\pi M\alpha}{M} M} v_M v_M^T & \text{for } M=\text{even} 
\end{cases} \]  

(5)

Here \(D\) is the diagonal matrix and \(T\) is for transpose. The matrix \(V\) is defined as

\[ V = [v_0, v_1, \ldots, v_{M-2}, v_{M-1}] \quad \text{for } M=\text{odd} \]

\[ V = [v_0, v_1, \ldots, v_{M-2}, v_M] \quad \text{for } M=\text{even} \]  

(6)

This is known as Eigen decomposition form of DFRFT.

3. Proposed Method for Image Encryption and Decryption.

**Encryption Model:**

Encryption is very ancient technique to hide data. It is a process in which information is secured with the help of a key to protect it from the unauthorized person, information which has to be encrypted can be in form of text or image etc. In proposed method image encryption of gray scale image is done using double random discrete fractional Fourier transform method. In Gray scale image the value of each pixel carries only intensity information. They are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. It is also known as gray scale image. The intensity range is from 0 to 255.

In double random matrix DFRFT method, input image is multiplied with the first exponential random matrix \(S\) after that the DFRFT of order \(\alpha\) is applied then, resulting matrix is multiplied by the second exponential random matrix \(C\) and again DFRFT of order \(\beta\) is applied to get the encrypted image. Random matrix at encryption and decryption should be orthogonal to each other.
Exponential random matrix S and C should be independent of each other. The value of \( S = e^{j\alpha m} \) and \( C = e^{j\beta m} \).

Now let understand the mathematics of proposed encryption process.

\[
W' = P \otimes e^{j\alpha n}
\]  
(7)

Where P is input image matrix multiplied by S the random matrix \( W'' = X^\alpha(P \otimes e^{j\alpha n}) \) (8)

DFRFT of order \( \alpha \) is applied.

\[
W''' = (X^\alpha(P \otimes e^{j\alpha n})) \times e^{j\beta m}
\]  
(9)

Then it is multiplied by random matrix C.

\[
E = X^\beta((X^\alpha(P \otimes e^{j\alpha n})) \times e^{j\beta m})
\]  
(10)

In equation 10 we apply the DFRFT of order \( \beta \) to get encrypted Image E.

**Decryption Model:**

Decryption is the process of retrieving the original information from the encrypted form. It is reverse process of the encryption part. Input here is encrypted image .input image ‘E’ is taken then DFRFT of order ‘-\( \beta \)’ is applied then to it random matrix C* is multiplied which cancel out the effect of random matrix C as they both are orthogonal to each other .To the resulting matrix DFRFT of order ‘-\( \alpha \)’ is applied then multiplied by the random matrix S* to get the decrypted image.

\[
E' = X^{-\beta}(E)
\]

\[
= X^{-\beta}(X^\beta((X^\alpha(P \otimes e^{j\alpha n})) \otimes e^{j\beta m}))
\]  
(11)
Then it is multiplied by the random matrix $C^*$ as it will cancel out the effect of $C$ as they are orthogonal.

$$E^* = (X^{-\beta^2} (X^{\beta} ((X^2 (P \otimes e^{j\varphi})) \otimes e^{j\beta})) \otimes e^{-j\beta})$$

(12)

Now, DFRFT of order $-\alpha$ is applied

$$E' = X^{-\alpha} ((X^{-\beta} (X^{\beta} ((X^2 (P \otimes e^{j\varphi})) \otimes e^{j\beta})) \otimes e^{-j\beta}))$$

(13)

Then random matrix $S^*$, is multiplied

$$D = (X^{-\alpha} ((X^{-\beta} (X^{\beta} ((X^2 (P \otimes e^{j\varphi})) \otimes e^{j\beta})) \otimes e^{-j\beta})) \otimes e^{-j\varphi})$$

(14)

Where D is the decrypted image and after solving it gives original image ‘P’ as output.

4. Salient Features

A. Security

Security is main aim. Key here is formed by the combination of the order of discrete fractional Fourier transform order and the random matrix, as there can be large amount of the combination so this gives formidable key sets, thus providing higher amount of security. This is also effective against brute force attack i.e. if all the set of key are known. In this case as the key set is large time taken is very large in brute force attack thus making it impractical to crack the correct key.

B. Sensitivity

The method of encryption and decryption should be sensitive that means if the any key other than the correct key is used it will not give correct result with our simulation we have checked that our image and is very much sensitive to the deviation in the original key.

C. Complexity

There is tradeoff between the complexity and the security. For image of dimension $M \times N$ as we are applying Eigen vector decomposition type of DFRFT in the proposed technique. It lacks Fast Fourier Transform (FFT) algorithm. To get the encrypted and decrypted results multiplications between matrices is done and the no of complex multiplication which take place is $M^2N + MN^2$.

5. Results

We have successfully encrypted and decrypted the image using double random matrix DFRFT method in this paper. Simulation of the proposed method has been done on a greyscale image of Lena of dimension $300 \times 300$. Image was encrypted for order $\alpha = 0.8, \beta = 1.2$ by using two exponential random matrix S and C which are independent to each other. As we can see that fig3(a) is the original image and after encryption we get the encrypted image as shown in the fig 3(b).for the decryption process we have to apply the order $\alpha = -0.8$ and $\beta = -1.2$ to get the correct decrypted image which we can see in the figure 3(c) and if the proper value of the order is not used then it will not give the correct result as we can see in fig 3(d),here the order used was $\alpha = 0.9, \beta = 1.1$ the image can be decrypted only by using the correct order.

Histogram is plotted for original image and encrypted image which summarizes the intensity of an image frequency at each pixel value shown in fig 4 . In fig 4(a) and 4(b) shows the histogram of the original image and the encrypted image of the image of Lena. As we can see that the histogram of the encrypted image is completely different from that of original image so it doesn’t give any idea to unauthorized person to carry on the attack.

MSE (mean square error) is also calculated between the original image and decrypted image it is calculated by
The Mean Square Error (MSE) of images is calculated to check the consistency of the proposed technique. Size of the entire image taken is different and they are encrypted /decrypted using the proposed method and 201 Iteration were done for each image to get the result as shown in the table. The method is quite consistent. Image taken is different and they are encrypted /decrypted using the proposed method and as shown in the table. The method is quite consistent.

Fig. 5 shows the sensitivity of key, image will be correctly decrypted only by the use of original key, if there is small deviation in the key then it will show a sharp increase in the normalized MSE. Comparison of FRFT and DFRFT has been done. Results show that DFRFT is more sensitive to the deviation in key.
6. Conclusion

In this paper a novel method is proposed for encryption using double random matrix using DFRFT. The algorithm used with DFRFT is Eigen vector decomposition type. Encryption and decryption has been done successfully. Various parameters have been analyze and discussed like MSE, sensitivity and key space etc.

References

[1] R. Tao, B. Deng, and Y. Wang, “Research progress of the fractional Fourier transform in signal processing,” Springer, vol. 49, pp. 1–25, Jan 2006.
[2] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, The Fractional Fourier Transform with Applications in Optics and Signal Processing. New York: Wiley, 2000.
[3] L. B. Almeida, “The fractional Fourier transform and time-frequency representations,” IEEE Trans. Signal Process., vol. 42, no. 11, pp. 3084–3091, Nov. 1994.
[4] V. Namias, “The fractional order Fourier transform and its application to quantum mechanics,” J. Inst. Math. Appl., vol. 25, pp. 241–265, 1980
[5] S. C. Pei and M. H. Yeh, “Improved discrete fractional Fourier transform,” Opt. Lett., vol. 22, pp. 1047–1049, 1997.
[6] C. Candan, M. A. Kutay, and H. M. Ozaktas, “The discrete fractional Fourier transform,” IEEE Trans. Signal Process., vol. 48, no. 5, pp. 1329–1337, May 2000.
[7] S. C. Pei and W. L. Hsue, “The multiple-parameter discrete fractional Fourier transform,” IEEE Signal Process. Lette., vol. 13, no. 6, pp. 329–332, Jun. 2006.
[8] G. Unnikrishnan and K. Singh, “Double random fractional Fourier-domain encoding for optical security,” Opt. Eng., vol. 39, pp. 2853–2859, 2000.
[9] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double random phase encoding in the fractional Fourier domain,” Opt. Lett., vol. 25, no. 12, pp. 887–889, 2000.
[10] Zhu B, Liu S, Ran Q: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. 25 (2000) 1159–1161.
[11] B. M. Hennelly and J. T. Sheridan, “Image encryption based on the fractional Fourier transform,” Proc. SPIE, vol. 5202, pp. 76–87, 2003.
[12] 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.
[13] R. Tao, X. M. Li, and Y. Wang, “Generalization of the fractional Hilbert transform,” IEEE Signal Process. Lett., vol. 15, pp. 365–368, 2008.

[14] Hennelly B, Sheridan JT: Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. 28 (2003) 269–271.

[15] S.C.Pei and W.L.Hsue, “Random discrete fractional Fourier transform,” IEEE Signal Process. Lett., vol. 16, no. 12, pp. 1015–1018, Dec. 2009.

[16] L. J. Yan and J. S. Pan, “Generalized discrete fractional Hadamard transformation and its application on the image encryption,” in Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, 2007, pp. 457–460.

[17] H. Al-Qaheri, A. Mustafi, and S. Banerjee, “Digital watermarking using ant colony optimization in fractional Fourier domain,” J. Inf. Hiding Multimedia Signal Process., vol. 1, no. 3, pp. 179–189, Jul. 2010.

[18] B. W. Dickinson and K. Steiglitz, “Eigenvectors and functions of the discrete Fourier transform,” IEEE Trans. Acoust., Speech, Signal Process., vol. ASSP-30, pp. 25–31, Jan. 1982.

[19] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, 767-769, (1995).

[20] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng. 36, 992–998 (1997).

[21] N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” J. Opt. Soc. Am. A 16, 1915 (1999).

[22] O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett. 24, 762-764 (1999).

[23] G. Unnikrishnan and K. Singh, “Optical encryption using quadratic phase systems,” Opt. Commun. 193, 51-67, (2001).