International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

Image Encryption Using Discrete Fourier Transform and Fractional Fourier Transform

Ashutosh, Deepak Sharma

Abstract*— Growing with the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. The security system based on the fractional Fourier transform (FRFT) is protected by only a certain order of FRFT. In this paper, we proposed a novel method to encrypt an image by using Discrete Fourier Transform (DFT) and Fractional Fourier Transform (FRFT). In this paper, we analyze the image encryption using DFT and FRFT based on double random phase matrix. The implementation of both techniques has been realized for experimental purposes. Detailed results in terms of security analysis and implementation are given. Comparative study with traditional encryption algorithms is shown the superiority. The proposed encoding scheme significantly enhances the data security in comparatively than DFT and FRFT.

Index Terms*— Discrete Fourier Transform (DFT), Decryption, Encryption, Fourier Transform (FT), Fractional Fourier Transform (FRFT).

I. INTRODUCTION

The continuous fractional Fourier transform (FRFT) is a generalization of the continuous Fourier transform and has been applied in optics, quantum mechanics, and signal processing areas [1–3]. The fractional Fourier transform (FRFT) is more flexible than the conventional Fourier transform (FT) due to the extra parameter of the transform order. With the transform order gradually varying from 0 to 1, the FRFT of a signal can develop from the original function to its FT [1-4]. Thus, it has recently shown its potential in the fields of the image and the optical encryption. Using the transform order to enlarge the key space, the systems based on the FRFT are of a higher security [5-15].

To obtain the discrete version of the continuous FRFT, the discrete fractional Fourier transform (DFRFT) was defined by pei and ozaktas [16-17]. The discrete fractional Fourier transform (DFRFT) is a generalization of the DFT with additional free parameters [16–18]. In [16], Pei and Yeh defined 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. The DFT eigenvectors used in [16] are Hermit –Gaussian like.

Manuscript received April, 2013.

Ashutosh, Department of Electronics and Communication, Jaypee University of Engg. And Technology, Guna, India.

Deepak Sharma, Department of Electronics and Communication, Jaypee University of Engg. And Technology, Guna, India.

These eigenvectors are computed from a DFT –commuting matrix proposed in [19]. Pei *et al.* first proposed the eigen decomposition- based definition of the DFRFT [16], and then Candan *et al.* consolidated this definition [17]. Hanna *et al.* considered generation eigenvectors by the singular value decomposition method and direct batch evaluation [20-22].

Information security has been receiving increasing attention in recent years. In the past twenty years, a number of optical encryption methods have been proposed by the researchers in [6-15] and [23-27]. Among them, the most widely used and highly successful optical encryption scheme is double random phase encoding proposed by Refregier and Javidi [23]. This method uses two random phase masks, one in the input plane and the other in the Fourier plane, to encrypt the primary image into stationary white noise. Unnikrishnan and Singh [6-7], [27] first proposed an optical encryption method using random phase encoding in the fractional Fourier domain and its optically-implemented approach. The two Fourier transform operators in Ref. 1 were replaced by two FRFT operators. The remarkable feature of optical encryption based on the FRFT is the fractional order, which enlarges the key space and further enhances the security of encryption systems. The resulting keys for decryption are the fractional order parameters of the FRFT and the random phase codes used in the encryption process.

To increase the security of data we always look forward to propose further more robust encryption schemes by which we protect the data for unauthorized user. 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. Our proposed scheme can be apply with the two or more image encryptions. The proposed encryption scheme is realized by the fast Fourier transform (FFT)-based algorithm. Simulation results demonstrate that the image decryption is highly sensitive to the deviations in the security keys.

We propose continuous FRFT with the double random phase encoding method to enhance its data security. We encrypted the image based on DFT and FRFT and subsequently decrypted an image with same transform order.

The outline of this paper is as follows: In section II we discuss the DFT and FRFT in more detail outlining a mathematical definition and the algorithm used. In section III we discussed the proposed DFT based image encryption model for both single and double random phase matrix along with their simulated results. Section V we have shown our FRFT based image encryption scheme with their simulated results. In section VI we discussed the numerical evaluation of simulated results and their comparison.

II. PRELIMINARIES

A. *Discrete Fourier Transform*

The DFT of a signal x_n is given by the expression,

$$X_k = \sum_{n=0}^{N-1} x_n e^{-j2\pi kn/N} \qquad k = 1, 2, ..., N \qquad (1)$$

for the line spectrum at frequency $\omega_k = (2\pi)\frac{k}{T}$

The inverse DFT (IDFT) which is used to reconstruct the signal is given by

$$x_n = \frac{1}{N}\sum_{k=0}^{N-1} X_k e^{j2\pi kn/N} \qquad (2)$$

B. *Fractional Fourier Transform (FRFT)*

The FRFT can be seen as a linear transformation, which rotates the signal through any arbitrary angle into a mixed frequency – space domain. It can be applied to the entire field where Fourier transform is applied with better results like image processing, quantum physics and communication. We can define the expression for the *p*-th FRFT of a signal $x(t)$ is defined as,

$$\{F_p[x(t)]\}(u) = \int_{-\infty}^{\infty} x(t) K_P(u,t)\,dt \qquad (3)$$

Here $\alpha = \frac{p\pi}{2}$ is the angle at which FRFT is to calculate.

Where K_P is the kernel defined as

$$K_p(t,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}}\exp\left(j\frac{t^2+u^2}{2}\cot\alpha - jut\csc\alpha\right) & p \neq 2n \\ \delta(t-u) & p = 4n \\ \delta(t+u) & p = 4n+2 \end{cases} \qquad (4)$$

The FRFT is periodic with the period of 4, the transform order can be limited in the interval [-2, 2].

III. IMAGE ENCRYPTION AND DECRYPTION USING DISCRETE FOURIER TRANSFORM

A. *Image Encryption using DFT with Single Random Matrix*

We have an input image of Lena "P" of 'N×M' size then we multiply the random matrix $e^{j\beta s)}$ to an input image "*P*" to get the modified image *Y*. Now we apply DFT transform to this modified image *Y* we get the encrypted image *P'*. For decryption part we take the IDFT of the encrypted image then we multiply with the same random matrix complex conjugate of the matrix S* such that it cancel the result of the previously multiplied random matrix for that we have taken the random matrix to be orthogonal. Here the key is formed by the combination of the transform and the random matrix. The model is also described with the help of block diagram.

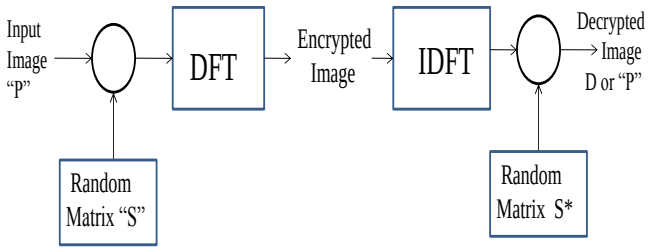


Fig.1 DFT based Encryption and Decryption using single random phase matrix

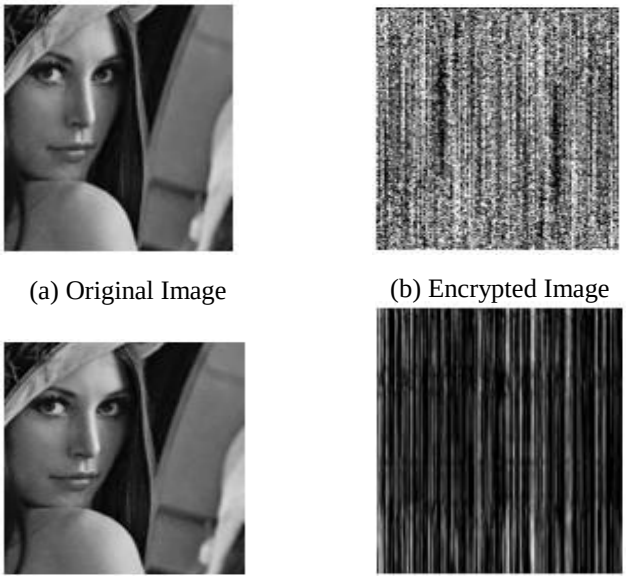
$$Y = P \otimes [e^{j\beta s)}] \qquad (5)$$

$$P' = \sum_{n=0}^{N-1} \left\{P \otimes [e^{j\beta s)}]\right\} e^{-j2\pi kn/N} \qquad (6)$$

$$Y' = \frac{1}{N}\sum_{k=0}^{N-1}\sum_{n=0}^{N-1} \left\{P \otimes [e^{j\beta s)}]\right\} e^{-j2\pi kn/N} e^{j2\pi kn/N} \qquad (7)$$

$$P = D = \frac{1}{N}\sum_{k=0}^{N-1}\sum_{n=0}^{N-1} \left\{P \otimes [e^{j\beta s}]\right\} e^{-j2\pi kn/N} e^{j2\pi kn/N} . e^{-j\beta s} \qquad (8)$$

After applying this process we found the simulated result on Matlab R2011a



(a) Original Image (b) Encrypted Image

(c) Correct decrypted Image (d) Decrypted Image with wrong key

Fig.2 Image encryption /Decryption using DFT with single random matrix

B. *Image encryption/decryption using double random matrix discrete Fourier transform*

This proposed scheme we used two random matrixes so that the complexity of the system is increased but encryption model is more robust towards brute force attack. In this scheme we have cascaded another stage of the image encryption and analyzed the model. We have an input image

of Lena "P" of 'N×M' size then we multiply the random matrix $e^{j\beta s}$ to an input image "P" to get the modified image Y. Now we apply DFT transform to this modified image Y we get the encrypted image P'. Again this image P' is multiplied by a random matrix $e^{j\beta c}$ then again we have taken the DFT of image. For decryption part we take the IDFT of the encrypted image "Q" then we multiply with the random matrix complex conjugate of the matrix $e^{-j\beta c}$ such that it cancel the result of the previously multiplied random matrix $e^{j\beta c}$ then again we take the IDFT of the still encrypted image the finally multiplied by the matrix $e^{-j\beta s}$ for that we have taken the random matrix to be orthogonal. It produces the finally decrypted image. Random matrix used 'S' and 'C' should be orthogonal. Key is formed by the combination of both the random matrix and the transformed used. Security is increased so is the complexity is higher with as compared to previous method. Now the entire process is depicted with the help of block diagram shown in fig. 3 and fig.4

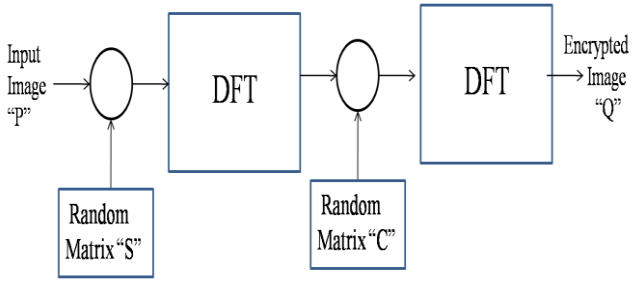


Fig.3 Block diagram for the encryption process using DFT

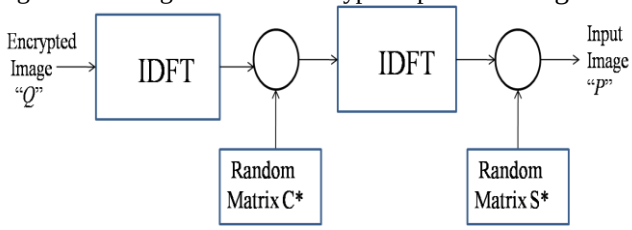


Fig.4 Block diagram for decryption process using DFT

Mathematically the encryption process in double random phase matrix can be given as

$$Y = P \otimes [e^{j\beta S)}] \tag{9}$$

$$Y' = \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S)}]\} e^{-j2\pi kn/N} \tag{10}$$

$$Y'' = \left\{ \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S}]\} e^{-j2\pi kn/N} \right\} e^{j\beta C} \tag{11}$$

$$Y''' = \sum_{n=0}^{N-1} \left\{ \left\{ \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S}]\} e^{-j2\pi kn/N} \right\} e^{j\beta C} \right\} e^{-j2\pi kn/N} = Q \tag{12}$$

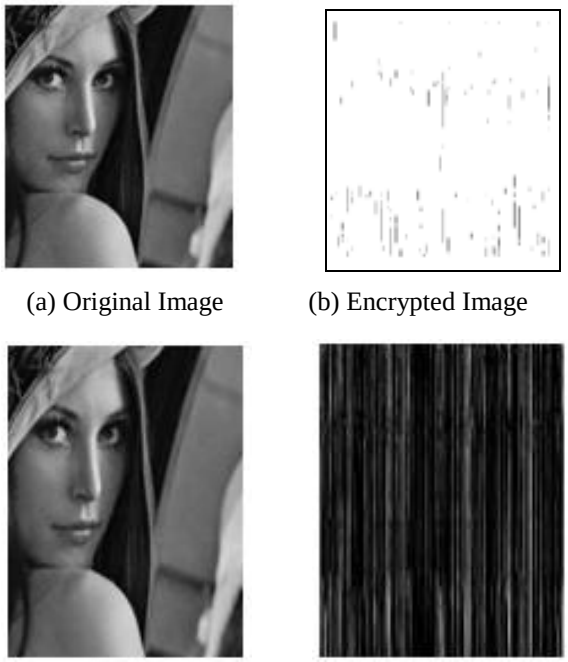
For the decryption process we have followed these steps.

$$Y'' = \frac{1}{N} \sum_{k=0}^{N-1} \left\{ \sum_{n=0}^{N-1} \left\{ \left\{ \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S}]\} e^{-j2\pi kn/N} \right\} e^{j\beta C} \right\} e^{-j2\pi kn/N} \right\} e^{j2\pi kn/N} \tag{13}$$

$$() \quad Y' = \left[\frac{1}{N} \sum_{k=0}^{N-1} \left\{ \sum_{n=0}^{N-1} \left\{ \left\{ \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S}]\} e^{-j2\pi kn/N} \right\} e^{j\beta C} \right\} e^{-j2\pi kn/N} \right\} e^{j2\pi kn/N} \right] e^{-j\beta C} \tag{14}$$

$$P = \frac{1}{N} \sum_{k=0}^{N-1} \left[\frac{1}{N} \sum_{k=0}^{N-1} \left\{ \sum_{n=0}^{N-1} \left\{ \left\{ \sum_{n=0}^{N-1} \{P \otimes [e^{j\beta S}]\} e^{-j2\pi kn/N} \right\} e^{j\beta C} \right\} e^{-j2\pi kn/N} \right\} e^{j2\pi kn/N} \right] e^{-j\beta C} e^{j2\pi kn/N} e^{-j\beta S} \tag{15}$$

The Proposed on MATLAB 2011 are shown below.



(a) Original Image (b) Encrypted Image

(c) Correct decrypted Image (d) Decrypted Image with incorrect key

Fig.5 Image encryption/decryption using double random matrix Discrete Fourier Transform..

IV. IMAGE ENCRYPTION/DECRYPTION USING FRACTIONAL FOURIER TRANSFORM

The word In this proposed scheme Encryption is done by with using two random phase matrix in by Fractional Fourier domain. This provides us with the extra parameter of order of the fractional Fourier transform which result in the better security than earlier two proposed schemes. The authors propose an encryption scheme very similar to the one described above, making use of the extra degree of freedom offered by the FRFT. Fig. 6 is used to represent the encryption scheme and fig.7 represents an idea of decryption schemes. Two phase matrices are used which are in the form of two statistically independent matrices. In this method author consist an input image '*L*' which is multiplied by the random matrix and their resulting matrix is

transformed through the order 'a' by taking its FRFT at an angle α to get the encrypted image at stage one similarly another random matrices is generated as $\{e^{j\gamma m}\}$ and then again FRFT is take by an order of b-a here the order is considered in the range of [-2 to 2] because the FRFT is of the periodicity of 4.the reverse process is applied for the decryption scheme. The key for decrypted image is formed here by the combination of the order of the Fractional Fourier transform and the random matrix .

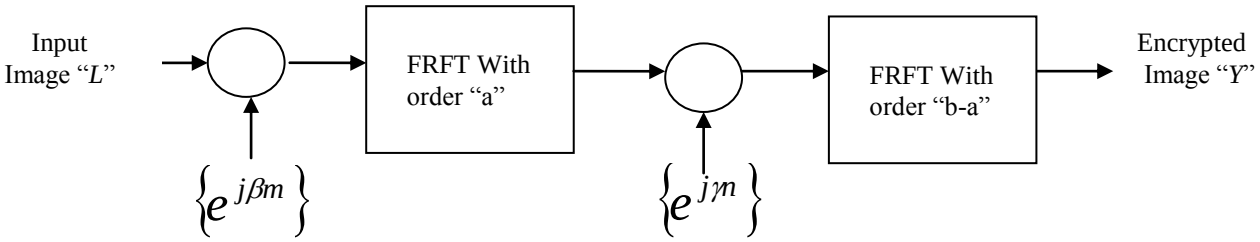


Fig.6 Proposed Image encryption Model using FRFT with double random matrix

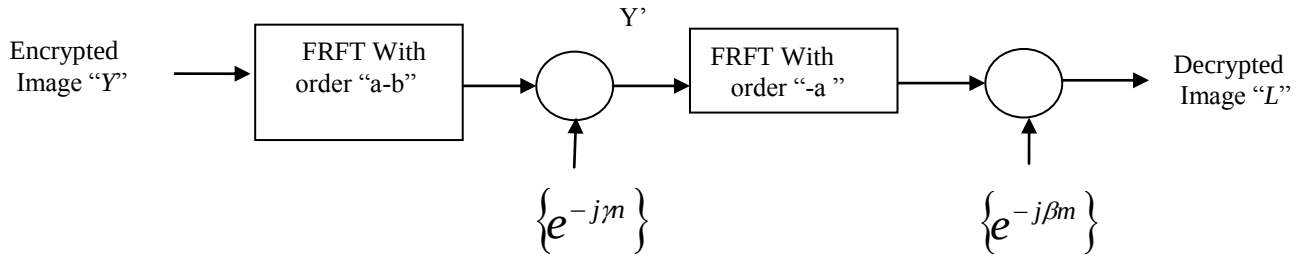


Fig.7 Proposed Decryption scheme using FRFT with double random matrix

Mathematically the encryption process can be summarized as, The input image $L(x)$ is multiplied by the random matrix $\{e^{j\beta m}\}$ then,

$$L' = L(x)\,e^{j\beta m} \tag{16}$$

The FRFT operation is applied by an order of "a" is given as,

$$L'' = F_a\left[L(x)\{e^{j\beta m}\}\right] \tag{17}$$

$$L''' = F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m} \tag{18}$$

$$L''' = F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m} \tag{19}$$

The finally encrypted image is given as,

$$L'''' = F_{b-a}\left[F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m}\right] = Y \tag{20}$$

Now the process at the decryption side is given as,

$$L''' = F_{a-b}\left\{F_{b-a}\left[F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m}\right]\right\} \tag{21}$$

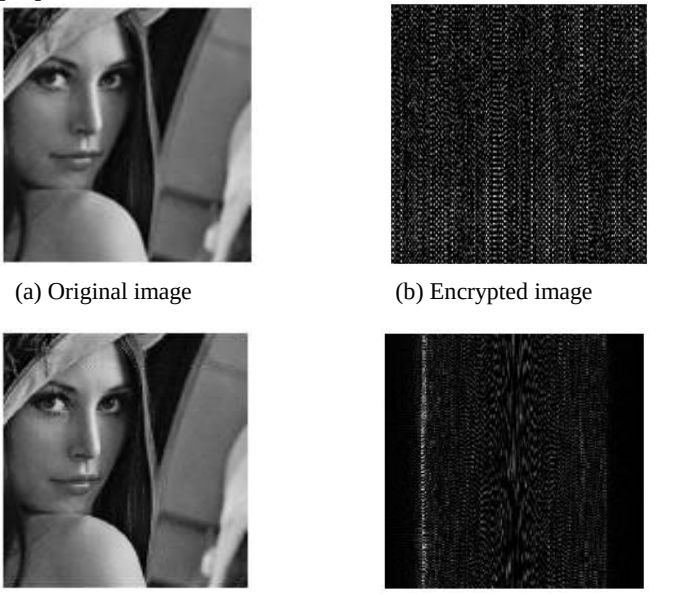
$$L'' = F_{a-b}\left\{F_{b-a}\left[F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m}\right]\right\}\left[e^{-j\chi m}\right] \tag{22}$$

$$L'' = F_{-a}\left[F_{a-b}\left\{F_{b-a}\left[F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m}\right]\right\}\right] \tag{23}$$

The finally decrypted image is given by,

$$L = \left[F_{-a}\left[F_{a-b}\left\{F_{b-a}\left[F_a\left[L(x)\{e^{j\beta m}\}\right]e^{j\chi m}\right]\right\}e^{-j\chi m}\right]\right]e^{-j\beta m} \tag{24}$$

The simulated results on MATLAB 2011 is given for proposed model is,



(a) Original image (b) Encrypted image

(c) Correct Decrypted image (d) Decrypted image at incorrect order

Fig.8 Image encryption/decryption using Fractional Fourier Transform.

V. RESULTS DISCUSSION AND CONCLUSION

In this paper we have encrypt the image using DFT single and double random phase matrix while using FRFT with double random phase matrix. Using these methods we decrypted an image successfully. The performance of the proposed encryption scheme is evaluated on the basis of the mean

square error (MSE) between the original image and the decrypted.

$$(\text{MSE}) = \frac{1}{AB}\sum_{i=1}^{A}\sum_{j=1}^{B}\left[L(i,j) - \hat{L}(i,j)\right]^2$$

Where A and B indicated the size of the image while $L(i,j)$ and $\hat{L}(i,j)$ indicates the original and decrypted image of pixel (i,j) respectively. The computation complexity of the DFT is calculated by the $O(N^2)$

Table 1

Encryption Schemes	Parameters	
	Mean Square Error (MSE)	Computational Complexity
DFT with Single Random Matrix	1.0401×10^{-13}	Less complex
DFT with Double Random Matrix	2.1118×10^{-13}	Moderate complex.
FRFT with Double Random Matrix	0.0577	Most Complex

ACKNOWLEDGMENT

The Authors thankfully acknowledge the all authorities of Jaypee University of Engineering & Technology, Guna (M.P.) - 473226 INDIA

REFERENCES

[1] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. New York: Wiley, 2000.
[2] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Trans. Signal Process.*, vol. 42, no. 11, pp. 3084–3091, Nov. 1994.
[3] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," *J. Inst. Math. Appl.*, vol. 25, pp. 241–265, 1980.
[4] D. Mustard, "The fractional Fourier transform and the Wigner distribution," *J. Aust. Math. Soc. B*, vol. 38, pp. 209–219, 1996.
[5] R. Tao, B. Deng, and Y. Wang, "Research progress of the fractional Fourier transform in signal processing," *Science in China (Ser.F, Information Science)*, vol. 49, pp. 1–25, Jan. 2006.
[6] G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.*, vol. 39, pp. 2853–2859, 2000.
[7] 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.
[8] Zhu B, Liu S, Ran Q: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. 25 (2000),pp 1159–1161
[9] B. M. Hennelly and J. T. Sheridan, "Image encryption based on the fractional Fourier transform," *Proc. SPIE*, vol. 5202, pp. 76–87, 2003.
[10] 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.
[11] R. Tao, X. M. Li, and Y.Wang, "Generalization of the fractional Hilbert transform," *IEEE Signal Process. Lett.*, vol. 15, pp. 365–368, 2008.
[12] Hennelly B, Sheridan JT: Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. 28 (2003),pp 269–271.
[13] 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.
[14] 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.
[15] 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.
[16] S. C. Pei and M. H. Yeh, "Improved discrete fractional Fourier transform," *Opt. Lett.*, vol. 22, pp. 1047–1049, 1997.
[17] 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.
[18] 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.
[19] 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.
[20] 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 singular value decomposition of its orthogonal projection matrices," *IEEE Trans. Circuits Syst. I*, vol. 51, no. 11, pp. 2245–2254, 2004.
[21] 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.
[22] 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.
[23] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, pp767-769, (1995).
[24] 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).
[25] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A 16, 1915 (1999).
[26] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. 24, pp762-764 (1999).
[27] G. Unnikrishnan and K. Singh, "Optical encryption using quadratic Phasesystems,"Opt.Commun.193,pp51-67,(2001).

ASHUTOSH has done his Bachelors of Technology from Maharishi Arvind institute of Engineering & Technology, Jaipur in 2010.Currently he is pursuing Masters of technology from Jaypee University of Engineering and technology, Guna .His area of interest are Image processing and Signal Processing.

DEEPAK SHARMA completed his M. Tech. (Microwave Engineering) from Madhav Institute of Technology and Science in 2006. Before joining JUET, he worked as a Lecturer in Electronics Department, MITS, Gwalior (M.P). His Research areas includes Microwave Engineering. Antenna Theory, Radar System and Signal processing and Image Processing.