A Novel Image Encryption Scheme based on Multiple Parameter Discrete Fractional Fourier Transform

Deepak Sharma
Department of Electronics & Communication Engineering
Jaypee University of Engineering & Technology
Guna (M.P.) 473226, INDIA

Rajiv Saxena
Department of Electronics & Communication Engineering
Jaypee University of Engineering & Technology
Guna (M.P.) 473226, INDIA

ABSTRACT

Security is one of the most challenging aspects in internet and Multimedia applications. Encryption is a process which is used to secure data. The Encryption algorithms and suitable transforms play a crucial role to form efficient security systems. In this regard the original information in the existing security system based on the fractional Fourier transform (FRFT) is protected by only a certain order of FRFT. In this paper, we propose a novel method to encrypt an image by using multiple parameters discrete fractional Fourier transform (DFRFT) with random phase matrices. The multiple-parameter discrete fractional Fourier transform (MPDFRFT) possesses all the desired properties of discrete fractional Fourier transform. The MPDFRFT converts to the DFRFT when all of its order parameters are the same. We exploit the properties of multiple-parameter DFRFT and propose a novel encryption scheme using the double random phase in the MPDFRFT domain for encrypting digital data. The proposed encoding scheme with MPDFRFT significantly enhances the data security compared to DFRFT and FRFT and it shows consistent performance with different images. The scheme offers a high degree of resistance towards bruteforce attack.

General Terms

Image Processing, Security, Encryption, Decryption, Algorithm

Keywords

Discrete Fractional Fourier Transform (DFRFT), Decryption, Encryption, Fourier Transform (FT), Fractional Fourier Transform (FRFT), Multiple Parameter Discrete Fractional Fourier Transform (MPDFRFT).

1. INTRODUCTION

The continuous fractional Fourier transform (FRFT) is 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 shown its potential in the fields of the image processing 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 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 Hermite –Gaussian function type. These eigenvectors are computed from a DFT –commuting matrix proposed in [19] by Dickson and Steigletz. Pei et al. [16], first proposed the eigen decomposition- based definition of the DFRFT 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 enormous attention in recent years due to increasing privacy and authentic document prevention. In the past twenty years, a number of optical encryption methods have been proposed by the various researchers in [6-15] and [23-43]. 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 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. Various optical encryption schemes based on the FRFT have been reported since 2009 [6-15, 23-46].

To increase the security of data robust encryption schemes are required to protect the data from unauthorized user. This criterion may be fulfilled by using more robust transform and applying this transform in a model to achieve more unauthorized user protected scheme for encryption. In proposed scheme robust transform MPDFRFT by adding an additional feature in DFRFT, is used using double random phase matrix with eigen vector decomposition algorithm. The proposed scheme can also 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.

The outline of this paper is as follows: In section. 2 the FRFT and DFRFT, MPDFRFT in briefly discussed with their mathematical definition. The algorithm used with DFRFT and

MPDFRFT elaborated in their sections respectively. In section 3 the proposed encryption, decryption model based on multiple parameters discrete fractional Fourier transform (MPDFRFT) is described with its block diagram and mathematical formulation. In 4th segment of this paper the performance parameters and salient features of the proposed encryption scheme are briefly present. In section 5 the simulation results are shown with their explanation. While section 6 the paper concludes with numerical comparisons and future research directions.

2. PRELIMINARIES

The a-th order FRFT $f_a(x_a)$ of a function $f(x)$ is defined as,

$$f_a(x_a) = F_a\{f(x)\}(x_a) = \int_{-\infty}^{+\infty} K_a(x, x_a) f(x) dx \qquad (1)$$

The kernel is given by,

$$K_a(x, x_a) = \begin{cases} = A_\varphi \exp[i\pi(x^2 \cot\varphi - 2x.x_a + x_a^2 \cot\varphi) & \text{for } 0 < |a| < 2 \\ \delta(x - x_a) & \text{for } a = 0 \\ \delta(x + x_a) & \text{for } a = \pm 2 \end{cases} \qquad (2)$$

Where,

$A_\varphi = \exp[-i\pi \operatorname{sgn}(Sin\varphi)/4 + i_\varphi/2)]$ and here $\varphi = \pi/2$

Here x and x_a represent the coordinate systems for the input or zeroth order domain and output a-th fractional domain.

2.1 Discrete Fractional Fourier Transform

The a −th order $N \times N$ DFRFT is developed based on the eigen decomposition, and its transform kernel is given on the basis of [16-17], [44] is,

$$F^{2\alpha/\pi} = VD^{2\alpha/\pi}V^T \qquad (3)$$

Here $a = 2\alpha/\pi$ the DFRFT order of the parameter.

Where α indicates the rotation angle of DFRFT. $\mathrm{V} = [\mathrm{v}_0|\mathrm{v}_1|........|\mathrm{v}_{\mathrm{N-2}}\|\mathrm{v}_{\mathrm{N-1}}|]$ for N is odd, $\mathrm{V} = [\mathrm{v}_0|\mathrm{v}_1|........|\mathrm{v}_{\mathrm{N-2}}\|\mathrm{v}_{\mathrm{N-1}}|]$for N is even, and v_k is the k-th order DFT hermite eigen vector. $D^{2\alpha/\pi}$ is a diagonal matrix with eigen values of DFRFT in the diagonal entries. The methods for finding the DFT Hermite eigenvectors v_k are presented in [16] and [44]. In Table 1, there exists a jump in the last eigen values for the two even-length cases.

The $N \times N$ DFT matrix F is given by,

$$F_{kn} = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{N}kn} \quad 0 \le k, n \le N - 1 \qquad (4)$$

Therefore, there are some differences in computing the DFRFT kernels between even- and odd-length cases.

Table 1. The Distinct Eigen Values

No.	N	Eigen Values
1.	$4m$	$e^{-jk\alpha}$ $for\ k = 0,1,2 \dots (4m-2), 4m$
2.	$4m+1$	$e^{-jk\alpha}$ $for\ k = 0,1,2 \dots (4m-1), 4m$
3.	$4m+2$	$e^{-jk\alpha}$ $for\ k = 0,1,2 \dots 4m, (4m+2)$
4.	$4m+3$	$e^{-jk\alpha}$ $for\ k = 0,1,2 \dots (4m+1), \{4m+2\}$

For the odd- and even- length cases, (1) can be written as follows:

$$F^{2\alpha/\pi} = \sum_{k=0}^{N-1} e^{-jk\alpha} v_k v_k^T \qquad (5)$$

(for the odd values of N)

$$F^{2\alpha/\pi} = \sum_{k=0}^{N-2} e^{-jk\alpha} v_k v_k^T + e^{-jN\alpha} v_N v_N^T \qquad (6)$$

(For the even values of N)

The DFRFT output is computed as a,

$$X_\alpha = \sum_{k=0}^{N-1} e^{-jk\alpha} v_k v_k^T x \qquad (7)$$

(For the odd values of N)

$$X_\alpha = \sum_{k=0}^{N-2} e^{-jk\alpha} v_k v_k^T x + e^{-jN\alpha} v_N v_N^T x \qquad (8)$$

(For the even values of N)

2.2 MPDFRFT and its Properties

The a −th order DFRFT matrix is $F^{2\alpha/\pi}$ given in eq. (3). The $F^{2\alpha/\pi}$ degenerates to the DFT matrix F in eq. (3), when$a = 1$. So the DFRFT is a generalization of the DFT. If we further generalize the DFRFT on the basis of taking different fractional power for the eigen values $\lambda_k = \exp(-j\pi k/2)$ of the DFT matrix. Subsequently the N point $N \times N$ MPDFRFT matrix given as,

$$F^{\overline{2\alpha/\pi}} = V.diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} ....(e^{-j\frac{\pi}{2}(N-1)})^{a_{N-1}} \right).V^T$$

for the odd values of N (9.1)

$$= V.diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} ......(e^{-j\frac{\pi}{2}(N-2)})^{a_{N-2}} (e^{-j\frac{\pi}{2}(N)})^{a_N} \right).V^T$$

for the even values of N (9.2)

When $diag(u_1, u_2, ..., u_n)$ represents the $N \times N$ diagonal matrix whose diagonal elements are $u_1, u_2, ..., u_n$. In eq. (9), $\bar{a}$ is a $1 \times N$ parameter vector consisting of the N independent order parameters of the MPDFRFT,

$$\bar{a} = \begin{cases} (a_0, a_1, a_2, ..., a_{N-1}) & \text{for N odd} \\ (a_0, a_1, a_2, ..., a_{N-2}, a_N) & \text{for N even} \end{cases} \qquad (10)$$

The diagonal matrix is simplified as

$$D^{\overline{2\alpha/\pi}} = \begin{cases} diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} ....(e^{-j\frac{\pi}{2}(N-1)})^{a_{N-1}} \right) & \text{for N is odd} \\ diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} ......(e^{-j\frac{\pi}{2}(N-2)})^{a_{N-2}} (e^{-j\frac{\pi}{2}(N)})^{a_N} \right) & \text{For N even} \end{cases}$$

(11)

The vector $\bar{a}$ is given in eq.(10) and $D^{\overline{2\alpha/\pi}}$ is the $N \times N$ diagonal matrix of the DFT eigen values,

$$D^{2\alpha/\pi} = \begin{cases} diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1} ....e^{-j\frac{\pi}{2}(N-1)} \right) & \text{for N is odd} \\ diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1} ....e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}(N)} \right) & \text{For N even} \end{cases}$$

(12)

Then eq. (8) can be expressed in summarized form as,

$$F^{\overline{2\alpha/\pi}} = VD^{\overline{2\alpha/\pi}}V^T \qquad (13)$$

The MPDFRFT of $X_{\bar{a}}$ of the $N \times 1$ data vector x with the parameter vector $\bar{a}$ can be given by,

$$X_{\bar{a}} = F^{\overline{2\alpha/\pi}}\mathrm{x} \qquad (14)$$

The main features of the MPDFRFT are discussed as follows.

1. If $\bar{a} = (a, a, \ldots\ldots, a),$ the MPDFRFT is converted into DFRFT so DFRFT is the special condition of the MPDFRFT.
2. The $N-$point MPDFRFT can have up to N independent and possibly different order parameters, Where as DFRFT has only one order parameter.
3. The computation complexity for the MPDFRFT is $O(N^2)$ same as DFRFT.

The MPDFRFT follows all the properties of DFRFT. We conclude that MPDFRFT possess all the properties of DFRFT as mentioned below.

1. Unitarity:

$$\left(F^{\overline{2\alpha/\pi}}\right)^H \left(F^{\overline{2\alpha/\pi}}\right) = \left(VD^{\overline{2\alpha/\pi}}V^T\right)^H \left(VD^{\overline{2\alpha/\pi}}V^T\right)$$
$$= \left(VD^{-\overline{2\alpha/\pi}}V^T\right)\left(VD^{\overline{2\alpha/\pi}}V^T\right)$$
$$= VV^T = I \qquad (15)$$

Where H denotes the conjugate or transposes operation.

2. Identity Matrix:

If $\bar{a} = \bar{0} = (0,0,\ldots,0)$

$$F^{\overline{2\alpha/\pi}} = VD^{\bar{0}}V^T = VV^T = I$$

reduces to an identity operator.

3. Fourier Transform: If the parameter vector,

$$\bar{a} = \bar{1} = (1,1,\ldots,1)$$

$$F^{\overline{2\alpha/\pi}} = VD^{\bar{1}}V^T = VDV^T = F \qquad (16)$$

Here F indicates the fourier transform.

4. Index additivity: if $\bar{a}_1$ and $\bar{a}_2$ are the two parameters of the same size then the MPDFRFT can be given as,

$$\left(F^{\overline{2\alpha_1/\pi}}\right)\left(F^{\overline{2\alpha_2/\pi}}\right) = \left(VD^{\bar{a}_1}V^T\right)\left(VD^{\bar{a}_2}V^T\right)$$
$$= \left(VD^{\bar{a}_1+\bar{a}_2}V^T\right) = F^{\overline{2(\bar{\alpha}_1+\bar{\alpha}_2)/2}} \qquad (17)$$

5. Index Commutativity:

$$\left(F^{\overline{2\alpha_1/\pi}}\right)\left(F^{\overline{2\alpha_2/\pi}}\right) = \left(VD^{\bar{a}_1+\bar{a}_2}V^T\right) = VD^{\bar{a}_2+\bar{a}_1}V^T = \left(F^{\overline{2\alpha_2/\pi}}\right)\left(F^{\overline{2\alpha_1/\pi}}\right) \qquad (18)$$

6. Inverse Transform: The inverse transform of the MPDFRFT of parameter vector $\bar{a}$ can be given as,

$$\left(F^{\overline{2\alpha/\pi}}\right)^{-1} = \left(F^{\overline{-2\alpha/\pi}}\right) \qquad (19)$$

7. Periodicity: The MPDFRFT $F^{\overline{2\alpha/\pi}}$ is periodic in parameter $\bar{a}_k$ with period $4/k$ if k is nonzero and if $F^{\overline{2\alpha/\pi}}$ is the same for different value of $\bar{a}_0$.

$$e^{-j\frac{\pi}{2}k\left(a_k+\frac{4}{k}\right)} = e^{-j\frac{\pi}{2}ka_k}, \qquad (20)$$

if $k \neq 0$ and $\left(e^{-j\frac{\pi}{2}0}\right)^{a_0} = 1$

Here $F^{\overline{2\alpha/\pi}}$ is periodic in $\bar{a}_k$ with the period of 4 for all values of k.

3. PROPOSED MODEL FOR IMAGE ENCRYPTION

On the basis of double random phase fractional Fourier domain encoding introduced by Unnikrishnan and Singh [7], we propose the double random phase encoding in the MPDFRFT domain to encrypt an images. The proposed encryption and decryption models are shown in Figure. 1 and 2 respectively. This encryption scheme significantly improves data security because the order parameters of the 2D-MPDFRFT can be exploited as extra keys for decryption and keeps computational complexity same as in the DFRFT.

For an image "L" of size 256 × 256, the 2D-MPDFRFT of "L" with MPDFRFT parameters vectors $(\bar{P}, \bar{Q})$ is given by

$$L_{(\bar{p},\bar{q})} = F^{\bar{p}}.L.F^{\bar{q}} \qquad (21)$$

Where $F^{\bar{p}}$ and $.F^{\bar{q}}$ are the 256 point MPDFRFT matrices respectively, $\bar{p}$ and $\bar{q}$ are the parameter vectors of sizes 1×256 and 1×256 matrices respectively. Here $e^{j\beta(n,m)}$ and $e^{j\gamma(n,m)}$ indicate the two random matrices having order 256×256. here $\beta(n,m)$ and $\gamma(n,m)$ are having $1 \le n \le 256$ and $1 \le m \le 256$ are uniformly distributed over the interval $[0,2\pi]$. Here $\beta(n,m)$ and $\gamma(n,m)$ are randomly generated matrices so these matrices may or may not be same. Now to deduce the encrypted image "*Y*" we multiply element by element random matrices $e^{j\beta(n,m)}$ with input image "L" then taking its 2D MPDFRFT by the vector parameters $\bar{p}$ and $\bar{q}$ then again performing element by element multiplication with random matrices $e^{j\gamma(n,m)}$ then finally taking 2D MPDFRFT by the vector parameters $\bar{r}$ and $\bar{s}$ to generate an encrypted image "*Y*".

Mathematically it is given as,

$$Y = L \otimes [e^{j\beta(n,m)}] \qquad (22)$$

$$Y = F^{\bar{p}}.\left(L \otimes [e^{j\beta(n,m)}]\right).F^{\bar{q}} \qquad (23)$$

$$Y = \left(F^{\bar{p}}.\left(L \otimes [e^{j\beta(n,m)}]\right).F^{\bar{q}}\right) \otimes \left[e^{j\gamma(n,m)}\right] \qquad (24)$$

$$Y = \left[\left\{F^{\bar{r}}.\left\{\left(F^{\bar{p}}.\left(L \otimes [e^{j\beta(n,m)}]\right)F^{\bar{q}}\right) \otimes \left[e^{j\gamma(n,m)}\right]\right\}\right\}.F^{\bar{s}}\right] \qquad (25)$$

To generate the original image or decrypted image at the receiver side we utilize the reversibility or inverse transform property of the MPDFRFT, mathematically we perform the operation for decrypted image,

$$Y' = \left[\left\{F^{-\bar{r}}.Y.F^{-\bar{s}}\right\} \otimes \left[e^{-j\gamma(n,m)}\right]\right] \qquad (26)$$

$$\hat{L} = \left[F^{-\bar{p}}\left\{F^{-\bar{r}}.Y.F^{-\bar{s}}\right\} \otimes \left[e^{-j\gamma(n,m)}\right]F^{-\bar{q}} \otimes [e^{-j\beta(n,m)}]\right] \qquad (27)$$

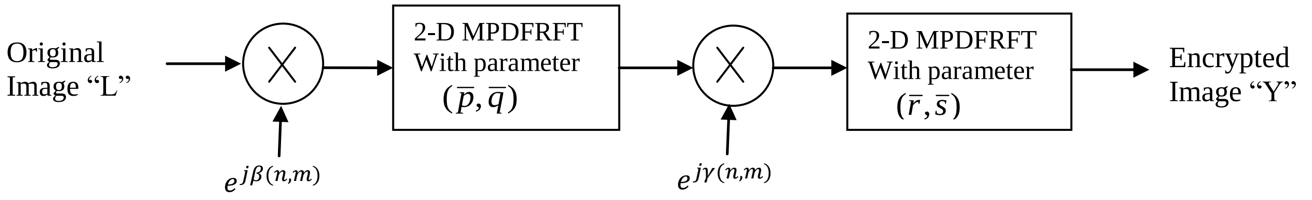

Original Image "L"
2-D MPDFRFT With parameter $(\bar{p},\bar{q})$
2-D MPDFRFT With parameter $(\bar{r},\bar{s})$
Encrypted Image "Y"
$e^{j\beta(n,m)}$
$e^{j\gamma(n,m)}$

Fig 1: Encryption Process using double random phase matrix with MPDFRFT

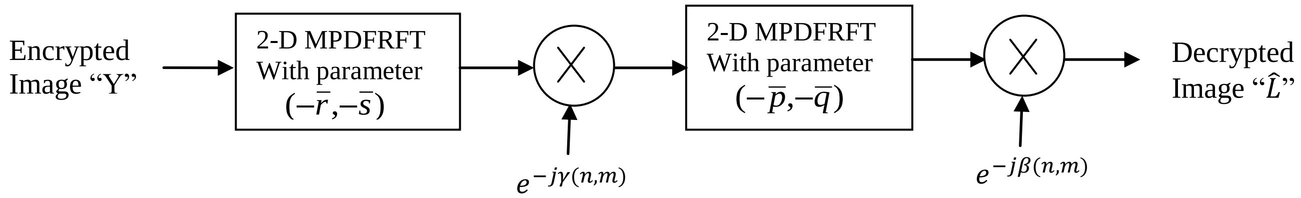

Encrypted Image "Y"
2-D MPDFRFT With parameter $(-\bar{r},-\bar{s})$
2-D MPDFRFT With parameter $(-\bar{p},-\bar{q})$
Decrypted Image "$\hat{L}$"
$e^{-j\gamma(n,m)}$
$e^{-j\beta(n,m)}$

Fig 2: Decryption Process using double random phase matrix with MPDFRFT

The random phase matrices $e^{j\beta(n,m)}$ and $e^{j\gamma(n,m)}$ for encryptions and its conjugate $e^{-j\beta(n,m)}$ and $e^{-j\gamma(n,m)}$ are used at the decryption side. Similarly for the encryption with MPDFRFT parameters vectors $(\bar{p},\bar{q})$ and $(\bar{r},\bar{s})$ are done while for the decryption MPDFRFT parameters vectors with $(-\bar{p},-\bar{q})$ and $(-\bar{r},-\bar{s})$ are used. The $\hat{L}$ represent decrypted image.

4. PERFORMANCE ANALYSIS AND DISCUSSION

1) Salient feature of proposed method

In the proposed method, the original image is first multiplied by random matrices, then taking its 2D MPDFRFT, again multiplied by random matrices and taking its 2D MPDFRFT to enhance the robustness of the encryption. This idea may also be applied with the first interpolating the images into subimages then each subimage can be encrypted by the different order of 2D MPDFRFT and the encrypted image is obtained by summing the two-dimensional 2D IMPDFRFT of the interpolated subimages by using identities of multirate signal processing. Thus, the proposed method can also be applied to double or more image encryptions by regarding the original images as subimages, which is impossible for most of the traditional methods based on the FRFT. The methods based on the random phase coding in the FRFD can also realize the double image encryptions. A random discrete fractional Fourier transform (RDFRFT) kernel matrix with random DFT eigenvectors and eigen values may also apply for security enhance image encryption scheme by taking its magnitude and phase of its transform output are both random as applied by Pei [13] may also be replaced in this model using MPDFRFT based on random DFT eigen values and eigenvectors.

2) Security

In the image decryption, the 2D MPDFRFT and random matrices both are used as the secret keys. The original image is processed by different orders of MPDFRFT and random matrices, it is demonstrated in equation (22) (23) (24) and (25). Now the decryption of the image needs the multiple parameters due to the nonorthogonality among the kernel functions of different orders of MPDFRFT and the inverse of same random matrices generated at the encryption side. The proposed and the existing image encryption based on the FRFT, comparison finds that the proposed method is with a larger key space with different orders, i.e., a higher security. We can also combine the proposed algorithm with the other encryption methods to further enhance the security of the system.

3) Complexity Analysis

In proposed encryption scheme based on the 2D MPDFRFT, uses eigenvector decomposition-type algorithm. This type of the DFRFT lacks fast algorithms. The encryption and the decryption procedures are both realized by the matrix multiplications. For an image with a size of$A \times B$, the computation complexity is same during the encryption and decryption process. Complexity of the proposed encryption scheme is less and equal than the existing methods specially DFRFT based encryption scheme. For the implementation by $M \times N$ times 2D MPDFRFT and 2D IMPDFRFT can be realized by using FFT and inverse FFT (IFFT). Then the complexity of the proposed encryption scheme is given by $MN \cdot (AB/2) \cdot [\log_2 AB + 8]$ complex multiplication. The computation burden of the proposed encryption scheme shows a linear increase with the extension of the multiple parameters.

The image decryption process is processed according to the eq.(27). The computation in decryption consist inversion of the matrices and multiplication with inverse of the 2D MPDFRFT. So the complexity remains same as in the encryption for decryption.

4.) Speed

A good image encryption algorithm should be fast and does encryption in smaller time period. The proposed model used less time. The time taken to simulate the model on Pentium core I-5 processor system on MATLAB R2011a platform takes 1.92sec to deliver a result. While same model for DFRFT instead of MPDFRFT uses 1.55sec. So complexity of MPDFRFT is higher than DFRFT but computation complexity remains same as DFRFT.

5.) Bruteforce Attack

Brute force attack is an attack that unauthorized person tests all possible keys to find the encryption key. When the key space is large enough, brute force attack will not be useful for an unauthorized person. The possible combination for an unauthorized user is N6×1016 for an image having N×N size so the possible combination to get correct image, an unauthorized person have to enter 1560576 entries. This much possible combination is only required to access one key only.

In this scheme possibly four key must be matched at a time to successfully decrypt image. This is not practically possible.

5. SIMULATION RESULTS

In this segment we show the performance of the proposed encryption technique. The performance is evaluated on the basis of the mean square error (MSE) between the original image and the decrypted image,

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

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 grayscale input image of “Lena” with a size of 256 × 256, as shown in Fig. 3(a), is serving as the original image which is to be encrypted. Fig. 3(c) shows the encrypted image “Y” using the double random phase encoding in the MPDFRFT domain, where the elements of the 1×256 encryption parameter vectors $\overline{p},\overline{q}$ and $\overline{r},\overline{s}$ are independent and randomly chosen from the interval [0, 2]. if the correct parameter vectors for decryption is used decrypted output is generated as shown in Fig. 3(d), which is almost same as the original image. The quality measure between original and decrypted image is measure by mean square error. If the incorrect key or wrong parameter vector is utilized to decrypt the image is retrieved as shown in fig. 3(e). If the key and parameter vectors are marginally deviated from its original key the decryption is failed. The results shown in fig. 4 are shows the robustness and effectiveness of the system towards change in the input image. The system also provides almost same MSE as received in the case of Lena Image than photographer image. The fig. 5 shows the sensitivity of system in order with deviation in original key with respect to the normalized MSE and it shows that the system is sensitive by the deviation from -0.005 to + 0.005. The deviation is independent of the parameter and uniformly distributed over the interval. Fig. 5 also plots the normalized MSEs of the decrypted images for the double random phase encoding in the DFRFT domain, Experiment results show that the double random phase encoding in the MPDFRFT domain is much more sensitive to the decryption parameter error than that in the DFRFT domain.

It concludes that a small deviation from its original secret key will result in the large errors between encrypted and decrypted image. The encrypted image can be perfectly decrypted if and only if the 2D MPDFRFT parameters are all perfectly matched. It should also be noted that if the size of the image increase the dealing with the sensitivity of the fractional orders increases considerably and the MSE of incorrectly decrypted images also increases considerably.

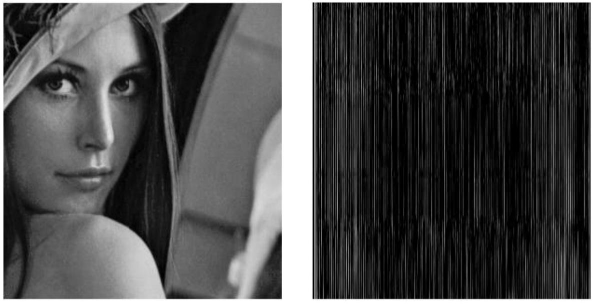
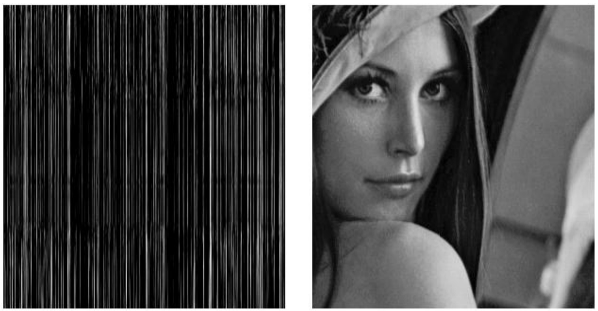
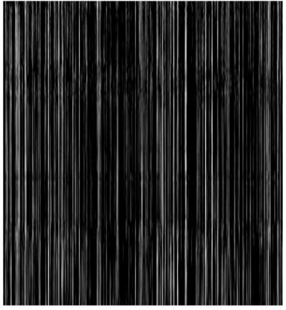


Fig.3 (a) Original Image (b) Image encrypted at 1st stage



(c) Image Encrypted at 2nd stage (d) Decrypted Image



(e) Decrypted Lenna Image with incorrect parameter

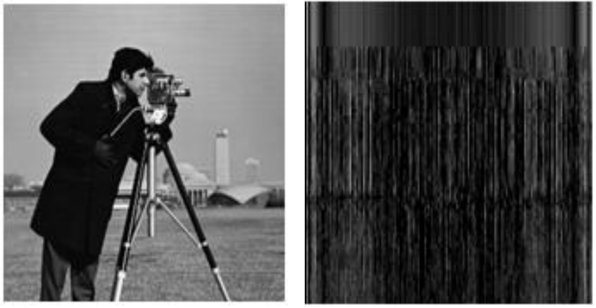
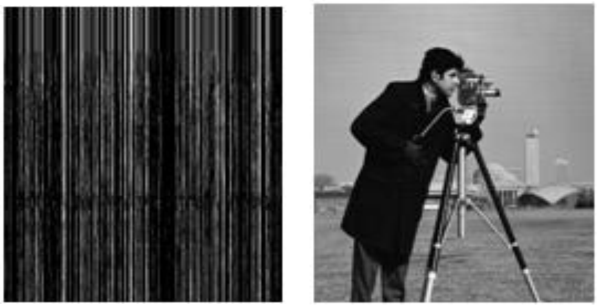
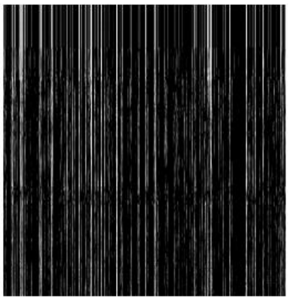


Fig.4 (a) Original Image (b) Encrypted Image at 1st level



(c) Image Encrypted at 2nd level (d) Decrypted Image with correct key



(e) Decrypted Cameraman Image with incorrect key

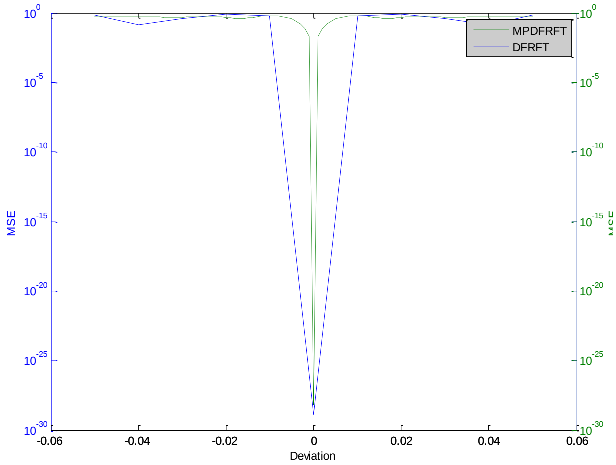


Fig 5: Normalized MSE by varying the original key in MPDFRFT and DFRFT domain.

Table 2. Mean Square Error (MSE) for Lena and Cameraman Images

MSE **Image**	**Min. MSE**	**Max. MSE**	**Average MSE**
Leena	6.8256×10^{-13}	1.0275×10^{-12}	8.5431×10^{-13}
Cameraman	1.1816×10^{-13}	1.6073×10^{-12}	9.1226×10^{-13}

Table 3. Time for algorithm execution

Image/Time	**Avg. time taken using MPDFRFT**	**Avg. time taken using DFRFT**
Proposed with Lena Image	1.92 Sec.	1.52 Sec.
Proposed with Cameramen Image	1.9 Sec.	1.48 Sec.
Pei and Hsue (2009) [13]	3.3455 Sec.	----
Mohammad & Shahriar (2012) [45]	2.8986 Sec.	-----

6. CONCLUSION

In this article, a new image encryption model is proposed on the basis of 2D-MPDFRFT with eigen decomposition based DFRFT by taking different fractional powers for different eigen values. The MPDFRFT is much more flexible than the DFRFT because it has multi order parameters. The proposed model utilizes the double random phase encoding in the MPDFRFT domain to encrypt digital images. This new encryption method significantly enhances data security, because the order parameters of the MPDFRFT can be exploited as extra keys for decryption comparative to DFRFT. The min MSE between the original and correctly decrypted image is 6.8256×10^{-13} and 1.1816×10^{-13} for Lena and cameraman images respectively. The computation complexity based on MPDFRFT remains same as of the DFRFT. The brutforce attack requires 1560576 min attempt to crack the original key. The time taken to execute an algorithm is reasonable than other algorithm executed by pei [13] and Shahriar [45].

7. ACKNOWLEDGEMENT

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

8. 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) 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) 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, 767-769, (1995).

[24] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng. 36, 992–998 (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, 762-764 (1999).

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

[28] Y. Zhang, C.H. Zheng, N. Tanno, “Optical encryption based on iterative fractional Fourier transform,” Opt. Commun. 202, 277-285, (2002).

[29] B. Zhu and S. Liu, “Optical Image encryption based on the generalized fractional convolution operation,” Opt. Commun. 195, 371-381, (2001).

[30] B. Zhu and S. Liu, “Optical Image encryption with multistage and multichannel fractional Fourier-domain filtering,” Opt. Lett. 26, 1242-1244, (2001).

[31] N. K. Nishchal, J. Joseph, and K. Singh, “Fully phase encryption using fractional Fourier transform,” Opt. Eng. 42, 1583–1588 (2003).

[32] B. Hennelly and J. T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” Opt. Lett. 28, 269-271 (2003).

[33] N. K. Nishchal, G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption using a localized fractional Fourier transform,” Opt. Eng. 42, 3566-3571, (2003).

[34] N. K. Nishchal, J. Joseph, and K. Singh, “Fully phase-based encryption using fractional order Fourier domain random phase encoding: Error analysis,” Opt. Eng. 43, 2266-2273 (2004).

[35] J. Zhao, H. Lu, X.S. Song, J.F. Li, and Y.H. Ma, “Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique,” Opt. Commun. 249, 493-499, (2005).

[36] A. Sinha, K. Singh, “Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes,” Opt. Eng. 44, 057001 (2005).

[37] G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” Opt. Lett. 30, 1306-1308 (2005).

[38] X. F. Meng, L. Z. Cai, M. Z. He, and G. Y. Dong and X. X. Shen, “Cross-talk-free double-image encryption and watermarking with amplitude-phase separate modulations” , J. Opt. A: Pure Appl. Opt. 7, 624 (2005).

[39] L. F. Chen and D. M. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” Opt. Exp. 14, 8552-8560 (2006),

[40] X. Wang, D. Zhao, F. Jing, and X. Wei, “Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics” Opt. Exp. 14, 1476-1486 (2006).

[41] M. S. Millán, E. Pérez-Cabré, and B. Javidi, “Multifactor authentication reinforces optical security,” Opt.Lett. 31, 721-723 (2006).

[42] G. Situ and J. Zhang, “Position multiplexing for multiple-image encryption,” J. Opt. A: Pure Appl. Opt. 8, 391 (2006).

[43] Z. Liu and S. Liu, “Double image encryption based on iterative fractional Fourier transform,” Opt. Commun. 275, 324–329 (2007).

[44] S. C. Pei, M. H. Yeh, and C. C. Tseng, “Discrete fractional Fourier transform based on orthogonal projections,” IEEE Trans. Signal Processing, vol. 47, pp. 1335–1348, May 1999.

[45] Mohammad Monajem and Shahriar Baradaran Shokouhi “A new method of image encryption with multiple-parameter discrete fractional Fourier transform” 2012 International Conference on Information and Computer Networks (ICICN 2012)IPCSIT vol. 27 (2012) (2011) IACSIT Press, Singapore

Deepak Sharma, born in 1981 Ambah, Madhya Pradesh, obtained his M. Tech. (Microwave Engineering) from Madhav Institute of Technology and Science in 2006. Currently working as an Assistant Professor in Jaypee University of Engineering and Technology (JUET), Guna Before joining JUET, he worked as a Lecturer in Electronics Department, MITS, Gwalior (M.P). presently Pursuing Ph. D. degree from Jaypee University of Engineering and

Technology, Guna under the guidance of Dr. Rajiv Saxena. His Research areas include Antenna Theory, Radar System, Signal processing, Image processing and Integral Transforms.

Rajiv Saxena, born at Gwalior in Madhya Pradesh in 1961, obtained B.E. (Electronics & Telecommunication Engineering) in the year 1982 from Jabalpur University, Jabalpur. Subsequently, Dr. Saxena joined the Reliance Industries, Ahmedabad, as Graduate Trainee. In 1984, Dr. Saxena joined Madhav Institute of Technology & Science, Gwalior as Lecturer in Electronics Engineering. He obtained his M.E. (Digital Techniques & Data Processing) from Jiwaji University, Gwalior in 1990. The Ph. D. degree was conferred on him in 1996-97 in Electronics & Computer Engineering from IIT, Roorkee (erstwhile UOR, Roorkee). Currently Dr. Saxena is head and professor in ECE department at JUET, Guna.