I.J. Computer Network and Information Security, **2014, 10, 1-12**
Published Online September 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.10.01

Hybrid Encryption-Compression Scheme Based on Multiple Parameter Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm

Deepak Sharma
Jaypee University of Engineering and Technology, Electronics and Communication Engineering Department, Guna, India
Email: deepakforu23@rediffmail.com

Rajiv Saxena and Narendra Singh
Jaypee University of Engineering and Technology, Electronics and Communication Engineering Department, Guna, India
Email: {rajiv.saxena, narendra.singh}@juet.ac.in

Abstract—Encryption along with compression is the process used to secure any multimedia content processing with minimum data storage and transmission. The transforms plays vital role for optimizing any encryption-compression systems. Earlier 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 article, a novel method for encryption-compression scheme based on multiple parameters of discrete fractional Fourier transform (DFRFT) with random phase matrices is proposed. 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-compression scheme using the double random phase in the MPDFRFT domain for encryption and compression data. The proposed scheme with MPDFRFT significantly enhances the data security along with image quality of decompressed image compared to DFRFT and FRFT and it shows consistent performance with different images. The numerical simulations demonstrate the validity and efficiency of this scheme based on Peak signal to noise ratio (PSNR), Compression ratio (CR) and the robustness of the schemes against bruit force attack is examined.

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

I. Introduction

The concept of FRFT was first introduced by N. Wiener in 1929, in quantum mechanics, the FRFT was recognized as a 'transform method' by mathematical bodies after the work of Victor Namias in 1980 [1] in which the concept of FRFT had introduced by considering fractional power of eigen functions of the ordinary FT. The FRFT of a signal can develop from the original function to its FT by varying transform order gradually from 0 to 1 [2, 3, 4]. The FRFT has shown its tremendous role in image processing as an application for encryption, compression and watermarking. The significant feature of fractional Fourier transform and cosine domain image compression benefits from its extra degree of freedom that is provided by their fractional orders [5]. The FRFT based encryption systems reveals higher security by varying transform order to enlarge the key space [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16].

Due to extensive use of internet and hostile attack encryption of data has become more demanding for the protection of data resources especially on the Internet, intranets and extranets by the users. The another challenge in multimedia applications is to transport data from one end to another end such as text, images and media contents such as audio and video with limited bandwidth and enormous data size. Now the data sizes has been increased due to high quality (HD) multimedia contents so the demand of higher bandwidth for data transmission and memory size increased a lot. It becomes necessary to apply compression algorithms on bulky data along with secure transmission with faster processing of

Manuscript received March 31, 2014; revised June 11, 2014; accepted June 22, 2014.

Copyright © 2014 MECS

data. The encryption compression scheme provides suitable solution for such type of emerging problems. Compression and encryption technologies are important to the efficient solving of network bandwidth and security issues.

The discrete fractional Fourier transform (DFRFT) was defined by Pei and Ozaktas is a generalization of the DFT with additional free parameters [17, 18, 19]. In [17] 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 [17] are Hermite – Gaussian function type. These eigenvectors are computed from a DFT –commuting matrix proposed in [20] by Dickson and Steigletz. Pei et al.in [17], first proposed the eigen decomposition- based definition of the DFRFT and then Candan et al. consolidated this definition [18]. Hanna et al. considered generation eigenvectors by the singular value decomposition method and direct batch evaluation [21, 22, 23].

In the past few years, numerous optical encryption methods have been proposed by the researchers in [24-44]. Among them, the most widely used and highly successful optical encryption scheme is double random phase encoding proposed by Refregier and Javidi [24]. 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 [7, 8, 28] first proposed an optical encryption method using random phase encoding in the fractional Fourier domain and its optically-implemented approach. There is various lossy and lossless compression approaches also discussed in literature by researcher in [45, 46, 47, 48, 49, 50, 51] using different transform like wavelet, discrete cosine transform, Fractional cosine transform and FRFT etc.

To increase the security of data with lesser space requirement can be achieve by applying suitable robust transform for protection of data from 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 and compression. Here more robust transform MPDFRFT is used by adding an additional feature in DFRFT, which also possess all the desirable properties of the DFRFT. The goal of our work is to propose a novel scheme based on multiple parameter discrete fractional Fourier transform for both encryption and compression.

The outline of this paper is as follows: In section II we discuss the FRFT, DFRFT and MPDFRFT briefly their mathematical definition, properties and the algorithm used with DFRFT and MPDFRFT. In III segment of this article the MPDFRFT based proposed encryption-compression and decompression-decryption model with random phase masking is developed. Its mathematical formulation is developed for proposed scheme. In section IV the performance analysis and salient features of the proposed encryption-compression scheme are discussed in detail. In section V the simulation results and its performance measuring parameters are evaluated in comparative manner. In section VI the article is concluded on the basis of performance measuring parameters and their merits, demerits of the scheme along with its future research directions.

II. FRFT, DFRFT AND MPDFRFT DEFINITION'S

The a -th order FRFT $f_a(x_a)$ of a function $f(x)$ is defined as [6],

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

The kernel is given by,

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

Where,

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

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

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 [17, 18, 52] is,

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

Here $a = 2\alpha/\pi$ the DFRFT order of the parameter and α indicates the rotation angle of DFRFT.

$$V = \left[v_0 \left| v_1 \right| ..... \left| v_{N-2} \right| \left| v_{N-1} \right| \right] \quad \text{for } N \text{ is odd,} \qquad (3.1)$$

$$V = \left[v_0 \left| v_1 \right| ..... \left| v_{N-2} \right| \left| v_{N-1} \right| \right] \quad \text{for N is even} \qquad (3.2)$$

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 [17] and [52]. Table 1, shows the last eigen values for the two even-length cases.

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

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

Table 1. The Distinct Eigen Values

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

Therefore, there are some differences in computing the DFRFT kernels between even- and odd-length cases. For the odd- and even- length cases, equation (1) can be written as follows,

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

(For the odd values of *N*)

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

(For the even values of *N*)

The DFRFT output is computed as a,

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

(For the odd values of *N*)

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

(For the even values of *N*)

The a -th order DFRFT matrix is $F^{2\alpha/\pi}$ given in equation (3). We know that $F^{2\alpha/\pi}$ degenerates to the DFT matrix F in equation (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 is,

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 equation (8), $\bar{a}$ is a $1 \times N$ parameter vector consisting of the N independent order parameters of the MPDFRFT,

$$\bar{a} = \begin{cases} (a_0, a_1, a_2, ..., a_{N-1}) & \text{for N odd} \\ (a_0, a_1, a_2, ..., a_{N-2}, a_N) & \text{for N even} \end{cases} \tag{9}$$

The diagonal matrix is simplified as

$$D^{\overline{2\alpha/\pi}} = \begin{cases} diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} .....(e^{-j\frac{\pi}{2}(N-1)})^{a_{N-1}} \right) & \text{for N is odd} \\ diag\left((e^{-j\frac{\pi}{2}0})^{a_0}, (e^{-j\frac{\pi}{2}1})^{a_1} .....(e^{-j\frac{\pi}{2}(N-2)})^{a_{N-2}} (e^{-j\frac{\pi}{2}(N)})^{a_N} \right) & \text{For N even} \end{cases} \tag{10}$$

The vector $\bar{a}$ is given in equation (9) and $D^{\overline{2\alpha/\pi}}$ is the $N \times N$ diagonal matrix of the DFT Eigen values

$$D^{2\alpha/\pi} = \begin{cases} diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1} .....e^{-j\frac{\pi}{2}(N-1)} \right) & \text{for N is odd} \\ diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1} .....e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}(N)} \right) & \text{For N even} \end{cases} \tag{11}$$

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

$$F^{\overline{2\alpha/\pi}} = V D^{\overline{2\alpha/\pi}} V^T \tag{12}$$

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

$$X_{\bar{a}} = F^{\overline{2\alpha/\pi}} x \tag{13}$$

The main features of the MPDFRFT are discussed as follows.

1. If $\bar{a} = (a, a, ..., a)$, 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, Whereas, 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:

$$\begin{aligned} \left(F^{\overline{2\alpha/\pi}}\right)^H \left(F^{\overline{2\alpha/\pi}}\right) &= \left(V D^{\overline{2\alpha/\pi}} V^T\right)^H \left(V D^{\overline{2\alpha/\pi}} V^T\right) \\ &= \left(V D^{-\overline{2\alpha/\pi}} V^T\right)\left(V D^{\overline{2\alpha/\pi}} V^T\right) \\ &= V V^T = I \end{aligned} \tag{14}$$

Where H denotes the conjugate or transposes operation.

Copyright © 2014 MECS

2. Identity Matrix:

   If $\bar{a}=\bar{0}=(0,0,...,0), F^{\overline{2\alpha/\pi}}=VD^{\bar{0}}V^{T}=VV^{T}=I$

   reduces to an identity operator.

3. Fourier Transform: If the parameter vector ,

$$\bar{a}=\bar{1}=(1,1,...,1), F^{\overline{2\alpha/\pi}}=VD^{\bar{1}}V^{T}=VDV^{T}=F \quad (15)$$

   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,

$$\left(F^{\overline{2\alpha_1/\pi}}\right)\left(F^{\overline{2\alpha_2/\pi}}\right)=\left(VD^{\bar{a}_1}V^{T}\right)\left(VD^{\bar{a}_2}V^{T}\right)$$
$$=\left(VD^{\bar{a}_1+\bar{a}_2}V^{T}\right)=F^{\overline{2(\bar{\alpha}_1+\bar{\alpha}_2)/2}} \quad (16)$$

5. Index Commutativity:

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

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

$$\left(F^{\overline{2\alpha/\pi}}\right)^{-1}=\left(F^{\overline{-2\alpha/\pi}}\right) \quad (18)$$

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 $\bar{a}_0$.

$$e^{-j\frac{\pi}{2}k\left(a_k+\frac{4}{k}\right)}=e^{-j\frac{\pi}{2}ka_k}, \quad (19)$$

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 .

III. The Proposed Model For Image Encryption-Compression Scheme

In this section we introduce our proposed encryption compression scheme fairly used for transmission and reception side. The concept of encryption scheme is based on 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 while compression concept is lie on transform coding based. The proposed encryption compression and decryption decompression models are shown in Figure 1 and Figure 2 respectively. This encryption method significantly improves data security because the extra order parameter of the 2D-MPDFRFT can be exploited as extra keys for decryption and keeps computational complexity same as in the DFRFT. The transform coding based compression scheme is mainly divided in three major steps block division, linear transform and bit allocation. Here in linear transforming multiple parameter discrete fractional Fourier transform is applied.

For an original image of size 256×256 , is first multiplied by random phase matrices $e^{j\beta(n,m)}$ here $\beta(n,m)$ having $1\le n\le 256$ and $1\le m\le 256$ are uniformly distributed over the interval $[0,2\pi]$. Matrix $e^{j\beta(n,m)}$ is randomly generated matrices so this matrix may or may not be same for two different instances. Now the image is converted into subimages of size 8×8 to reduce interpixel redundancy a large sub image size will lead less pixel correlation and becomes insignificant when the distance of pixels exceeds.

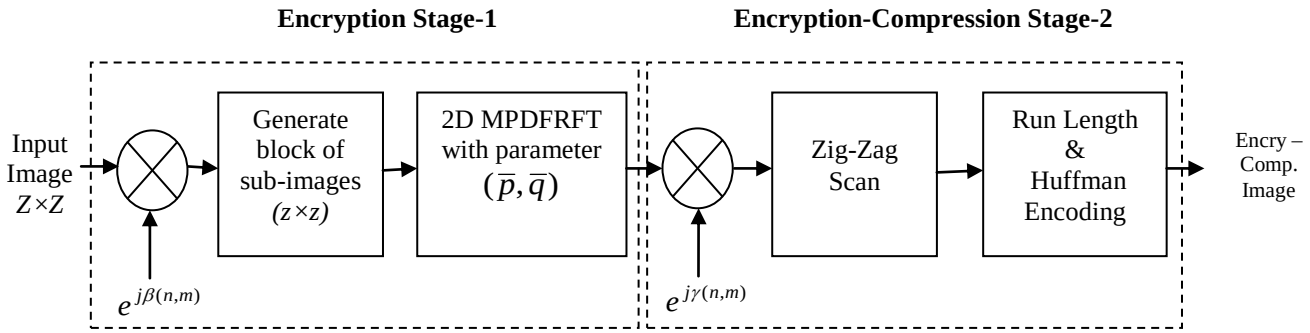


Fig 1. Encryption-Compression using double random phase matrix based on MPDFRFT

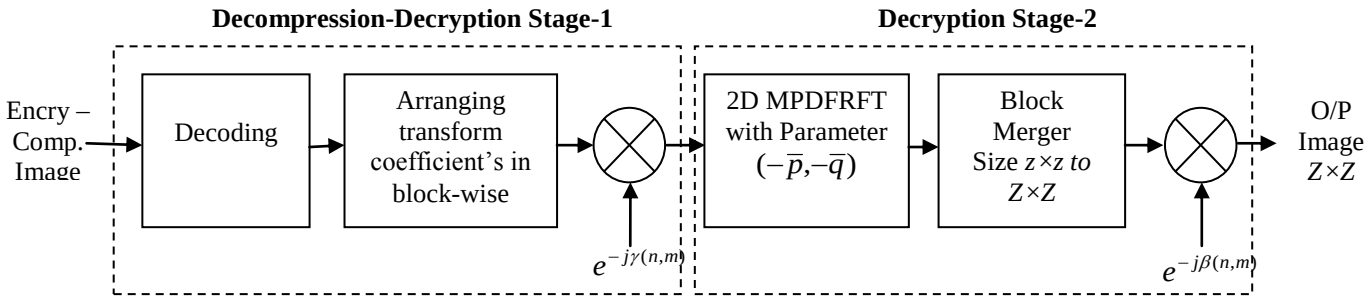


Fig 2. Decompression-Decryption using double random phase matrix based on MPDFRFT

On the other hand, a large size is not suitable for adaptation to local statistics, while adaptation is required in handling nonstationary images. For these reasons, sub image size should not be large. Then the for each sub image size 8×8 the 2D MPDFRFT is applied by the vector parameters $\bar{p}$ and $\bar{q}$ and 1st stage encrypted image can be generated. In second stage mathematical operations is performed that again $e^{j\gamma(n,m)}$ randomly generated matrices is multiplied using element by element multiplication but here $\gamma(n,m)$ is confined in the domain of $1\le n\le 8$ and $1\le m\le 8$ uniformly distributed over the interval $[0,2\pi]$. Mathematically it can be represented as,

$$\mathbf{Y}=\mathbf{L}_{Z\times Z}\otimes[\mathrm{e}^{\mathrm{j}\beta(\mathrm{n,m})}] \tag{20}$$

$$\mathbf{Y}=\mathbf{F}_{z\times z}^{\bar{p}}.\left(\mathbf{L}_{Z\times Z}\otimes[\mathrm{e}^{\mathrm{j}\beta(\mathrm{n,m})}]\right).\mathbf{F}_{z\times z}^{\bar{q}} \tag{21}$$

$$\mathbf{Y}=\mathbf{F}_{z\times z}^{\bar{p}}.\left(\mathbf{L}_{Z\times Z}\otimes[\mathrm{e}^{\mathrm{j}\beta(\mathrm{n,m})}]\right).\mathbf{F}_{z\times z}^{\bar{q}}\otimes\left[\mathrm{e}^{\mathrm{j}\gamma(\mathrm{n,m})}\right] \tag{22}$$

The zigzag scan operation is applied on 2D MPDFRFT transformed coefficients that convert the 2-D array of transform coefficients into a 1-D sequence. The number of consecutive zero-valued coefficients in the 1-D sequence is referred to as the run-length of zeros and is used to provide address information of nonzero transformed coefficients. The application of the Huffman coding to the magnitude of nonzero transform coefficients and run-lengths of zeros has been applied. Finally the encrypted and compressed image is achieved at the output of transmitting end.

Here the analysis is done for both gray scale and color mode based on RGB space. A color image based on RGB space is the composition of R, G, and B components and each component can be seen as a gray image. The RGB space is a color display space not suitable for human visual features so here it is processed in terms of YCbCr color mode, the Y component denotes the intensity, and the Cr and Cb components respectively denote the color differences between the red and blue. The conversion from RGB to YCbCr color space is formulated as,

$$\begin{bmatrix}\mathrm{Y}\\ \mathrm{Cb}\\ \mathrm{Cr}\end{bmatrix}=\begin{bmatrix}0.299 & 0.587 & 0.144\\ -0.16875 & -0.33126 & 0.5\\ 0.5 & -0.41869 & -0.08131\end{bmatrix}\begin{bmatrix}\mathrm{R}\\ \mathrm{G}\\ \mathrm{B}\end{bmatrix} \tag{23}$$

The inverse transformation from YCbCr to RGB can be applied as,

$$\begin{bmatrix}\mathrm{R}\\ \mathrm{G}\\ \mathrm{B}\end{bmatrix}=\begin{bmatrix}1 & 0 & 1.402\\ 1 & -0.3313 & -0.71414\\ 1 & 1.772 & 0\end{bmatrix}\begin{bmatrix}\mathrm{Y}\\ \mathrm{Cb}\\ \mathrm{Cr}\end{bmatrix} \tag{24}$$

To retrieve the original image from proposed decompression –decryption system applicable at receiver side follows the reverse operation applied at the transmitter. At receiver side the major operations performed as decoding, transform coefficient rearrangement, 2D MPDFRFT with reverse order vector parameters $-\bar{p}$ and $-\bar{q}$ and finally sub image merging for converting original image respectively. The random phase matrices $e^{-j\beta(n,m)}$ and $e^{-j\gamma(n,m)}$ indicate the same complex conjugate matrices utilized at the transmitter side in a similar fashion.

Mathematically the process of decoded and decryption operation can be summarized as,

$$\mathbf{Y}'=\left[\mathbf{Y}\otimes\left(\mathrm{e}^{-\mathrm{j}\gamma(\mathrm{n,m})}\right)\right] \tag{25}$$

$$\mathbf{Y}'=\left[\mathbf{F}_{z\times z}^{-\bar{p}}.\left\{\mathbf{Y}\otimes\left(\mathrm{e}^{-\mathrm{j}\gamma(\mathrm{n,m})}\right)\right\}\mathbf{F}_{z\times z}^{-\bar{q}}\right] \tag{26}$$

$$\mathbf{Y}'=\left[\mathbf{F}_{z\times z}^{-\bar{p}}.\left\{\mathbf{Y}\otimes\left(\mathrm{e}^{-\mathrm{j}\gamma(\mathrm{n,m})}\right)\right\}\mathbf{F}_{z\times z}^{-\bar{q}}\right]\otimes\left(\mathrm{e}^{-\mathrm{j}\beta(\mathrm{n,m})}\right) \tag{27}$$

Here Y represent the encrypted compressed image at transmitter output, while Y' at final stage is original decrypted decompressed image at receiver.

Copyright © 2014 MECS

IV. Performance Analysis And Discussion of Proposed Scheme

A. Salient Feature of Proposed Scheme

In the proposed scheme, 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 encrypted data. 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 multi-rate signal processing. Thus, the proposed scheme may also applied with double or more image encryptions by considering the original images as subimages, which is impossible for most of the traditional methods based on the FRFT [10], [12, 13, 14, 15]. The methods based on the random phase coding in the FRFD can also realize the double image encryptions [11]. 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 [14] may also be replaced in this model using MPDFRFT based on random DFT Eigen values and eigenvectors.

B. Security

For 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 already indicated from equation (20)-(22), equation (25)-(26) and equation (27) that the original image cannot be retrieved without applying correct fractional order and similar random phase matrices for the operation utilized at transmitter side for decompression-decryption of an image. 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.

C. Computation Complexity

In the existing encryption methods based on the 2D MPDFRFT, the eigenvector decomposition-type algorithm is used. 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 complexity of the encryption and the decryption is about equal. Complexity of the proposed decryption scheme is less and equal than the existing methods especially for DFRFT based encryption scheme because the computation cost of DFRFT and MPDFRFT is same. For the implementation by $M \times N$ times 2D MPDFRFT it can be realized by using FFT and inverse FFT (IFFT) algorithm for fast computation. 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-decompression process is processed according to the equation (26). The computation in decryption-decompression consist inversion of the matrices and multiplication with reverse order of the 2D MPDFRFT so the complexity remains same during encryption-compression and decompression-decryption process.

D. Computation Time

A good image encryption-compression algorithm should be fast and does encryption in a short time. 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 3.2 sec to deliver a result. While same model for DFRFT instead of MPDFRFT uses 2.7 second because of higher complexity involved in for the calculation of MPDFRFT. The MPDFRFT based system consume little higher time than the system based on solely DFRFT.

E. Bruteforce attack

Brute force attack is an attack that unauthorized person tests all possible keys to find the encryption key or in other words it consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space. When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. When the key space is large enough, brute force attack will not be easier for an unauthorized person. The resources required for a brute-force attack grow exponentially with increasing key size, not linearly. The possible combination for an unauthorized user is Z6×1016 for an image having $Z \times Z$ size so the possible combination to get correct image, an unauthorized person have to enter 4681728 entries. This much possible combination is only required to access one key only. In this scheme possibly three key must be matched at a time to successfully decrypt image i.e. all random phase matrix along with the correct order of MPDFRFT should be matched for correct image decryption which is not practically possible.

Copyright © 2014 MECS

V. Simulation Results and Performance Analysis

A. Simulation results

This section shows the performance of the proposed encryption-compression scheme on the basis of the mean square error (MSE), Peak Signal to noise ratio (PSNR), compression ratio (CR), sensitivity of system towards original key and time taken by the algorithm to execute proposed scheme.

1. Mean Square Error (MSE): mean square error is the measure of dissimilarity between the decompressed-decrypted image and the original one.

An input image L of size $A \times B$ and its recovered decompressed-decrypted image approximation is $\hat{L}$, Then *MSE* can be calculated as,

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

Where A and B indicated the size of the image while $L(i, j)$ and $\hat{L}(i, j)$ indicates the original and decompressed decrypted image of pixel (i, j) respectively.

2. Peak Signal to Noise Ratio (PSNR): PSNR is most commonly used to measure the quality of reconstruction of lossy compression. The input image is the original data, and the noise is the error introduced during compression. PSNR is most easily defined via the mean squared error (*MSE*).

The PSNR is defined as,

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{\mathrm{Max}_{\mathrm{I}}^2}{\mathrm{MSE}} \right)$$

Here, MAX_I is the maximum possible pixel value of the image.

For a color image, the PSNR is calculated as,

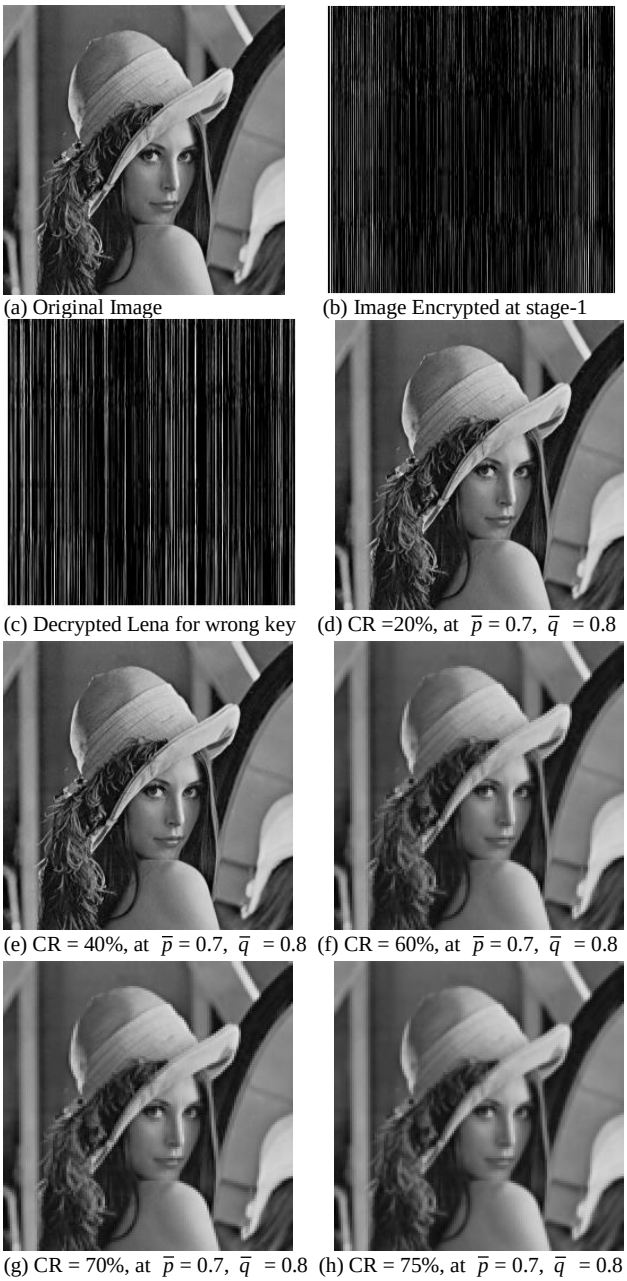
$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{255 \times 255 \times 3}{\mathrm{MSE(R)} + \mathrm{MSE(G)} + \mathrm{MSE(B)}} \right)$$

3. Compression ratio (CR): It is defined as the ratio between the uncompressed size and compressed size of data.

$$\text{Compression Ratio} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}}$$

Similarly, the space savings is defined as the reduction in size relative to the uncompressed size

$$\text{Space Saving} = 1 - \frac{\text{Compressed Size}}{\text{Uncompressed Size}}$$



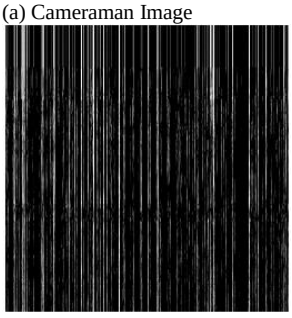
(a) Original Image (b) Image Encrypted at stage-1
(c) Decrypted Lena for wrong key (d) CR =20%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8
(e) CR = 40%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (f) CR = 60%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8
(g) CR = 70%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (h) CR = 75%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

Fig 3.

We use the random phase matrices $e^{j\beta(n,m)}$ and $e^{j\gamma(n,m)}$ for encryption-compression transmission side and its conjugate $e^{-j\beta(n,m)}$ and $e^{-j\gamma(n,m)}$ are used at the decompression-decryption receiver side. Similarly for the encryption-compression MPDFRFT parameters vectors $(\bar{p}, \bar{q})$ used and for decompression-decryption MPDFRFT parameter vectors with reverse order $(-\bar{p}, -\bar{q})$ are used in the range of 0 to 4. Figure 3(a) shows the original Lena image which has to encrypt and compress figure 3(b) is encrypted image at stage 1 before compression and figure 3(c) represent the decompressed-decrypted image at incorrect key parameter.

(a) Cameraman Image

(b) Image at Encryption stage-1


(c) Decrypted C'man for wrong key

(d) CR =20%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(e) CR = 40%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(f) CR = 60%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(g) CR = 70%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(h) CR = 75%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

Fig 4.

Figure 3(d), (e), (f), (g) and (h) shows the results of decompressed-decrypted image at compression ratio at 20, 40, 60, 70 and 75 percent respectively at fractional order $\bar{p}$ = 0.7 and $\bar{q}$ = 0.88 for optimum results. Similar analysis is done for using cameraman image for testing the authenticity of a proposed system. Figure 4(a) shows the original Cameraman image which has to encrypt and compress figure 4(b) is encrypted image at stage 1 before compression and figure 3(c) represent the decompressed-decrypted image at incorrect key parameter. Figure 4 (d), (e), (f), (g) and (h) shows the results of decompressed-decrypted image at compression ratio at 20, 40, 60, 70 and 75 percent respectively at fractional order $\bar{p}$ = 0.7and $\bar{q}$ = 0.8 for optimum results.

The figure 5 shows variation of compression ratio with respect to PSNR keeping MPDFRFT parameter fixed at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 for most best result.

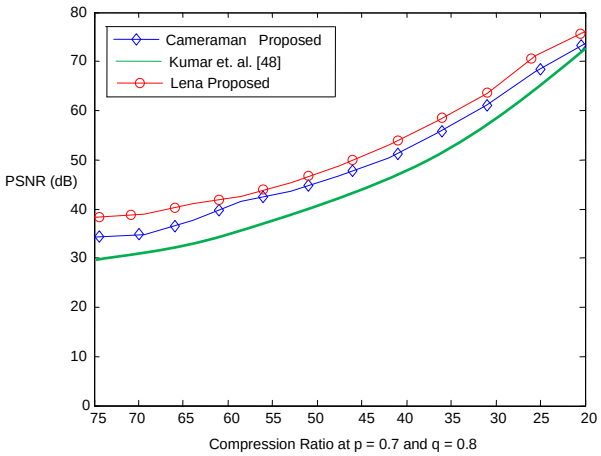
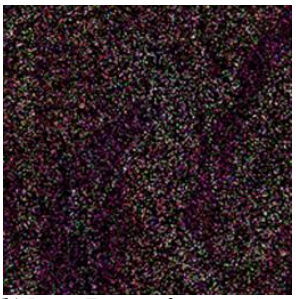
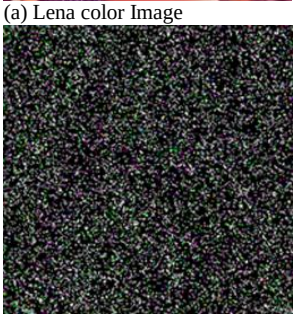


Fig 5. PSNR versus Compression ratio at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

The similar proposed scheme is also tested for Color images using Lena, Baboon and Satellite image using equation (23)-(24). The results are measures at MPDFRFT parameter fixed at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 for optimum results.

(a) Lena color Image


(b) Image Encrypted at stage-1


(c) Decrypted Lena for wrong key

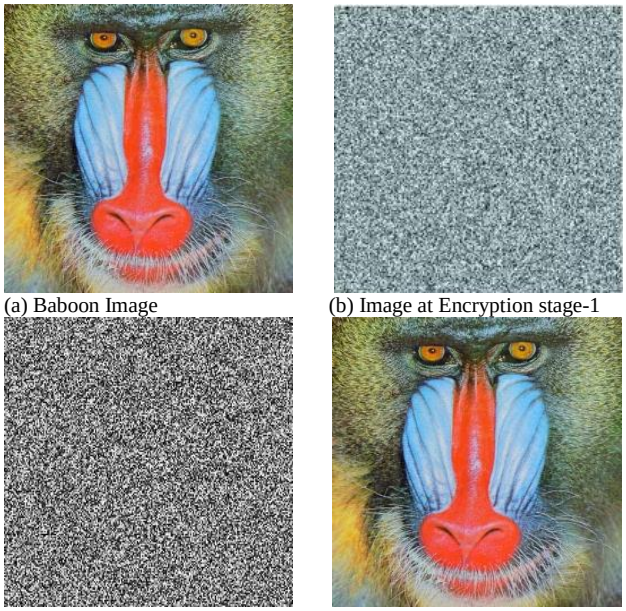
(d) CR =20%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(e) CR = 40%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(f) CR = 50%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(g) CR = 60%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (h) CR = 70%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

Fig 6.



(a) Baboon Image (b) Image at Encryption stage-1

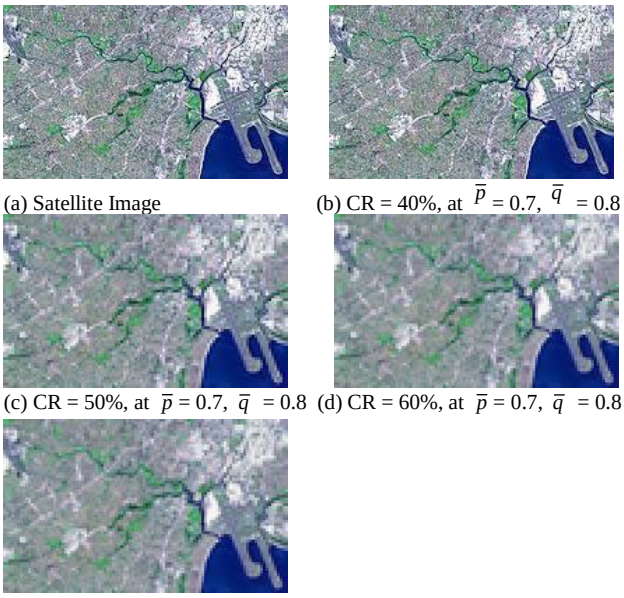
(c) Decrypted Baboon at wrong key (d) CR =20%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(e) CR = 40%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (f) CR = 50%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(g) CR = 60%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (h) CR = 70%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

Fig 7.

The results in figure 8 are shown for HD satellite image here the encrypted image is not shown only compression results are shown in summarized manner for compression ratio 40, 50, 60 and 70 percent respectively. All results are deduced for the 2D MPDFRFT parameter at fractional order $\bar{p}$ = 0.7and $\bar{q}$ = 0.88.



(a) Satellite Image (b) CR = 40%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(c) CR = 50%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8 (d) CR = 60%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

(e) CR = 70%, at $\bar{p}$ = 0.7, $\bar{q}$ = 0.8

Fig 8.

Figure 9 shows the variation of PSNR versus CR for color image of Lena, baboon and satellite. In figure below the SPNR for Lena and baboon shows similar kind of nature towards the proposed scheme when ever for satellite image the nature of proposed scheme is slightly deviate.

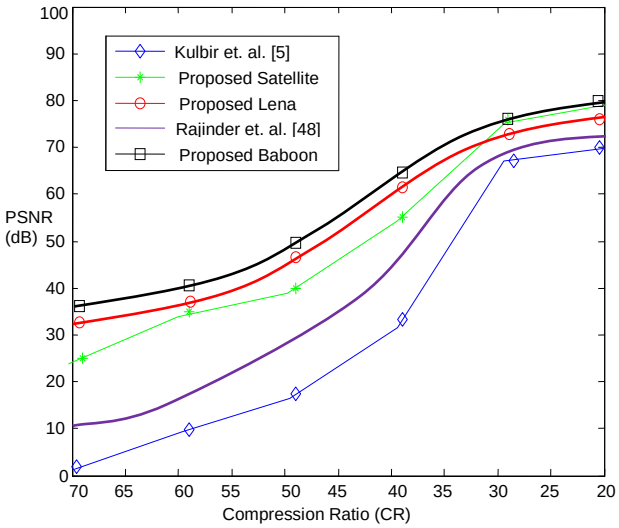


Fig 9. PSNR versus compression ratio for color images

Figure 10 shows the sensitivity of MPDFRFT and DFRFT versus normalized MSE. The figure10 reveals that the sensitivity of MPDFRFT is much higher than the sensitivity of DFRFT. The sensitivity towards original key is less than 0.01 in case of MPDFRFT while in case of DFRFT it is more than .02 for very fractional deviation in very short interval. This clearly reveals that 2D PDFRFT is a more robust and sensitive towards its

original key.

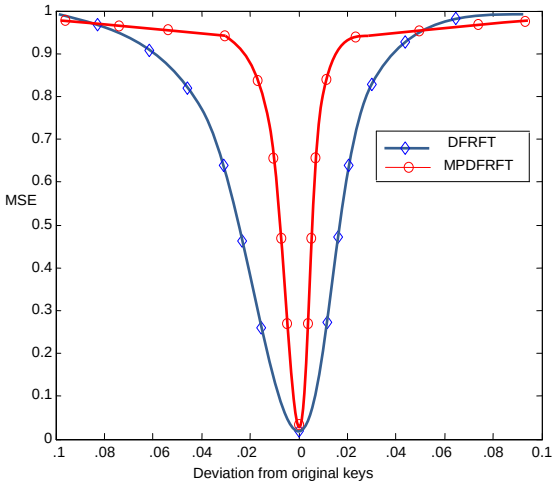


Fig 10. Sensitivity of key towards variation of key versus MSE

The concluded results are summarized in comparative manner table 2.

Table 2. PSNR of various images at different values of CR

Images and Schemes	Peak Signal to Noise ratio (PSNR)	Compression Ratio (CR)	Computation complexity
Proposed Leena Gray	76.4 dB	20	$O(N)^2$
	50.8 dB	40	
	42.3 dB	60	
	39.8 dB	70	
	39.1 dB	75	
Proposed Cameraman Gray	74.1 dB	20	$O(N)^2$
	48.6 dB	40	
	38.9 dB	60	
	34.8 dB	70	
	33.9 dB	75	
Rajinder et.al. [48] for gray	73.8 dB	20	$O(N)^2$
	43.8 dB	40	
	33.3 dB	60	
	31.2 dB	70	
	30.0 dB	75	
Proposed Lena Color	68.1 dB	20	$O(N)^2$
	55.8 dB	40	
	41.3 dB	50	
	35.1 dB	60	
	31.8 dB	70	
Proposed Baboon Color	80.0 dB	20	$O(N)^2$
	60.7 dB	40	
	49.3 dB	50	
	41.2 dB	60	
	36.1 dB	70	
Rajinder et.al. [48] for color	69.9 dB	20	$O(N)^2$
	34.4 dB	40	
	24.3 dB	50	
	14.8 dB	60	
	10.2 dB	70	
Kulbir et.al. [5] for color	68.1 dB	20	$O(N)^2$
	26.4 dB	40	
	12.2 dB	50	
	8.6 dB	60	
	1.5 dB	70	
Proposed Satellite Image	79.8 dB	20	$O(N)^2$
	49.4 dB	40	
	36.8 dB	50	
	32.8 dB	60	
	23.2 dB	70	

The table 3 produces the time taken to execute the algorithm the other compared algorithm is based on either encryption scheme or compression scheme solely while proposed scheme incorporate both encryption and compression simultaneously.

Table 3. Time taken for algorithm execution

Image/Time	Avg. time taken using MPDFRFT (for 1000 sample)	Avg. time taken using DFRFT (for 1000 sample)
Proposed with Gray Lena Image	3.2 Sec.	2.7 Sec.
Proposed with Gray Cameramen Image	3.1 Sec.	2.5 Sec.
Pei and Hsue (2009) [14]	3.34 Sec.	----
Mohammad and Shahriar (2012) [53]	2.89 Sec.	-----
Rajinder et.al. [48]	--	2.4 sec.
Kulbir et.al. [5]	--	2.6 sec.
Proposed Lena color Image	3.7 Sec.	2.9 Sec.
Proposed Baboon color Image	3.5 Sec.	2.8 Sec.
Proposed Satellite color Image	3.8 Sec.	3.1 Sec.

The proposed scheme shows better time taken to execute algorithm than Pei and Hue while if this algorithm computes for solely encryption find also better suited for Mohammad and Shahriar (2012) [53] also while both encryption and compression technique implementation it consume slight more time than Mohammad and Shahriar [13].

VI. Conclusions

The proposed scheme provides a two way options for data encryption and compression as well. The scheme shows a significant improvement in PSNR value for Lena, cameraman, baboon and satellite images maximum PSNR is achieved 76.4, 74.1, 80 and 79.8dB respectively for lower value of CR at 20% while the PSNR is achieved 39.8, 34.8, 36.1 and 23.2 dB respectively for higher value of CR at 70%. Now from encryption point of view the scheme shows high order resistance towards bruitforce attack. The scheme offers salient features in terms of time required for algorithm execution than already existed encryption scheme based on MPDFRFT. The scheme also offers a high degree of sensitivity towards the original key figure 10 shows that the MSE error increase as the unauthorized person move away from original key by more than 0.01 of its value. The computational complexity of scheme based on MPDFRFT remains same as scheme based on DFRFT. Finally the scheme offers high degree of robust encryption along with high CR with well quality of decompressed decrypted image.

Copyright © 2014 MECS

REFERENCES

[1] V. Namias. The fractional order Fourier transform and its application to quantum mechanics. In Journal of the Institute of Mathematics and Its Applications, March 1980. 25 (3): p. 241–265.

[2] L. B. Almeida. The fractional Fourier transform and time-frequency representations. In IEEE Trans. Signal Processing, November 1994. 42(11): p. 3084–3091.

[3] D. Mustard. The fractional Fourier transform and the Wigner distribution. In Journal of the Australian Mathematical Society series-B, 1996. 38: p. 209–219.

[4] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay. *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. New York: Wiley, 2000.

[5] Kulbir Singh, Navdeep Singh, Parvinder Kaur and Rajiv Saxena. Image Compression By Using Fractional Transforms. In International Conference on Advances in Recent Technologies in Communication and Computing 2009. p. 411-413.

[6] R. Tao, B. Deng, and Y. Wang. Research progress of the fractional Fourier transform in signal processing. In Science in China (Ser.F, Information Science), January 2006. 49: p. 1–25.

[7] G. Unnikrishnan and K. Singh. Double random fractional Fourier-domain encoding for optical security. In Optical. Eng. journal, 2000. 39: p. 2853–2859.

[8] G. Unnikrishnan, J. Joseph, and K. Singh. Optical encryption by double random phase encoding in the fractional Fourier domain. In opt. Letter, 2000. 25(12): p. 887–889.

[9] B. Zhu, S. Liu, and Q. Ran. Optical image encryption based on multifractional Fourier transforms. In Opt. Letter 2000. 25: p.1159–1161

[10] B. M. Hennelly and J. T. Sheridan. Image encryption based on the fractional Fourier transform. In Proc. SPIE, 2003. 5202: p.76–87.

[11] R. Tao, Y. Xin, and Y. Wang. Double image encryption based on random phase encoding in the fractional Fourier domain. In Opt. Express, 2004. 15(24): p. 16067–16079.

[12] R. Tao, X. M. Li, and Y.Wang, "Generalization of the fractional Hilbert transform," IEEE Signal Process. Lett., vol. 15, pp. 365–368, 2008.

[13] B. Hennelly and J. T. Sheridan. Optical image encryption by random shifting in fractional Fourier domains. In Opt. Letter, 2003. 28: p. 269–271.

[14] S. C. Pei and W. L. Hsue. Random discrete fractional Fourier transform. In IEEE Signal Process. Letter, December 2009. 16(12): p. 1015–1018.

[15] L. J. Yan and J. S. Pan. Generalized discrete fractional Hadamard transformation and its application on the image encryption. In Proceeding of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007. p. 457–460.

[16] H. Al-Qaheri, A. Mustafi, and S. Banerjee. Digital watermarking using ant colony optimization in fractional Fourier domain. In Journal of Information Hiding Multimedia Signal Processing, July 2010. 1(3): p. 179–189.

[17] S. C. Pei and M. H. Yeh. Improved discrete fractional Fourier transform. In Opt. Letter, 1997. 22: p. 1047–1049.

[18] C. Candan, M. A. Kutay and H. M. Ozaktas. The discrete fractional Fourier transform. In IEEE Transaction Signal Processing, May 2000. 48(5): p. 1329–1337.

[19] 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.

[20] B. W. Dickinson and K. Steiglitz. Eigenvectors and functions of the discrete Fourier transform. In IEEE Trans. Acoustic, Speech, Signal Processing, January 1982. ASSP-30 (1): p. 25–31.

[21] 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. In IEEE Transaction on Circuits and Systems, November 2004. 51(11): p. 2245–2254.

[22] M. T. Hanna. Direct batch evaluation of optimal orthonormal eigenvectors of the DFT matrix. In IEEE Transaction on Signal Processing, May 2008. 56(5): p. 2138–2143.

[23] 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. In IEEE Transaction on Signal Processing, July 2006. 54(7): p. 2815–2819.

[24] P. Refregier and B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding. In Opt. Letter, 1995. 20: p. 767-769.

[25] B. Javidi, A. Sergent, G. Zhang, and L. Guibert. Fault tolerance properties of a double phase encoding encryption technique. In Opt. Eng., April 1997. 36(4): p. 992–998.

[26] N. Towghi, B. Javidi, and Z. Luo. Fully phase encrypted image processor. In The Journal of the Optical Society of America-A, 1999. 16 (8): p.1915-1927.

[27] O. Matoba and B. Javidi. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. In Optics Letters, 1999. 24(11): p.762-764.

[28] G. Unnikrishnan and K. Singh. Optical encryption using quadratic phase systems. In Elsevier Optics Communications, June 2001. 193(1-6): p.51-67.

[29] Y. Zhang, C. H. Zheng and N. Tanno. Optical encryption based on iterative fractional Fourier transform. In Elsevier Optics Communications, Feburary 2002. 202 (4-6): p. 277-285.

[30] B. Zhu and S. Liu. Optical Image encryption based on the generalized fractional convolution operation In Elsevier Optics Communications, August 2001. 195 (5-6): p.371-381.

[31] B. Zhu and S. Liu. Optical Image encryption with multistage and multichannel fractional Fourier-domain filtering. In Optics Letters, 2001. 26(16): p.1242-1244.

[32] N. K. Nishchal, J. Joseph, and K. Singh. Fully phase encryption using fractional Fourier transform. In Optical Engineering, June 2003. 42(6): p.1583–1588.

[33] B. Hennelly and J. T. Sheridan. Optical image encryption by random shifting in fractional Fourier domains. In Optics Letters, 2003. 28(4): p. 269-271.

[34] N. K. Nishchal, G. Unnikrishnan, J. Joseph, and K. Singh. Optical encryption using a localized fractional Fourier transform. In Optical Engineering, January 2003. 42(12): p. 3566-3571.

[35] N. K. Nishchal, J. Joseph, and K. Singh. Fully phase-based encryption using fractional order Fourier domain random phase encoding: Error analysis. In Optical Engineering, January 2004.43 (10): p. 2266-2273.

[36] 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. In Optics Communications, May 2005. 249 (4-6): p.493-499.

[37] A. Sinha and K. Singh. Image encryption by using fractional Fourier transform and jigsaw transform in image

bit planes. In Optical Engineering, May 2005. 44(5): 057001.
[38] G. Situ and J. Zhang. Multiple-image encryption by wavelength multiplexing. In Optics Letters, 2005. 30(11): p. 1306-1308.
[39] 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. In Journal of Optics A: Pure and Applied Optics, October 2005. 7(11): p. 624.
[40] L. F. Chen and D. M. Zhao. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. In Optics Express, 2006. 14(19): p. 8552-8560.
[41] X. Wang, D. Zhao, F. Jing and X. Wei. Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics. In Optics Express, February 2006. 14(4): p.1476-1486.
[42] M. S. Millán, E. Perez-Cabre and B. Javidi, "Multifactor authentication reinforces optical security," In Optics Letters, March 2006. 31(6): p.721-723.
[43] G. Situ and J. Zhang. Position multiplexing for multiple-image encryption. In Journal of Optics A: Pure and Applied Optics, 2006. 8(5): p. 391.
[44] Z. Liu and S. Liu. Double image encryption based on iterative fractional Fourier transform. In Elsevier Optics Communications, July 2007. 275(2): p.324-329.
[45] H. Cheng and X. Li. Partial encryption of compressed images and videos. In IEEE Transactions on Signal Processing, August 2000. 48(8): p. 2439-2451.
[46] C. Vijaya and J. S. Bhat. Signal compression using discrete fractional Fourier transform and set partitioning in hierarchical tree. In Elsevier Signal Processing, August 2006. 86(8): p.1976–1983.
[47] K. Nagamani and A. G. Ananth. Image Compression Techniques for High Resolution Satellite Imageries using Classical Lifting Scheme. In International Journal of Computer Applications, February 2011. 15(3): p. 25-28.
[48] Rajinder Kumar, Kulbir Singh and Rajesh Khanna Satellite Image Compression using Fractional Fourier Transform. In International Journal of Computer Applications, July 2012. Volume 50 (3): p. 20-25.
[49] E. Celikel and M. E. Dalkilic. Experiments on a secure compression algorithm. In Proceedings of the International Conference on Information Technology: Coding and Computing, April 2004. 2: p.150-152.
[50] Bryan Usevitch. A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000. In IEEE Signal Processing Magazine, September 2001. p. 22-35.
[51] A. S. Lewis and G. Knowles. Image Compression Using the 2-D Wavelet Transform. In IEEE Transaction on Image Processing, April 1992. 1(2): p. 244-250.
[52] S. C. Pei, M. H. Yeh, and C. C. Tseng. Discrete fractional Fourier transform based on orthogonal projections. In IEEE Transaction on Signal Processing, May 1999. 47(5): p. 1335–1348.
[53] Mohammad Monajem and Shahriar Baradaran Shokouhi. A new method of image encryption with multiple-parameter discrete fractional Fourier transform. In International Conference on Information and Computer Networks (ICICN 2012), Singapore. Vol. 27, IACSIT Press

Deepak Sharma, Obtained his M. Tech. (Microwave Engineering) from Madhav Institute of Technology and Science (MITS), Gwalior (M.P.) 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, he is pursuing his Ph.D. degree from Jaypee University of Engineering and Technology, Guna under the guidance of Prof. Rajiv Saxena and Dr. N. Singh.

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). Dr. Saxena was former head and professor at Jaypee University, Guna (M.P.) for seven year. Currently Dr. Saxena is Director at Jaypee University, Anupshahar (U.P.).

Narendra Singh, born at Orai in Uttar Pradesh in 1977, obtained B. Tech. (Electronics & Instrumentation Engineering) in the year 2001 from Bundelkhand University, Jhansi, M. Tech. in Digital Systems in the year 2004 from M.N.N.I.T. Allahabad (Deemed University) and obtained PhD from Jaypee University of Engineering & Technology, Guna, (M.P.) in the year 2012. Narendra Singh joined JIET, Guna, as lecturer in Electronics and Communication Engineering in 2004. Currently he is assistant professor (senior grade) in ECE department at JUET, Guna.

How to cite this paper: Deepak Sharma, Rajiv Saxena, Narendra Singh,"Hybrid Encryption-Compression Scheme Based on Multiple Parameter Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm", IJCNIS, vol.6, no.10, pp.1-12, 2014. DOI: 10.5815/ijcnis.2014.10.01