Journal of ELECTRICAL ENGINEERING, VOL. 64, NO. 4, 2013, 250–255

IMAGE RETRIEVAL ALGORITHM BASED ON DISCRETE FRACTIONAL TRANSFORMS

Neeru Jindal — Kulbir Singh *

The discrete fractional transforms is a signal processing tool which suggests computational algorithms and solutions to various sophisticated applications. In this paper, a new technique to retrieve the encrypted and scrambled image based on discrete fractional transforms has been proposed. Two-dimensional image was encrypted using discrete fractional transforms with three fractional orders and two random phase masks placed in the two intermediate planes. The significant feature of discrete fractional transforms benefits from its extra degree of freedom that is provided by its fractional orders. Security strength was enhanced $(1024!)^4$ times by scrambling the encrypted image. In decryption process, image retrieval is sensitive for both correct fractional order keys and scrambling algorithm. The proposed approach make the brute force attack infeasible. Mean square error and relative error are the recital parameters to verify validity of proposed method.

K e y w o r d s: discrete fractional transforms, image retrieval, mean square error, relative error, security

1 INTRODUCTION

Secure image retrieval is facing challenges with the brisk development of networked multimedia techniques. In the past decade, several algorithms and architectures [1]-[6] for image security have been suggested. The most widely used and highly successful methods are based on fractional transforms [7]-[8]. The fractional Fourier transform (FrFT) (generalization of the conventional Fourier transform) has shown its potential in the field of image processing and optics communication. Discrete fractional transforms approached in continuation with the dawn of computers and enhanced computations [9]. The one dimensional applications include filtering using window functions, optimal filtering of faded signal, beam forming for the mobile antenna etc. The performance of discrete fractional transforms in two-dimensional applications is anticipated in the present paper.

Image scrambling can be used in pre-process or post-process of digital image processing, information hiding etc. The image scrambling literature include methods based on Arnold transform, Gray code [10], FAN transform [11], Random shuffling strategy [12], Fibonacci numbers [13], Cat chaotic mapping [14], AES and error correcting code [15] etc. These methods were exhausted in time when scrambled. The queue scrambling transformation based on geometry transform also uses module operation [17] and conquers the time limit.

This paper is organized as follow: Section 2 reviews concept of discrete fractional transforms. The principle of scrambling is in section 3. Section 4 present algorithm and computer simulations, and at last section 5 gives a conclusion.

2 DISCRETE FRACTIONAL TRANSFORMS (THEORETICAL ANALYSIS)

The whole of an entity going into fractions of it represents main theoretical rise. The fourth power of 3 may be defined as $3^4 = 3 \times 3 \times 3 \times 3$, but it is not obvious from this definition that how $3^{3.5}$ might be defined. It must have taken sometime before the common definition $3^{3.5} = 3^{7/2} = \sqrt{3^7}$ emerged. The first and second derivative of the function $f(x)$ is commonly denoted by $df(x)/dx$ and $\frac{d^2 f(x)}{dx} = \frac{d}{dx}\left[\frac{df(x)}{dx}\right] = \frac{d[df(x)/dx]}{dx} = \left(\frac{d}{dx}\right)^2 f(x)$ respectively. Similarly higher order derivatives are defined. The 2.5-th derivative of a function is not defined from here. Let $F(\mu)$ denote the FT of $f(x)$. The FT of the n-th derivative of $f(x)$ *ie* $\frac{d^n f(x)}{dx^n}$ is known to be given by $(j2\pi\mu)^n F(\mu)$ for any positive integer n. Now let us generalize this property by replacing n with the real order a and take it as the a-th derivative of $f(x)$. Thus to find $\frac{d^a f(x)}{dx^a}$, the a-th derivative of $f(x)$, find the inverse Fourier transform of $(j2\pi\mu)^a F(\mu)$. Both of these examples are dealing with the fractions of an operation performed on an entity, rather than fractions of the entity itself. $4^{0.5}$ is the square root of the integer 4. The function $[f(x)]^{0.5}$ is the square root of the function $f(x)$. But $\frac{d^{0.5} f(x)}{dx^{0.5}}$ is the 0.5-th derivative of $f(x)$, with $\left(\frac{df(x)}{dx}\right)^{0.5}$ being the square root of the derivative operator $\frac{d}{dx}$.

The process of going from the whole of an entity to fractions of it underlies several of the more important conceptual developments. For example the fuzzy logic, where the binary 1 and 0 are replaced by continuous values representing certainty or uncertainty of a proposition. The fractional Fourier transform (FrFT) was introduced in 1980 by Victor Namias [19] and it was established in the same year that the other transforms could also be fractionalized. Its improvement and mathematical defi-

Department of ECE, Thapar University, Patiala - 147004, Punjab, India, neeru.jindal@thapar.edu

DOI: 10.2478/jee-2013-0036, Print ISSN 1335-3632, On-line ISSN 1339-309X, © 2013 FEI STU

nition was explored by McBride and Keer in 1987 [20]. Furthermore, a general definition of FrFT for all classes of signals (one dimensional and multidimensional, continuous and discrete, periodic and non-periodic) was given by Cariolario *et al* .

2.1 Discrete Fractional Fourier Transform

The discrete domain of FrFT is called discrete fractional Fourier transform (DFrFT) [22]-[23]. Santhanam and McClellan first reported the work on DFrFT in 1995. The transformation kernel of DFrFT can be easily defined by determining the fractional powers of the eigen values. The transform kernel of the DFrFT can be calculated as $D_\alpha = F^{2\alpha/\pi} = VD^{2\alpha/\pi}V^T$, where α indicates the rotation angle of the DFrFT. $V = [v_0\,|v_1\,|\cdots|v_{N-2}\,|v_{N-1}\,]$ for odd N, $V = [v_0\,|v_1\,|\cdots|v_{N-2}\,|v_N\,]$ for even N and v_k is the k-th order DFT Hermite eigenvector $D^{2\alpha/\pi}$ is the diagonal matrix with eigenvalues of DFrFT as the diagonal entries. A method for finding the DFT Hermite eigenvectors v_k is presented and transform kernel can be written as: $D_\alpha = \sum_{k=0}^{N-1} e^{-jk\alpha} v_k v_k^T, forN = 4m+1, 4m+3$. The DFrFT of a signal $x(m)$ can be computed with transformation kernel through equation $D_\alpha x = F^{2\alpha/\pi}x = VD^{2\alpha/\pi}V^T x$. To compute inverse DFrFT (IDFrFT), DFrFT is calculated with inverse order $-\alpha$: $x = F^{-2\alpha/\pi}D_\alpha = VD^{-2\alpha/\pi}V^T D_\alpha$.

For 2D DFrFT, two individual angles of rotation α and β in two dimensions are taken and can be implemented by row-column computation in case of 2D separable kernel. Then the forward and inverse 2D DFrFT for (m,n), and (p,q) point are defined with separable form as: $D_{(\alpha,\beta)}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} x(p,q)\,D_{(\alpha,\beta)}(p,q,m,n)$ and $x(p,q) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} D_{(\alpha,\beta)}(m,n)\,D_{(-\alpha,-\beta)}(p,q,m,n)$.

This 2D DFrFT also keep the preferred properties of continuous 2D FrFT. In the present paper, applications of DFrFT in two dimensions will be explored in image retrieval.

2.2 Discrete Fractional Cosine Transform

The DFrCT share many useful properties of the regular DCT, and it has a free parameter, its fraction. When the fraction is zero, we get the cosine modulated version of the input signal [24]. When it is unity, we get the conventional DCT. The DCT of a sequence $\{x[n], 0 \leqslant n \leqslant N-1\}$ is defined by

$$X(k) = \alpha(k)\sum_{n=0}^{N-1} x[n]\cos\left[\frac{(2n+1)\pi k}{2N}\right], 0 \leqslant k \leqslant N-1 \tag{1}$$

where

$$\alpha(k) = \begin{cases} \frac{1}{\sqrt{N}} for k = 0 \\ \sqrt{\frac{2}{N}} for 1 \leqslant k \leqslant N-1 \end{cases}$$

The elements of one dimensional DCT kernel matrix are given as

$$E_{DCT}(k,n) = \begin{cases} \frac{1}{\sqrt{N}}, k = 0; 0 \leqslant n \leqslant N-1 \\ \sqrt{\frac{2}{N}}\cos\left[\frac{(2n+1)\pi k}{2N}\right]; \\ 1 \leqslant k \leqslant N-1; 0 \leqslant n \leqslant N-1 \end{cases} \tag{2}$$

Because the sequence is orthogonal, the inverse DCT (IDCT) can be recovered by

$$x[n] = \sum_{k=0}^{N-1} \alpha(k)X(k)\cos\left[\frac{(2n+1)\pi k}{2N}\right], 0 \leqslant n \leqslant N-1 \tag{3}$$

Similar to DFrFT, the N point DFrCT kernel can be identified as: C^α=HG.D$^{2\alpha}/\pi HG^T$. Performance of discrete fractional transforms for one dimensional and two dimensional applications is given in [9]. The n-stage of discrete fractional transforms can provide n-dimensional extra keys indicated by the fractional orders. In case of two-dimensional discrete fractional transforms, there are two different fractional orders along x-axis and y-axis respectively. Such a system can have $n-1$ random phase filters, so that the total encryption keys can be increased to as many as $3n-1$. Thus the security strength of the encryption keys may be greatly enhanced.

The a order along x and y direction are taken to be same *ie* $\alpha_x = \alpha_y = \alpha$ and three stages of DFrCT are cascaded together. Thus in the intermediate planes two randomly encoded phase masks are used. Algorithm consists of two parts, encryption to encrypt the image and decryption to retrieve the image.

Let $f(m_0, n_0)$, be a real valued two dimensional data, denote the image we want to encrypt. The image is discrete fractional Fourier cosine transformed three times using fractional orders α_1, α_2 and α_3 respectively. In the intermediate stages we put two random phase mask (RPM),

$$\Re_1(m_1, n_1) = \exp[-j2\pi\phi_1(m_1, n_1)]$$

$$\Re_2(m_2, n_2) = \exp[-j2\pi\phi_2(m_2, n_2)]$$

respectively serving as phase filters.

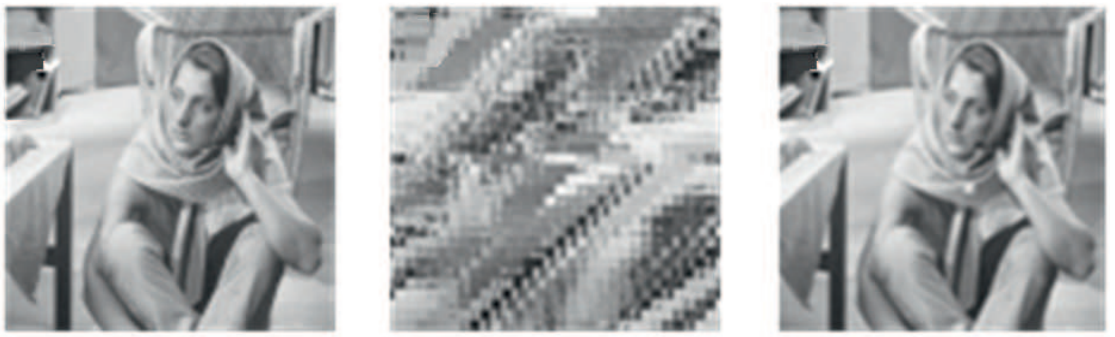
The functions $\phi_1(m_1,n_1)$ and $\phi_2(m_2, n_2)$ are randomly generated homogeneously distributed functions with values (0,1). Thus the resultant transformed function $\psi(m,n)$ can be written as

$$\psi(m,n) = F_c^{\alpha 3}(\psi_2(m_2,n_2)\Re(m_2,n_2)$$

$$\psi_2(m_2,n_2) = F_c^{\alpha 2}\{\psi_1(m_1,n_1)\Re(m_1,n_1)\}$$

and

$$\psi_1(m_1,n_1) = F_c^{\alpha 1}\{f(m_0,n_0)\}.$$



(a) (b) (c)

Fig. 1. The scrambling-descrambling queue: (a) – original image, (b) – scrambled, and (c) – descrambled

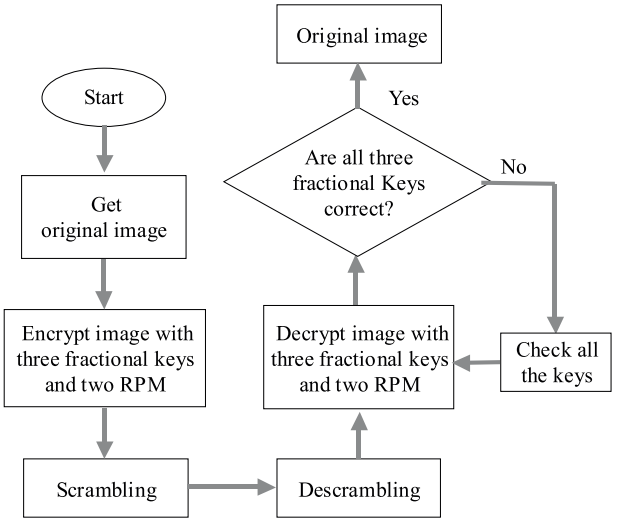


Fig. 2. Flow Chart of proposed Algorithm

The final resultant $\psi(m,n)$ function can be regarded as the encrypted image.

The decryption process *ie* inverse DFrCT (IDFrCT) is the turnaround operation with respect to the encryption with inverse fractional orders and conjugate RPMs [18].

3 SCRAMBLING

Scrambling is encryption of image when unauthorized user can not acquire any information about the original image. The digital image matrix P consists of rows and columns assumed as queues. In simulation, the original image is divided into subsections of $n \times n$ pixels (n=2, 4, 8, 16) in row queue, which are repositioned relative to one another and scrambled image is achieved. After one row queue scrambling transform element of every row comes from different row [16].

The principle of scrambling is depicted in Fig. 1. Simulation results on various images house, boat, baboon, pentagon, Barbara of 256×256 are deliberated. The results Barbara image 256×256 are shown in Fig. 1(a). The divided 1024 subsections of 8×8 pixels are repositioned relative to one another according to reference point (2,3) and row queue transform [16]. Scrambled image, after some random shuffling in pixels is achieved in Fig. 1(b). Perceptibly, descrambled or original image is final result as in Fig. 1(c) by applying all divergent operations.

3.1 Image Retrieval Algorithm Based on Discrete Fractional Transforms (Numerical Simulations)

Let image $f(m,n)$ of size 256×256 is encrypted based on DFrFT or DFrCT transform with three fractional keys (1,0.9,0.8) and two random phase masks. The encrypted image is queue scrambled to enhance security strength. Image retrieval algorithm steps are divergent from transmission. Image is reverse queue scrambled, and IDFrFT or IDFrCT transformed with keys (-1,-0.9,-0.8), and acquired the retrieved image at receiver. The encryption keys are used between 0 and 1. The fractional keys can be increased due to extra degree of freedom provided by fractional orders. Hence, it becomes almost impossible for intruder to crack the algorithm. The effect of wrong fractional keys on decrypted image is also considered. The flow chart and simulation results for proposed algorithm are shown in figure 2 and 3, 4.

In order to evaluate performance of algorithm variety of images like Flower, baboon, house, peppers have been tested. Mean square error (MSE) between the input image and decrypted image (resumed image), is defined. The MSE can be defined as follows: $MSE = \left[\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[r\left(i,j\right)-o\left(i,j\right)\right]^2\right]$ where M,N are the sizes of images, $|r\left(i,j\right)|$ and $|o\left(i,j\right)|$ are the matrix elements of the decrypted and original image, respectively. The MSE as a function of the deviation of the fractional order a is shown in Fig. 6. We observed that change in MSE with deviation in $-\alpha_3$ is more rapid as compared to $-\alpha_1$. It demonstrate that decryption procedure is more sensitive to fractional order $-\alpha_3$ than $-\alpha_1$.

The normalized MSE called relative error (RE) between the output image and input image is often used to

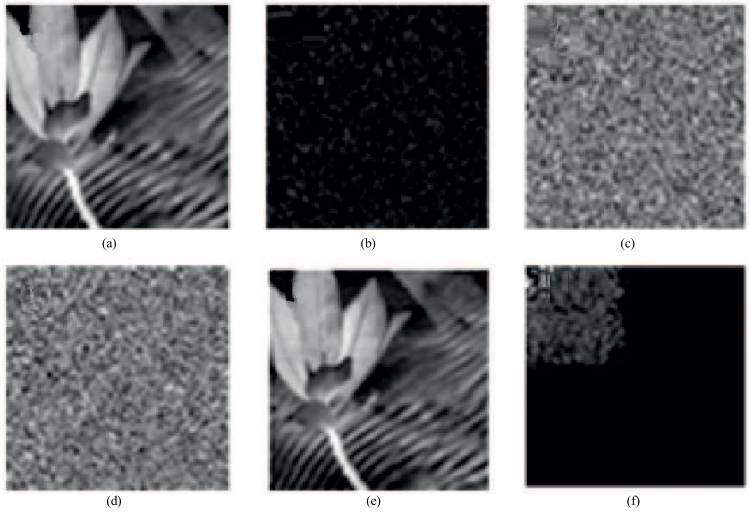


Fig. 3. Results of encryption based on DFrFT and scrambling: (a) – input image, (b) – encrypted image (c) – encrypted scrambled image, (d) – descrambled image, (e) – decrypted image with right fractional keys, (f) –decrypted image with wrong fractional key

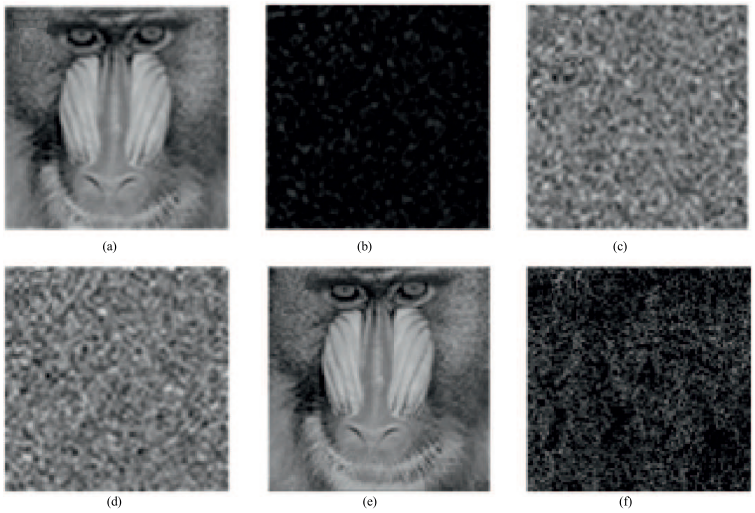


Fig. 4. Results of encryption based on DFrCT and scrambling: (a) – input image, (b) – encrypted image, (c) – encrypted scrambled image, (d) – descrambled image, (e) – decrypted image with right fractional keys, (f) – decrypted image with wrong fractional key

verify the quality of the reconstructed image and defined as:

$$RE = \frac{\sum_{i}^{M}\sum_{j}^{N} ||r(i,j)| - |o(i,j)||^2}{\sum_{i}^{M}\sum_{j}^{N} |o(i,j)|^2}$$

The dependence of RE on the change of fractional order $-\alpha_3$ is shown Fig. 5, with T =1,2,4,8,16, respectively, where T is number of iterations. In the decryption procedure, image can be retrieved with correct fractional orders keys and iterations only.

We observed in Fig. 5, that at correct fractional order value 0.8 the relative error is minimum for all values of T. The corresponding deviations $\delta\alpha$ in fractional order are 0.016, 0.008, 0.004, 0.002 and 0.001 for T = 1,2,4,8, and 16, respectively. With T increases, the decryption procedure becomes sensitive to change of fractional orders and relative error also increases rapidly. When RE> 0.2, the user failed to distinguish the decrypted image with the naked eye [24]. As shown in Fig. 5., the sensitivity to fractional orders can be accustomed by alteration in number of iterations. Thus one can adjust the accuracy of right resumption with slight difference in fractional order and the difficulty of brute force breaking attempts.

In case of $T = 4$, and deviation in fractional order 0.004, the total possible number of searches will be around 3.9×10^{21} [24], this is an extremely large number for an unauthorized person who tries to access the encrypted image. In our simulations, the original image is divided into 1024 subsections. The security strength of iterative discrete fractional transforms encryption without scrambling will be $15.6 \times 10^{21} \times 2^{256\times256\times4}$, [24]. After introducing scrambling operation, the security strength of proposed method will be $15.6 \times 10^{21} \times 2^{256\times256\times4} \times (1024!)^4$, enlarged $(1024!)^4$ times [18]. This is an extremely large number for an eavesdropper to search correct fractional order keys by scanning through all possible combinations.

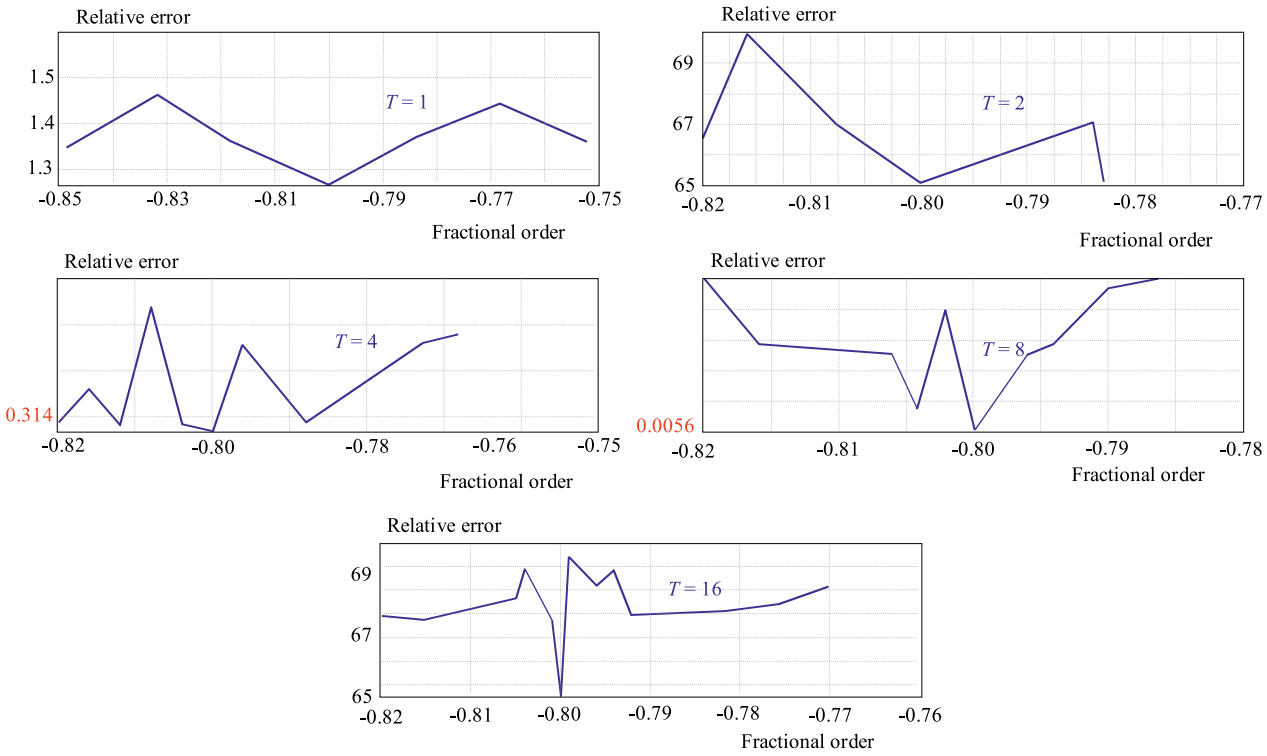


Fig. 5. Relative Error for different iterations

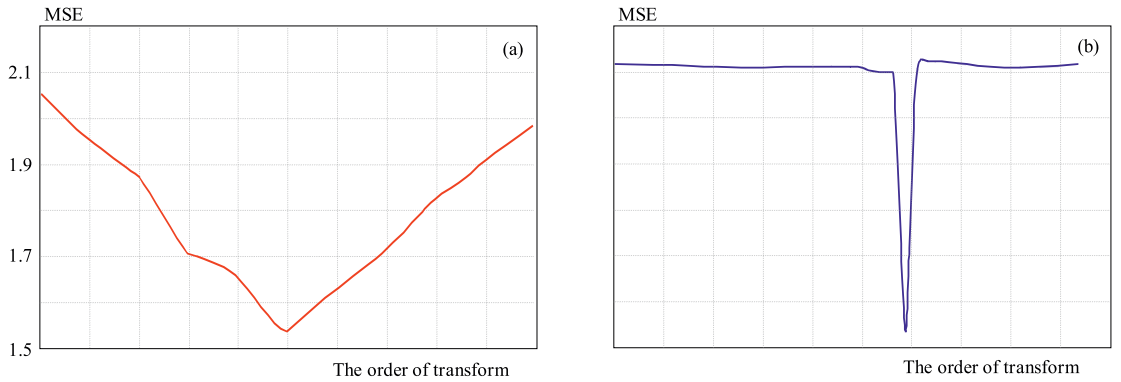


Fig. 6. MSE *vs* deviation in decryption fractional order $-\alpha_1$ and α_3

Dividing the image into more number of subsections will further enhance the security strength. Security to algorithm is also granted by multiple encryption keys in algorithm. In cryptography, the plaintext is the original information to be encrypted. The ciphertext is the encrypted plaintext. The ciphertext-only attack is an attack model in which an attacker tries to deduce the security keys by only studying the ciphertext [25]. This attack can be used to recover the original image data by studying the encrypted images. If fewer portions of the images are encrypted, more portions of the original images can be recovered by an attacker without knowing the encryption algorithm and its security keys. An encryption scheme has an extremely low security level if it cannot withstand this attack. From the experiment results the encrypted images are totally unrecognizable and different from original image.

4 CONCLUSION

In summary, we have proposed an algorithm for secure image retrieval based on discrete fractional transforms. The novelty of our contribution concerns three aspects: (I) we have proposed new algorithm for double security of image. The multiple discrete fractional keys were used between 0 and 1 for encryption. (II). Security strength can be increased by extra degree of freedom provided by fractional orders. keys. Secondly, more subsections of image in scrambling algorithm strengthen the security. Scrambling has enhanced security strength $(1024!)^4$ times for 256×256 image divided into 8×8 subsections (III). Sensitivity of fractional order $-\alpha_3$ *vs* mean square error confirm robustness of algorithm. The increase in number of iterations of algorithm increases the relative error and hence more sensitivity for fractional orders. The robust-

ness of algorithm is checked with brute force attack and cipher-text-only attack.

References

[1] JAYARAMAN, S.—ESAKKIRAJAN, S.—VEERAKUMAR, T.: Digital Image Processing, Tata McGraw Hill Pte. Ltd: New Delhi, 2009.

[2] ZHAO, H.—RAO, Q.—GE, G.—MA, J.—TAN, L.: Image encryption based on random fractional discrete cosine and sine transforms, First int. workshop on Educational Technology and Comput. Science. 1, 2009, 804-808.

[3] WANG, X.—ZHAO, D.—CHEN, L.: Image encryption based on extended fractional Fourier transform and digital holography technique, Opt. Commun. **260(2)** (2006), 449-453.

[4] TAO, R.—XIN, Y.—WANG, Y.: Double image encryption based on random phase encoding in the fractional Fourier domain, Opt. Express **15(24)** (2007), 16067-16079.

[5] GONZALEZ, R. C.—WOODS, R. E.: Digital Image Processing, Pearson Education (Singapore) Pte. Ltd: Delhi, 2004.

[6] OZTURK, I.—SOGUKPINAR, I.: Analysis and comparison of Image Encryption Algorithms, World Academy of Science, Engineering and Technology **3** (2005), 26-30/.

[7] HENNELLY, B. M.—SHERIDAN, J. T.: Image encryption and fractional Fourier transform, Optik **114** (2003), 251-265.

[8] LIU, S.—YU, L.—ZHU, B.: Optical image encryption by cascaded fractional Fourier transform with random phase filtering, Opt. Commun. **187** (2001).

[9] SINGH, K.: Performance of Discrete Fractional Fourier Transform Classes in Signal Processing Applications. PhD Thesis, Thapar University, Patiala, 2006.

[10] ZOU, J.—WARD, R. K.: Introducing two new image scrambling methods, IEEE Trans. on Sig. Process. **2** (2003), 708711.

[11] JING, F.—FEI, H.: FAN transform in image scrambling encryption application, IEEE Trans. on Sig. Process. (2009), 1-4.

[12] LPING, S.—ZHENG, Q.—BO, L.—JUN, Q.—HUAN, L.: Image scrambling algorithm based on random shuffling strategy, IEEE Trans. on Sig. Process. (2008), 22782283.

[13] ZOU, J.—WARD, R. K.—QI, D.: A new digital image scrambling method based on Fibonacci numbers, ISCAS: III, 2004, 965-968.

[14] LIEHUANG, Z.—WENZHUO, L.—LEJIAN, L.—HONG, L.: A novel algorithm for scrambling digital image based on cat chaotic mapping, IEEE conf. on IIH-MSP, 2006, 601-604.

[15] JIPING, N.—YONGCHUAN, Z.—ZHIHUA, H.—ZUQIAO, Y.: A digital image scrambling method based on AES and error correcting code, IEEE Computer Society, 2008, 677-680..

[16] ZHANG, H. Y.: A new image scrambling algorithm based on queue transformation, IEEE Int. conf. on machine learning and cybernetics, 2007, 1526-1530.

[17] ZHANG, H. Y.: A new image scrambling algorithm, IEEE Int. conf. on machine learning and cybernetics, 2008, 1088-1092.

[18] ZHAO, J.—LU, H.—SONG, X.—LI, J.—MA, Y.: Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique, Optics Comm. **249** (2005), 493-499.

[19] NAMIAS, V.: The Fractional Order Fourier Transform and its Applications to Quantum Mechanics, J. Inst. Math Applications **25** (1980), 241-265.

[20] MCBRIDE, A. C.—KEER, F. H.: On Namia's Fractional Fourier Transform, IMA J. Appl. Math **239** (1987), 159-175.

[21] PEI, S. C.—DING, J. J.: Closed-Form Discrete fractional and Affine Fourier Transforms, IEEE Trans. on Signal Process. (2000), 1338-1353.

[22] CANDAN, C.—KUTAY, M. A.—OZAKTAS, H. M.: Discrete fractional Fourier transform, IEEE Trans. on Signal Process. (2000), 1329-1337.

[23] OZAKTAS, H. M.—ZALEVSKY, Z.—KUTAY, M. A.: The Fractional Fourier Transform with Applications in Optics and Signal Processing, John Wiley & Sons: 2001.

[24] ZHANG, Y.—ZHENG, C.—TANNO, N.: Optical encryption based on iterative fractional Fourier transform, Opt. Commun. (2002), 277-285.

[25] MENEZES, A. J.—PAUL, C.—OORSCHOT, V.—VANSTONE, S. A.: Handbook of Applied Cryptography, CRC Press: NewYork, 1997.

Received 27 June 2012

Neeru Jindal received the BTech and MTech degree in Electronics and Communication in 2002 and 2007 respectively from Punjab Technical University, Jalandhar, Punjab, India. She has been involved in various research activities in the area of image and video processing. She holds the position of Research Scholar in the department of Electronics and Communication Engineering, Thapar University Patiala, Punjab, India.

Kulbir Singh received the BTech degree in 1997, MTech degree in 2000. He received PhD degree in 2006 from the Department of Electronics and Communication Engineering, Thapar University, Patiala, Punjab, India. He is having more than ten years of experience in research and academic activities. He has wide number of publications in the area of Image Processing and reviewer of prestigious journals. Presently he holds the position of Associate Professor in Department of Electronics and Communication Engineering, Thapar University, Patiala, Punjab, India.