American International Journal of Research in Science, Technology, Engineering & Mathematics

Available online at http://www.iasir.net

ISSN (Print): 2328-3491, ISSN (Online): 2328-3580, ISSN (CD-ROM): 2328-3629

AIJRSTEM is a refereed, indexed, peer-reviewed, multidisciplinary and open access journal published by International Association of Scientific Innovation and Research (IASIR), USA
(An Association Unifying the Sciences, Engineering, and Applied Research)

Digital Image Encryption with Discrete Fractional Transforms and Chaos: A Comparative Analysis

Bharti Ahuja, Dr. Rajiv Srivastava, Rashmi Singh Lodhi
Computer Science & Engineering
Sagar Institute of Research & Technology, Bhopal, Madhya Pradesh, INDIA

***Abstract**: Information security has been most popular and important issue in the fastest growing age of communication. Therefore various techniques for the security of image have been developed which is commonly known as image encryption techniques. Many methods have already been proposed and in this context the Fourier Transform and its different fractional orders are very recent advancements in this area. In this paper the comparative analysis is done on two methods i.e. DFrFT and DFrST with chaos function. The computer simulations are presented to compare the validity of the methods with histogram analysis between the original images and the decrypted images. The PSNR is also compared between two methods.*
***Keywords**: Image Encryption, Discrete Fractional Transform (DFrT), Discrete Fractional Fourier Transform (DFrFT), Discrete Fractional Sine Transform (DFrST),Chaos, Logistic Map.*

I. Introduction

Security of multimedia information is used to protect the multimedia content from unauthorized access. Cryptography is the technique which is used for secure communication over the network. By using Cryptography technique readable information is converted into unreadable form. Image information is different from the text data, it has larger amount of data, higher redundancy and stronger correlation between pixels. In recent years, many image cryptosystems are proposed. As encryption process is applied to the whole image, it is difficult to improve the efficiency. Encryption of digital image processing becomes more important for Internet data transportation and many methods can be applied for the processing.

The FrFT is a generalization of the ordinary Fourier transform [1] with an order parameter α and is identical to the ordinary Fourier transform when this order α is equal to p/2. Since the ordinary Fourier transform and related techniques are of importance in various different areas like communications, signal processing and control systems, it is natural to expect the FrFT to find many applications in these fields as well. In fact, the FrFT has already found many applications in the areas of signal processing and communications [2-3].

We know that the Cosine and Sine transforms and their discrete versions are useful tools in signal and image processing, such as signal coding [4], watermarking [5] and restoration of de-focused images [6]. In the Ref. [7] Pei and Yeh extended the Cosine transform to the discrete fractional cosine transform (DFrCT) and the discrete fractional sine transform (DFrST). Both of them possess well the angle additivity property of the DFrFT. Moreover, the DFrCT and DFrST are used in the digital computation of FrFT for the reducing computational load of the DFrFT.

The success of FrFT in its application has promoted the development of other kinds of fractional transforms like fractional Hartley transform, fractional Hadamard transform, fractional cosine transform and fractional sine transform (FrST). Pei Soo-Chang redefined the fractional cosine transform and fractional sine transform based on fractional Fourier transform in 2001 [8-9]. FrST is the extension of sine transform and it has been widely used in domain of digital signal and image processing [10]. The definition of DFrST is based on the Eigen decomposition of DST kernel. This is the same idea as that of the discrete fractional Fourier transform (DFrFT).

The rest of this paper is organized as follows. In Section II and III, the FrFT and FrST are explained respectively. In section IV the Logistic Map is explained.

In section V the encryption and decryption algorithm is explained and In Section VI, the performance of the proposed method is verified by the simulation examples. Finally, in Section VII, we make a conclusion.

II. Fractional Fourier Transform

The fractional Fourier transform is a generalization of the ordinary Fourier transform with an order (or power) parameter 'α'. The FrFT belongs to the class of time–frequency representations that have been extensively used by the signal processing community [11].

The angle parameter "a" associated with FrFT, governs the rotation of the signal to be transformed in time-frequency plane from time-axis in the time-frequency plane. A 1-D and 2-D signals of FrFT, denoted by x and y respectively, can be written as matrix multiplications as follows [11]:

$$X_\alpha = R^\alpha x \tag{1}$$

$$Y_\alpha = R^\alpha y\left(R^\alpha\right)^t \tag{2}$$

Where R^α is kernel transform matrix of the DFrFT and can be expressed as:

$$R^\alpha = VD^\alpha V^t \tag{3}$$

In the kernel matrix D^α is diagonal matrix generated by a set of values $\{\exp(-2i\pi m\alpha / M) : n = 0,1,2,....N-1\}$ which are considered to be the Eigen values of the DFrFT. Where α indicates the fractional order of the DFrFT. M is a positive number, usually is an integer which has a meaning of periodicity with respective to the fractional order α in Eigen values. D^α is written as follows:

$D^\alpha = diag[1, \exp(-2i\pi\alpha / M), \exp(-4i\pi\alpha / M),..,\exp(-2i\pi(N-1)\alpha / M)]$The randomness of the transform comes from the matrices V and V^t, where $[...]^t$ indicates the transpose matrix of the matrix $[...]$. The matrix V is generated by N orthogonal vectors $\{v_1, v_2,..., v_N\}$ as:

$$V = [v_1, v_2,..., v_N]$$

The FrFT is defined using this Kernel is given by:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t) R_\alpha(t,u) \tag{4}$$

$$Where\ \alpha = a\frac{\pi}{2}$$

The inverse FrFT is given by:

$$x(t) = \int_{-\infty}^{\infty} X_\alpha(u) R_{-\alpha}(u,t)\, du \tag{5}$$

When FrFT is analyzed in discrete domain there are many definitions of Discrete Fractional Fourier Transform (DFrFT) [12].

The one-dimensional FrFT is useful in processing single-dimensional signals such as speech waveforms. For analysis of two-dimensional (2D) signals such as images, we need a 2D version of the FrFT. For an M×N matrix, the 2D FrFT is computed in a simple way: The 1D FrFT is applied to each row of matrix and then to each column of the result. Thus, the generalization of the FrFT to two dimensions is given by [13],

$$X_{\alpha\beta}(u,s) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R_{\alpha\beta}(u,s;t,r) x(t,r) dt\, dr$$

$$Where,\quad R_{\alpha\beta}(u,s;t,r) = R_\alpha(u,t) R_\beta(s,r) \tag{6}$$

In the case of the two-dimensional FrFT we have to consider two angles of rotation α=aπ/2 and β=bπ/2. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel.

III. Fractional Sine Transform

Discrete fractional sine transform (DFrST) is extended by discrete Fourier transform (DFrFT). DFrST is also a general form of the discrete cosine transform (DST), which has a similar relationship with that between DFrST and the discrete Fourier transform (DST). In mathematics, the discrete sine transform (DST) is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using a purely real matrix. It is equivalent to the imaginary parts of a DFT of roughly twice the length, operating on real data with odd symmetry (since the Fourier transform of a real and odd function is imaginary and odd), where in some variants the input and/or output data are shifted by half a sample.

The definitions of DFrST can be directly given from the DFrFT. Similar to the definitions of DFrCT and DFrST, of which the eigenvectors can obtained from the eigenvectors of the DFrFT[7], the eigenvectors of DFrST are the same with that of the DFrFT if the same symmetric random matrix Q are used. That means when we construct the DFrST, we use the same method to generate the matrix $V = [v_1, v_2,..., v_N]$. However, in the following discussion, we denote the eigenvectors of the DFrST by matrices:

$$V_s = [s_1, s_2,..., s_N] \tag{7}$$

Bear in mind that $v_n = s_n$ for the same matrix Q.

The Kernel matrices of DFrST are defined as follows:

$$R_s^{\alpha} = V_s D_s^{\alpha} V_s^t \tag{8}$$

However the eigenvalue diagonal matrices for DFrST, i.e. D_s^{α} is respectively, chosen as follows:

$D_s^{\alpha} = diag[\exp(-2i\pi\alpha/M), \exp(-6i\pi\alpha/M), ...\exp(-2i\pi(2N-1)\alpha/M)]$ The eigenvalue matrices of the DFrST is also diagonal matrices with the diagonal elements chosen within the set of $\{\exp(-2i\pi n\alpha/M) : n = 0,1,2,....2N-1\}$.The elements of the DFrST is formed by the values with $n = 2j+1$.The parameter α indicates the fractional order of the transform and M relate with the periodicity.

The DFrST of a 1-D signal x and a 2-D image y then can be expressed as:

$$X_s^{\alpha} = R_s^{\alpha} x \tag{9}$$

$$Y_s^{\alpha} = R_s^{\alpha} y \left(R_s^{\alpha}\right)^t \tag{10}$$

When α = 0, the kernels of the DFrST is identity matrices.

On the definitions of DFrST, we adopt the method of Pei and Yeh [7]. Because we use orthogonal eigenvectors to define the DFrST, the mathematical properties of DFrST are thus similar to DFrFT.

IV. LOGISTIC MAP

Chaotic phenomenon is an uncertain and similarly random process appearing in the nonlinear dynamical systems. The random process is neither periodical nor convergent and has an extremely sensitive dependence on the initial value. From the time-domain, the sequence obtained from a chaotic map is similar to the random sequence with weak correlation and a good characteristic of similar white noise. Therefore, it can be used to generate pseudo-random signal or pseudo-random code. With the number of iterations increased, the periodicity of the pseudorandom code can be very long, which generates a long code easily. Due to its extremely sensitive to the initial value and structural parameter; the chaotic system can provide a large number of non-related and similar random signals. With these characteristics, Chaos has been widely used in secure communication [14].

The chaotic function is sensitive to initial condition, is unpredictable, indecomposable and yet contains regularity. Logistic map is a simple equation of chaos functions, which is defined as, [14] [15].

$$x_{n+1} = u * x_n * (1 - x_n) \tag{11}$$

Where $X_n \in (0,1)$ and $u \in [0,4]$ are the variable and parameter, respectively, and n is the number of iterations. Thus, given an initial value x_0 and a parameter u , the series is computed.

V. ENCRYPTION WITH DFRT AND CHAOS

To encrypt a digital image, we need to use an algorithm of two-dimensional DFrT. We can divide it into two one dimensional discrete fractional transforms, then using the periodicity of DFrT; we continue to use the appropriate order of DFrT to decrypt the encrypted image. (Algorithm is same for both DFrFT and DFrST except Fourier and Sine Transform)

The encryption and decryption of DFrT steps are as follows.

1. Logistic map is applied on original image F and the resulted transformed image is F1.
2. Each row vector of the image F1 is transformed by one-dimensional DFrT, with the transform fractional order being α and the resulted transformed image F2.
3. Each column vector of F2 is transformed by another one-dimensional DFrT, with the transform fractional order being β and the resulted transformed image F3. F3 is regarded as the encrypted image and α, β are taken as the cipher keys.
4. Each row vector of F3 is transformed by one dimensional DFrT, using the transform fractional order α'= (-α) and the transformed image is F2'.
5. Each column vector of F2' is transformed by one dimensional DFrT, using the transform fractional order β'= (-β) and the transformed image is F1'.
6. Remove the logistic map from the transformed image F1' and the resulted transformed image is F '. F ' is the decrypted image.

The encryption and decryption processes are shown in Figure 1 (Encryption process with Logistic Map and DFrT) and Figure 2 (Decryption process with DFrT and Logistic Map).

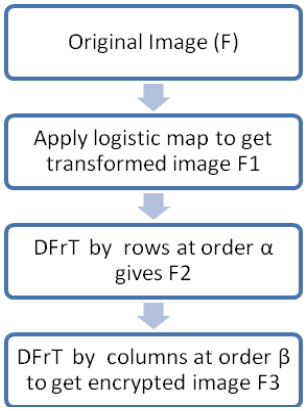


Fig.1. Encryption process with Logistic Map and DFrT.

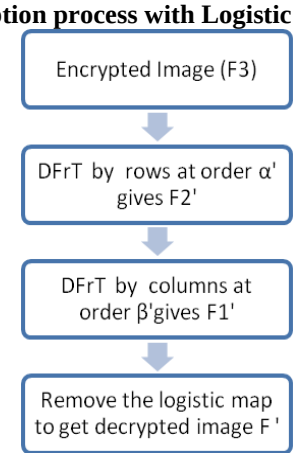
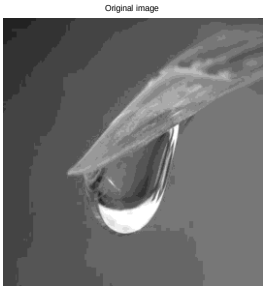


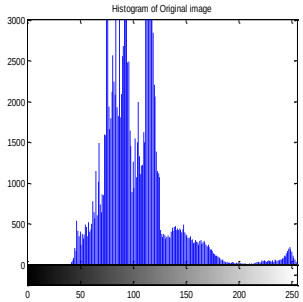
Fig. 2. Decryption process with DFrT and Logistic Map.

VI. Simulation Results

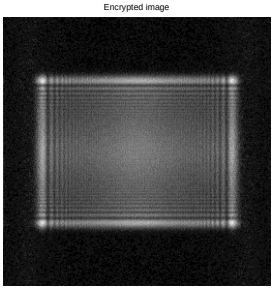
Numerical simulations have been performed on a Matlab platform to verify the validity of the proposed technique. Fig. 3(a) is the original 400 × 400 image drop.jpg of grayscale 256, and Fig. 3(c) is the encrypted image transformed using the keys α =0.6, β = 0.7 of DFrFT and u = 3.9, x_0 = 0.1 of the logistic map. Fig. 3(e) is the correct decrypted image of lena transformed using the keys α'= 0.6, β' =0 .7 of DFrFT and u = 3.9, x_0 = 0.1 of the logistic map.



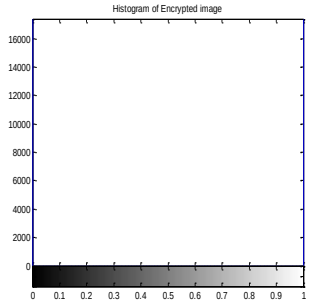
(a) Original image



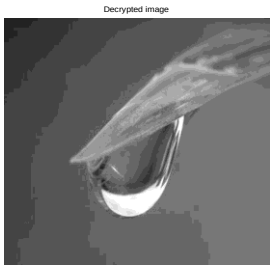
(b) Histogram of Original image

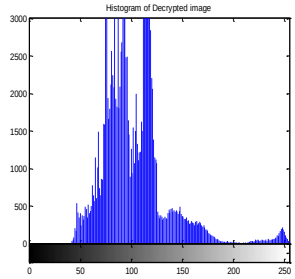


(c) Encrypted image



(d) Histogram of Encrypted image

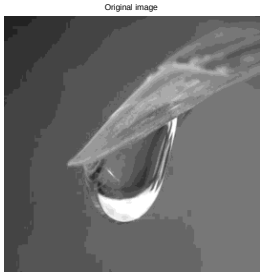


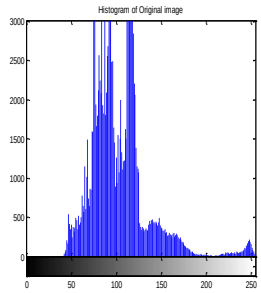


(e) Correct Decryption **(f) Histogram of Correct Decrypted images**

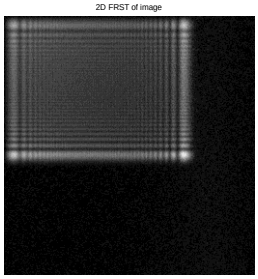
Fig.3 Encryption and decryption results of Drop image using FrFT with Chaos

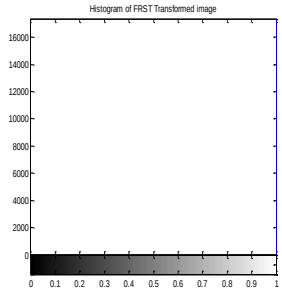
Fig. 4(a) is the original 400 × 400 image drop.jpg of grayscale 256, and Fig. 3(c) is the encrypted image transformed using the keys α = 0.6, β = 0.7 of DFrST and u = 3.9, x_0 = 0.1 of the logistic map. Fig. 3(e) is the correct decrypted image of lena transformed using the keys α'=0.6, β' =0.7 of DFrST and u = 3.9, x_0 = 0.1 of the logistic map.



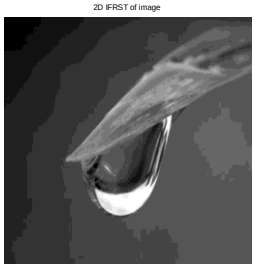


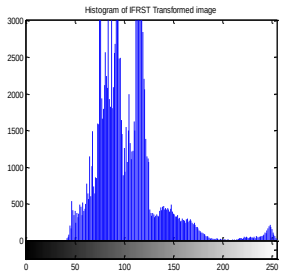
(a) Original image **(b) Histogram of Original image**





(c) Encrypted image **(d) Histogram of Encrypted image**





(e) Correct Decryption **(f) Histogram of Correct Decrypted images**

Fig. 4 Encryption and decryption results of Drop image using FrFT with Chaos

Peak Signal to Noise Ratio:

The PSNR is the only rigorously defined metric. The main reason for this is that no good rigorously defined metrics have been proposed that take effect of the Human Visual System (HVS) into account. PSNR is provided only to give us a rough approximation of the quality of cryptography.

For a good encryption, PSNR should be maximum. The PSNR in mathematical form can be given as equation 12,

$$PSNR = 10log_{10}\left[\frac{256 \times 256}{MSE}\right] \quad (12)$$

Image	PSNR	
	FrFT with chaos	FrSTwith chaos
Drop	238.06 dB	236.74 dB
Lena	235.85 dB	233.87 dB
Cameraman	238.37 dB	236.62 dB

Table 1. PSNR comparison between FrFT and FrST.

VII. CONCLUSIONS

Security is main key here. It is formed by the combination of the order of discrete fractional transform order and the logistic map, as there can be large amount of the combination so this gives formidable key sets, thus providing higher amount of security. Both the methods of encryption and decryption is sensitive that means if the any key other than the correct key is used it will not give correct result with our simulation we have checked that our image and is very much sensitive to the deviation in the original key .

And in the concluding remark it can be said that DFrFT with chaos is slightly better than the DFrST with chaos for image encryption and decryption.

REFERENCES

[1] M. Ozaktas, Z. Zalevsky, and M. A. Kutay, The Fractional Fourier Transform. West Sussex, U. K.: Wiley, 2001.

[2] L.B. Almeida, The fractional Fourier transform and time–frequency representations, IEEE Trans. Signal Proc. 42 (11) (1994) 3084–3093.

[3] D. Mendlovic, Advances in Imaging and Electron Physics, vol. 106,Academic Press, New York, 1999.

[4] F. Bellifemine and R. Picco, Video signal coding with DCT and vector quantization, IEEE. Trans. Commun. 42, (1994) 200.

[5] H. T. Chang and C. L. Tsan, Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain, Appl.Opt. 44, (2005) 6211.

[6] E. Y. Lam and J. W. Goodman, Discrete cosine transform domain restoration of defocused images, Appl. Opt. 37, (1998) 6213.

[7] S. C. Pei and M. H. Yeh, The discrete fractional cosine and sine transform, IEEE Trans. Signal Processing, 49, (2001) 1198.

[8] A.W.Lohmann, D. Mendlovic , Z. Zalevsky, and R.G.Dorch, Some important fractional transformation for signal processing. Opt.commun,vol.125,pp.18-20,1996

[9] Pei Soo-Chang, Min-Mung ,The Discrete Fractional Cosine and Sine Transform. IEEE Trans Signal Processing, 2001, 49(6): 1198-1207.

[10] Conf on Information Sci and Eng . 2009, 1864-1867.

[11] Zhengjun Liu, Qing Guo and Shutian Liu, The discrete fractional random. cosine and sine transforms, Harbin Institute of Technology, Department of Physics, Harbin 150001 P. R.CHINA.

[12] Soo-Chang Pei and Jian-Jiun Ding, "Closed-Form Discrete Fractional And Affine Fourier Transforms", IEEE Transactions on SignalProcessing, Vol. 48, No. 5, May 2000.

[13] I.S. Yetik, M.A. Kutay, H.M.Ozaktas, "Image representation andcompression with the fractional Fourier transform", Opt.Communication. 197 (2001) 275-278.

[14] P. Oprocha and M. Štefánková, "Specification property anddistributional chaos almost everywhere," Proc. Amer. Math. Soc. Vol. 136, pp. 3931–3940, June 2008.

[15] Chris L. Bresten and Jae-Hun Jung, "A study on the numerical convergence of the discrete logistic map," Commun Nonlinear Science Numer Simulat, vol.9, pp. 3076–3088, November 2008.