An Approach to Image Encryption and Decryption using DFF Transform with Chaos

Rajiv Srivastava, Bharti Ahuja, and Rashmi Singh Lodhi

Abstract—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 therefore many methods have been applied for the processing. To focus on security aspect, in this paper we proposed a novel method of image encryption using discrete fractional Fourier transform (DFrFT) with chaos. This technique has been implemented and results are discussed in detail with analyzing parameters like Security, Sensitivity and MSE.

Keywords—Image Encryption, Discrete Fractional Fourier Transform (DFrFT), Discrete Fractional Cosine Transform (DFrCT), Chaos, Logistic Map.

I. INTRODUCTION

As a result of the development of computer network technology, communication of information through personal computer is becoming more convenient. Meanwhile, it also gives hackers opportunities to attack the network. Therefore the communication security is now an important issue for multimedia communications.

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information. Therefore it’s very important to protect our image from unauthorized access. There are so many algorithms available to protect image from unauthorized access.

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 and more important for Internet data transportation and many methods can be applied for the processing [1]. Encryption is the process of transforming information (plaintext) using an algorithm (cipher) to produce a unreadable data to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. Numerous works has been carried out in the literature for the encryption of image using fractional Fourier transform (FrFT). Alok et al [3] had proposed a technique in which the Jigsaw transform was utilized with FrFT for encryption. Phase retrieval method and phase masking were employed with FrFT to encrypt the image.

A new method for image encryption with discrete fractional Fourier transform (DFrFT) and chaos is proposed in this work. Chaos functions have extreme sensitivity to the initial conditions. Logistic map is a simple equation of chaos functions and are used for long key space.

The fractional Fourier transform (FrFT) is more flexible than the conventional Fourier transform (FT) due to the extra parameter of the transform order. With the transform order gradually varying from 0 to 1, the FrFT of a signal can develop from the original function to its FT [4][5]. Thus, it has recently shown its potential in the fields of the image and the optical encryption. Using the transform order to enlarge the key space, the systems based on the FrFT are of a higher security than the corresponding systems based on the FT or cosine transform [6][7][8].

The rest of this paper is organized as follows. In Section II and III, the FrFT and logistic map are explained respectively. In section IV the encryption and decryption algorithm is explained and in Section V, the performance of the proposed method is verified by the simulation examples. Finally, in Section VI, we make a conclusion.

II. FRACTIONAL FOURIER TRANSFORM

The ordinary Fourier transform and related techniques are of great importance in many areas of science and engineering. The fractional Fourier transform is a generalization of the ordinary Fourier transform with an order (or power) parameter ‘a’. The FrFT belongs to the class of time–frequency representations that have been extensively used by the signal processing community [14].

The FrFT is defined for entire time–frequency plane (time and frequency are orthogonal quantities). 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. The FrFT is defined with the help of the transformation kernel $K_a$, as,
The FrFT is defined using this Kernel is given by:

$$X_{\alpha}(u) = \int_{-\infty}^{\infty} x(t)K_{\alpha}(t,u), \text{ Where } \alpha = \frac{\pi}{2}$$

The inverse FrFT is given by:

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

When FrFT is analyzed in discrete domain there are many definitions of Discrete Fractional Fourier Transform (DFrFT) [16].

FrFT computation involves following steps:
- Multiply by a chirp.
- Fourier transform with its argument scaled by ‘csc’.
- Multiply with another chirp.
- Product by a complex amplitude factor.

Properties of the fractional Fourier transform [17]. Let $F_{\alpha}$ denote the operator corresponding to the FrFT of angle $\alpha$. Under this notation, some of the important Properties of the FrFT operator are listed below:

- Identity operator: $F_{0}$ is the identity operator. The FrFT of order $\alpha=0$ is the input signal itself. The FrFT of order $\alpha = 2\pi$ corresponds to the successive application of the ordinary Fourier transform 4 times and therefore also acts as the identity operator, i.e. $F_{0} = F_{2\pi} = I$.
- Fourier transform operator: $F_{\pi/2}$ is the Fourier transform operator. The FrFT of order $\alpha = \pi/2$ gives the Fourier transform of the input signal.
- Successive applications of FrFT: Successive applications of FrFT are equivalent to a single transform whose order is equal to the sum of the individual orders, i.e. $F_{\alpha}(F_{\beta}) = F_{\alpha+\beta}$.
- Inverse: The FrFT of order $-\alpha$ is the inverse of the FrFT of order $\alpha$ since, $F_{-\alpha}(F_{\alpha}) = F_{-\alpha+\alpha} = F_{0} = I$.

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 $M\times N$ 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 [18],

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

Where,

$$k_{\alpha\beta}(u,s;t,r) = k_{\alpha}(u,t)k_{\beta}(s,r)$$

In the case of the two-dimensional FrFT we have to consider two angles of rotation $\alpha = a\pi/2$ and $\beta = b\pi/2$. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel.

In the proposed work, the discrete Fractional Fourier Transform by Eigen-decompose the transform matrix of discrete Fourier Transform is used.

Discrete Fractional Fourier Transform matrix can be written as:

$$F_{N} = UDU^{T}$$

Here D is the diagonal matrix consists of Eigen values of $F_{N}$, U is the orthogonal matrix and T is for transpose. The matrix U is defined as:

$$U = \begin{bmatrix} u_{1}, u_{2}, \ldots, u_{M-1} \end{bmatrix} \text{ For } M=\text{odd}$$

$$U = \begin{bmatrix} u_{1}, u_{2}, \ldots, u_{M} \end{bmatrix} \text{ For } M=\text{even}$$

This is known as Eigen decomposition form of DFrFT. The theoretical framework and the justification for the DFrFT are provided in Ref. [17] and [19].

III. 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 [19]. 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, [18][20]

$$x_{n+1} = u \ast x_{n} \ast (1-x_{n})$$

Where $X_{0} \in (0,1)$ 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.

IV. ENCRYPTION WITH DFrFT AND CHAOS

Digital images contain a number of data but the data are
high correlative and stationary images always contain lots of spatial redundant information. In this paper, we propose a method for image encryption and decryption with discrete fractional Fourier transform and chaos.

To encrypt a digital image, we need to use an algorithm of two-dimensional DFrFT. We can divide it into two one-dimensional discrete fractional Fourier transforms, then using the periodicity of DFrFT; we continue to use the appropriate order of DFrFT to decrypt the encrypted image. In fact, this is a direct result of the property of periodicity of DFrFT.

The encryption and decryption steps are as follows [21].

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 DFrFT, 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 DFrFT, 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 DFrFT, using the transform fractional order α' = (-α) and the transformed image is F2'.

5. Each column vector of F2' is transformed by one-dimensional DFrFT, 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 proposed encryption and decryption processes are shown in Fig. 1:

V. PERFORMANCE PARAMETER

A. Mean Square Error

This parameter is defined as the mean square of difference of corresponding pixel values in the original image and encrypted-image. Similarly root mean square can be defined as the root mean square of difference of corresponding pixel values in the original image and encrypted-image. For a good cryptography, MSE should be minimum. Further, the root mean square can be calculated by taking square root of MSE. The mean square error can be expressed as in equation (9),

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left( f^{'(i, j)} - f(i, j) \right)^2$$  (9)

B. SECURITY

Security is main aim. Key here is formed by the combination of the order of discrete fractional Fourier 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.

C. SENSITIVITY

The method of encryption and decryption should be sensitive that means if any key other than the correct key is used it will not give correct result. In the simulation results we have shown that our image and is very much sensitive to the deviation in the original key.

VI. SIMULATION AND RESULTS

As Numerical simulations have been performed on a Matlab platform to verify the validity of the proposed technique. Fig. 2(a) is the original 256 × 256 image Lena.jpg of gray scale 256. Fig. 2(c) is the encrypted image transformed using the keys α =0.6, β = 0.7 of DFrFT and u = 3.9, x0 = 0.1 of the logistic map. Fig. 2(e) is the incorrect decrypted image transformed using the keys α = 0.9 β = 0.6 of DFrFT and u = 3.9, x0 = 0.1 of the logistic map. Fig. 2(g) is the correct decrypted image of Lena transformed using the keys α' = 0.6, β' = 0.7 of DFrFT and u = 3.9, x0 = 0.1 of the logistic map.
Histogram of FRFT Transformed image

(c) Encrypted image

(d) Histogram of Encrypted image

(e) Incorrect Decryption

(f) Histogram of Incorrect Decrypted image

(g) Correct Decryption

(h) Histogram of Correct Decrypted image

Fig. 3 Encryption and Decryption results of Lena image.

TABLE I

<table>
<thead>
<tr>
<th>Image</th>
<th>MSE (in dB)</th>
<th>Elapsed Time in the Process (in Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.jpg</td>
<td>1.6885×10^{-15}</td>
<td>46.502098</td>
</tr>
</tbody>
</table>

VII. CONCLUSION

We have proposed a new technique to encrypt and decrypt the image using discrete fractional Fourier transform and chaos. Because chaos function has extreme sensitivity to the initial conditions, the effect of image encryption with DFrFT and chaos is better than in the case of DFrFT. Due to the reality of DFrFT and the confusion properties, the proposed cryptosystem is extremely secure and robust. The algorithm used with DFrFT is Eigen vector decomposition type. Encryption and decryption has been done successfully with almost zero process error and less time to complete the whole process. Various parameters have been analyze and discussed like MSE, sensitivity and key space etc.

REFERENCES

http://dx.doi.org/10.1109/IAS.2009.89