Improved Security Mechanism for Color Images using Fractional Fourier Transforms

[1]Dr.Jitendra Singh Chauhan, [2]Mr. Devendra Suthar, [3]Mr. Sandeep Bordia
[1]Associate professor & Head of Department, [2, 3]Assistant professor
Department of Computer Science & Engineering, Aravali Institute of Technical Studies, Udaipur, India
Email - [1]chauhan.jitendra@live.com, [2]dev_arya123@yahoo.com, [3]sandeep11d@gmail.com

Abstract: *In this paper we are presenting a comparison between chaotic function and different random phase masks, which is used encryption decryption of color images, based on Fractional Fourier Transform (FRT). Random The different fractional orders and random phase masks used during the process of encryption and decryption are the keys to enhance the security of the presented system. The mean square error between the decrypted image and the input image for the correct order and the incorrect order of the fractional Fourier transform has also been calculated.*

Key Words: *Encryption; Decryption; Fractional Fourier transform; Mean square error (MSE).*

1. INTRODUCTION:

Information security is one of the important issues in the present information age where information is being disseminated from one place to other at a rapid rate [1]. A number of optical image encryption systems have been proposed in the literature for the same [1, 3]. Out of the various techniques proposed for image encryption [1–3], double random phase encoding [3] is the most well-known technique. This technique uses two statistically independent random phase masks in the input and the Fourier planes to encrypt the input image into a stationary white-noise. An extension of this technique to the fractional Fourier domains has also been presented in [6–9].

In this paper we evaluate the difference random phase masks using chaotic functions for channel encryption of the colored images. A brief review of the FRT and chaos functions is discussed in next section. The discussion of the image encryption using several random phase masks and the simulation results are presented in section III and IV respectively. Conclusions are presented in the last section V.

2. REVIEW OF PREVIOUS WORK:

1. The FRT and Chaos function

$f_p(x_p) = F_p\{f(x)\}(x_p) = \int f(x) K_p(x, x_p)\, dx$ where the kernel is given by:

$$K_p(x, x_p) = \frac{\exp[-i(\pi\theta/4 - \phi/2)]}{\sqrt{\sin\phi}} \exp[i\pi(x^2 \cot\phi - 2x\, x_p \csc\phi + x2 \cot\phi)], \quad 0 < |p| < 2,$$

$$= \delta(x - x_p), \quad p = 0,$$

$$= \delta(x + x_p), \quad p = \pm 2$$

Here $\phi = p(\pi/2)$, $\theta = \text{sgn}(\sin\phi)$ and p is the order of the FRT. The symbol Fp expresses the FRT of order 'p', x and x_p are the coordinates in the input domain and output *p*th fractional domain, respectively. For p=1, the FRT is equivalent to the ordinary Fourier transform. The fourth order of the FRT is equivalent to the original function. The FRT is a linear transform. The FRT is additive in indices, i.e.

$$F_{p1}\{F_{p2}\{f(x)\} = F_{p1+p2}\{f(x)\}$$

Chaos functions have also been used mainly to develop the random phase masks for phases encrypt of color images [ ]. These functions generate iterative values which are completely random in nature but limited between bounds.

2. Double random Fourier plane encoding [10]

Let (x, y) denote the space coordinates, and (u, v) the coordinates in the Fourier domain as shown in Fig. 1a. The real-valued function $f(x, y)$ denotes the original two dimensional images to be encrypted, n denotes the index of primary color components (n = 0, 1, 2) i.e. $f_0(x, y)$, $f_1(x, y)$ and $f_2(x, y)$ correspond to red, green, and blue color components respectively. The above three components are multiplied by a random phase mask $\Phi_1(x, y)$ and is subsequently Fourier transformed. In the next step, the Fourier transformed data is multiplied with another phase mask Φ_2 (u, v), which is statistically independent of $\Phi_1(x, y)$. Random phase masks are generated by chaos functions. Fourier transform is then performed on this image to obtain the encrypted image.

During the decryption process shown in Fig. 1b, the encrypted image is inverse Fourier transformed and multiplied with complex conjugate of Φ2 (u, v). The image thus obtained is inverse Fourier transformed and consequence again multiplies with complex conjugate of Φ1 (x, y) to get the decrypted image. The two random

phase masks used for encryption acts as keys for the data security and decryption.

3. Double random Fractional Fourier plane encoding [10]

This method may be regarded as a generalization of the previous method in the sense that the input, random phase mask, encryption and the output planes are related to each other by FRT. This technique establishes to be more secure as compared to its Fourier counterpart, because one needs to know the fractional orders relating the input-, encryption and output-planes in addition to the random phase mask.

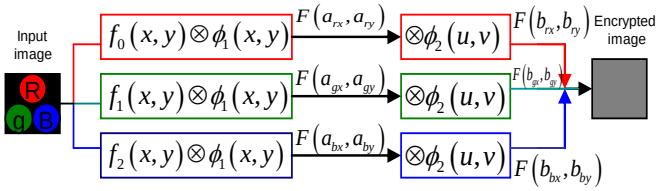

Fig.1 a

3. PRESENT WORK:

In the present work, different random phase masks have been evaluated with reference to the method discussed in the subsection 2.3 For the two-dimensional chaos function, two seed values are required to generate the random phase mask. The FRT with different fractional orders along each spatial coordinate is performed for all the three color components i.e. (a_{rx} , a_{ry}) for red, (a_{gx}, a_{gy}) for green, and (a_{bx}, a_{by}) for blue respectively as shown in Fig 1.a. The transformed primary color images are then multiplied with three phase masks Φ_2 (u, v) in the fractional domain, where u and v denote the coordinates in the respective fractional domain. In the final step, these three encrypted images are combined to get the colored encrypted image e(x, y). The presented technique involves 16 input parameters in all, including 12 different fractional orders and four seeds values for two random independent phase masks which can be considered as keys for decryption. Improper selection of any of these parameters during decryption fetches negative results.

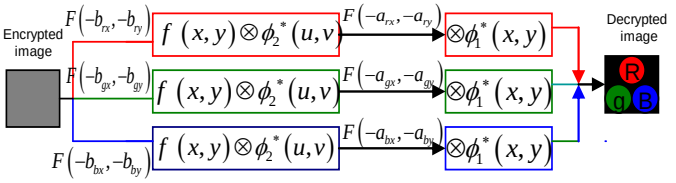

Fig. 1 b

The decryption process is described in Fig.1 b. The encrypted image is first decomposed into three primary colors masks Φ^*_2 (u, v) in the fractional domain where '*'denotes complex conjugate. Finally these three images are combined to get the decrypted image.

4. RESULTS AND DISCUSSION:

Comparison of different random phase masks using chaotic functions have been performed on MATLAB and the MSEs are obtained.

Fig.2a

Fig.2b

Fig. 2c. Color images has to encrypted

Chaos functions used in the simulations are as follows:

a. $x_{n+1} = a \,.\, x_{n.} \, mod \, 1$
$y_{n+1} = a \,.\, y_n . \cos(4\pi x_n)$.
This is bounded for $0 \le a \le 2$ and $0 \le b \le 1$ with 'x_0' as the initial value.

b. $x_{n+1} = a \,.\, x_{n.} \, mod \, 1$
$y_{n+1} = a \,.\, y_n . \sin(4\pi x_n)$

c. $x_{n+1} = 4 . x_n . (1- x_n)$
$y_{n+1} = (2 - y_n^2)$

d. $x_{n+1} = 4 . x_n . (1- x_n^2)$
$y_{n+1} = (2 - y_n^3)$

e. $x_{n+1} = 4 . x_n . (1- y_n^3)$
$y_{n+1} = (2 - y_n^4)$

Fig 3. Shows decrypted color images with random phase at (b) mask and FRT orders (.1, 1.9), (.2, 1.8), (.3, 1.7) for red, green, blue channels respectively and the corresponding MSEs are (784.1942, 280.4309, 6.3023e+003), (336.6144, 646.3686, 6.9029e+003), (992.2804, 1.2312e+003, 2.9889e+003) with FRT orders (0.1, 1.9), (0.2, 1.8), (0.3, 1.7) for red, green, blue

channels respectively for all three images i.e., peppers football, greens respectively.

Fig.3a

Fig.3b

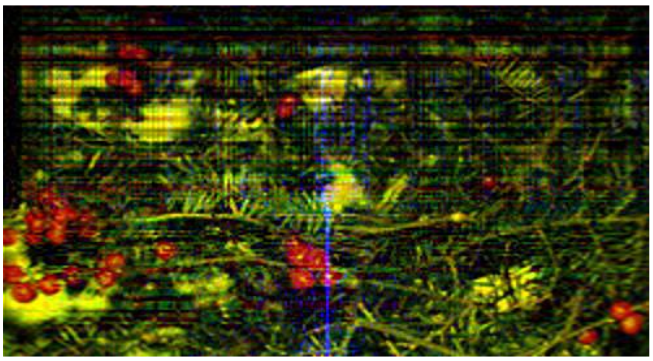

Fig .3c Original color image on Receiver with FRT(b)

Fig. 4 shows similar results using random phase mask (c) and FRT orders (0.1, 1.9), (0.2, 1.8), (0.3, 1.7) for red, green, blue channels respectively and the MSEs are (593.3102, 158.9205, 4.3023e+003), (296.4202, 219.2870, 8.2424e+003) (4.3755e+003, 566.8170, 4.7596e+003) for peppers, football, greens respectively.

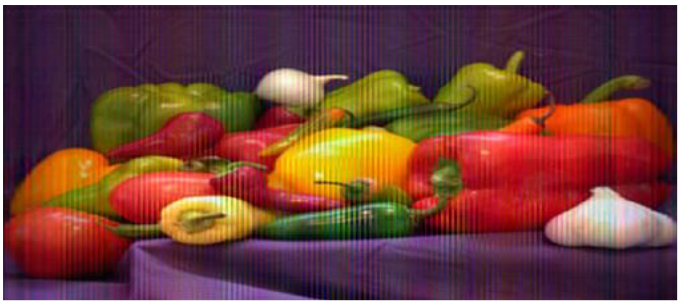

Fig.4a

Fig.4b

Fig. 4c Original color image on Receiver with FRT(c)

Fig. 5 shows similar results using random phase mask (d) for FRT orders (.1, 1.9), (.2, 1.8), (.3, 1.7) for red, green, blue channels respectively and MSEs are (487.0846, 129.2242, 4.3771e+003), (252.4211, 184.8263, 8.3264e+003), (534.0363, 544.2486, 4.8176e+003) for peppers football, greens respectively.

Fig.5a

Fig.5b

Fig.5c Original color image on Receiver with FRT(d)

Fig. 6 shows similar results with random phase mask (e) and FRT orders (.1, 1.9), (.2, 1.8), (.3, 1.7) for red, green, blue channels respectively and the MSEs are (394.4273, 104.1323, 4.4407e+003), (211.5072, 154.9592, 8.4022e+003), (503.5351, 512.9515, 4.8723e+003) for peppers, football, greens respectively.

Fig. 6a

Fig. 6b

Fig. 6c Original color image on Receiver with FRT(e)

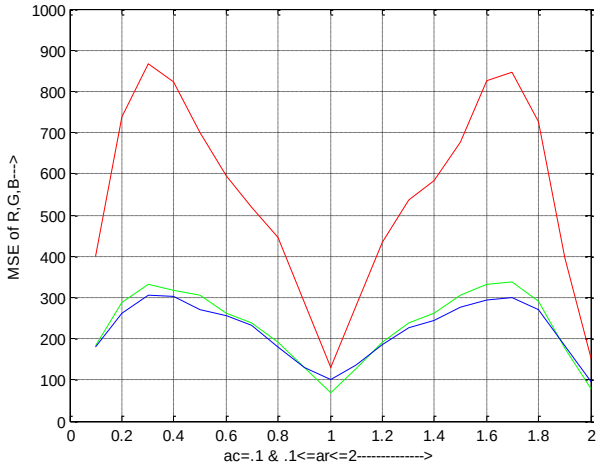

Fig.7. MSE vs. fractional orders of FRT for red, green and blue color channels.

The MSEs using the chaos phase mask (a) for all three color images are found to be (456.9932, 270.5058, 4.0572e+00), (222.9313, 401.5761, 7.0384e+003) (813.8844, 1.0634e+003, 4.2100e+003). On comparison with this MSEs with MSEs corresponding to previous random phase masks, it is observed that the random phase (e) is more superior to chaos phase mask due to lesser MSEs of all thee channels for all color images. It can be observed that the encrypted colored image is fully secured against unauthorized access only when fractional orders in all the three channels are incorrect. The performance of the presented technique has been numerically evaluated. In order to quantitatively evaluate the effect caused by the deviation of different fractional orders, the MSE between the input image and the output image is defined as:

$$\mathrm{MSE}(I_1,I_2)=\frac{1}{NxN}\sum_{i=1}^{N}\sum_{j=1}^{N}|(I_2(i,j)-I_1(i,j)|^2$$

The MSE between the decrypted image and the original image is calculated with respect to variation in only one fractional order across all the three channels and is plotted in Fig. 7. For all the three channels, the MSE is calculated between the respective color channels of the original image and the decrypted image. It is also observed that, the error in the fractional order of 0.02 will protect the data when the fractional orders are used as a key

5. CONCLUSIONS:

We have compared different random phase masks with chaotic phase mask in the present work. It is observed that random phase mask which is defined as in (e) is superior to chaotic phase mask because MSEs of all three channels corresponding to the color images considered here.

REFERENCES:

1. Nishchal NK, Joseph J, Singh K. Fully phase-encrypted memory using cascaded extended fractional Fourier transform. *Opt Lasers Eng 2004;42(2):141–51*.
2. Hennelly BM, Sheridan JT. Image encryption and the Fractional Fourier transform. Optik 2003;114(6):251–65. encryption schemes based on double random phase keys. *Opt Lett 2005;30(13):1644–6.*
3. Liu S, Yu L, Zhu B. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. *Opt Commun 2001;187(1–3):57–63*.
4. Zhang Y, Zheng CH, Tanno N. Optical encryption based on iterative fractional Fourier transform. *Opt Commun 2002;202(4–6):277–85.*
5. Zhu B, Liu S. Optical image encryption based on the generalized fractional convolution operation. *Opt Commun 2001;195(5–6): 371–81.*
6. Zhu B, Liu S. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. *Opt Lett 2001; 26(16):1242–4.*
7. Hennelly BM, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. *Opt Lett 2003;28(4):269–71*.
8. Lohmann AW. Image rotation, Wigner rotation, and the Fractional Fourier transform. J Opt Soc Am A 1993; 10 (10): 2181–6.
9. Ozaktas HM, Zalevsky Z, Kutay MA. The Fractional Fourier Transform with applications in optics and signal processing. *UK: Wiley; 2001*.
10. Madhusudan Joshi , Chandrashakher , Kehar Singh Color image encryption and decryption using fractional Fourier transforms *Optics Communications 279 (2007) 35–42.*