ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

MODIFIED IMAGE ENCRYPTION APPROACH

Meenakshi Jagawat
E-Mail Id: msept.05@gmail.com
Malaviya National Institute of Technology, Jaipur

Abstract-Discrete fractional Fourier transform is an extension of Fourier transform with an additional order parameter. It finds application in encryption of digital images. In the present paper the image is first divided into subimages. The cryptographic algorithm is applied independently to each subimage. It uses five keys made up of three fractional orders and two random phase masks for each of the subimage thereby increasing total number of keys used for the image as a whole. All these keys are necessary to properly decrypt the image. The proposed encryption scheme enhances data security and the net bits used in the image transmission are reduced.

Keywords: Encryption, Decryption, DFRFT, Chaos.

1. INTRODUCTION

Information Security is the protection of information in potentially hostile environments. It is a crucial factor in the growth of information-based processes in industry, business, and administration. During the last decades, information security has become an interesting topic of research due to its importance in many fields such as banking, telecommunications and broadcasting. This has led to the need for systems and algorithms for information encryption. Image security is an important part of information security for applications in engineering, industrial and medical processes. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and, more generally, in the emerging information society. The digital image is encrypted using fractional Fourier transform (FRFT)[1-3]. FRFT is the generalization of Fourier transform. This technique uses two statistically independent random phase masks (RPM) and the Fourier planes to encrypt the input image[4]. An extension of this technique to the Fractional Fourier domain has been presented by Unnikrishnan et al.[5] and later significant work has been done in this area by other researchers [6-8]. In this work the image is first divided into four subimages and encryption is carried out independently to each part. Each subimage uses five keys for encryption thereby increasing total number of keys used to four times for the complete image. It reduces the net bits used for the subimage to ¼th of that of the image. To evaluate the performance of the proposed technique digital simulation is carried out and statistical analysis is done.

2. PRELIMINARIES

2.1 Fractional Fourier Transform

The continuous fractional Fourier transform (FrFT) of order p, is a linear integral operator that maps a given function f(x) onto function f_p (ξ), by:

$$f_p(\xi) = F^p[f(x)] = \int_{-\infty}^{+\infty} K_p(\xi,x) f(x)\,dx \tag{1}$$

Where kernel this defined as

$$K_p(\xi,x) = C_\alpha \exp\left(-i\pi\left(\frac{2x\xi}{\sin\alpha} - (x^2+\xi^2)\cot\alpha\right)\right) \tag{2}$$

$$C_\alpha = \frac{\exp\left(-i\left[\left(\pi\frac{sgn(\sin\alpha)}{4}\right)-\frac{\alpha}{2}\right]\right)}{\sqrt{|\sin\alpha|}} \tag{3}$$

where α = πp/2.

The discrete fractional Fourier transform (DFrFT) is the defined by Candan[9] as,

$$F^p[m,n] = \sum_{k=0,k\neq(N-1+N^2)}^{N} u_k[m]\, e^{-i\frac{\pi kp}{2}}\, u_k[n] \tag{4}$$

$$f_p[n] = F^p(f(n)) = \sum_{n=0}^{N} F^p[m,n]\, f[n] \tag{5}$$

Where $u_k[n]$ is the kth discrete Hermite-Gauss function and $(N)_2$=Nmod2, this discrete transformation is also periodic in p, with period 4.

2.2 Logistic Chaotic Map

The logistic map is a polynomial mapping of degree 2 where a complex, chaotic behaviour can arise from a simple non-linear dynamical equations. The map was popularized in a 1976 paper by the biologist Robert May[10] as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst. Mathematically, the logistic map is represented by a nonlinear difference equation:

$x_{(n+1)} = f\lambda(x_n) = \lambda\, x_n\,(1-x_n)$

where $0 \leq x_0 \leq 1$,

x_0 and λ are the system variable and parameter respectively, and n is the number of iterations.

The quadratic function $f\lambda(x_n)= \lambda x_n (1-x_n)$ exhibits extremely complex random behavior as λ varies from 1 to 4.

3. ENCRYPTION/DECRYPTION

The steps involved in the process of encryption/decryption are as follows:
STEP 1: The image is first divided into four subimages of NxN each.
STEP 2: Each subimage is then placed as the phase of complex exponential.
STEP 3: The result obtained in step 2 is fractionally transformed three times and in intermediate steps it is multiplied by two statistically independent random phase masks.
STEP 4: To decrypt the subimage encrypted in step 3, conjugated complex of the encrypted subimage is taken and the encryption procedure is applied inversely.
STEP 5: To recover the initially encrypted subimage negative of the phase of the result of step 4 is taken.
STEP 6: Step 2 to 5 is repeated for rest of the subimages.
STEP 7: Finally, the decrypted subimages are combined to get the complete image.

4. RESULTS

The technique is shown to be quite suitable for the encryption and decryption of digital images as only partial and meaningless information is recovered when unauthorized keys are selected. Here we applied the encryption techniques and corresponding to that the results obtained as shown.

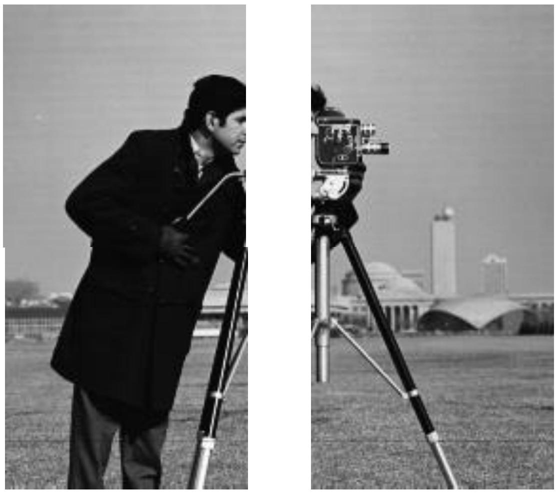


Fig. 4.1 Original Image Divided into Four Subimages

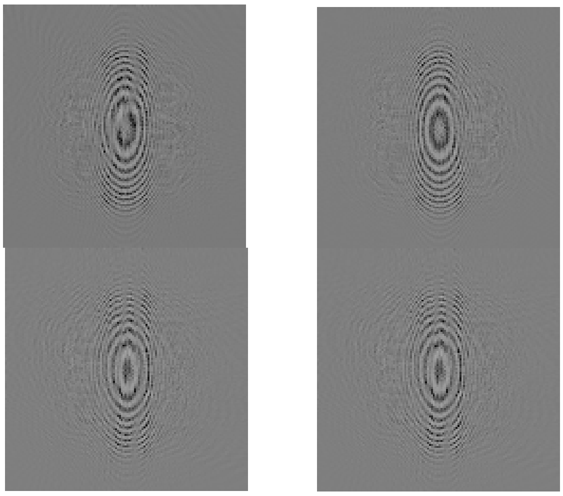
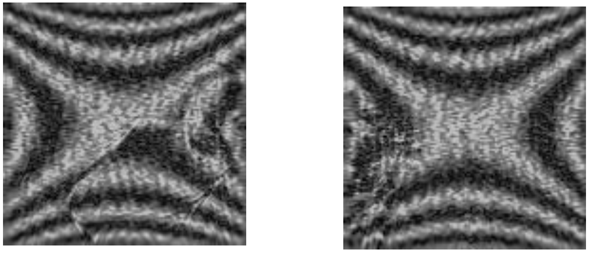


Fig.4.2 Encrypted Subimages

Intensity distribution of encrypted image varies with changing keys. The image will not be recovered, if the keys used in the decryption process are not equal to the keys used in the encryption process.



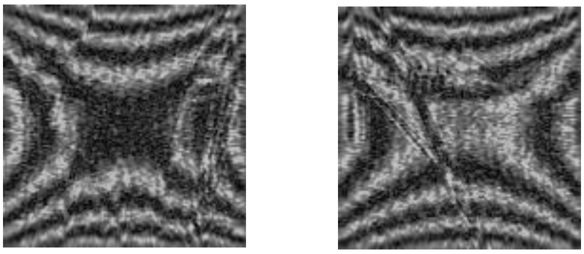


Fig. 4.3 Subimages Decrypted with wrong Keys

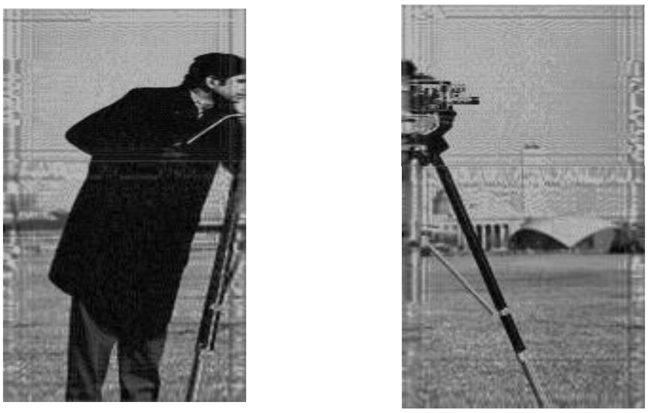
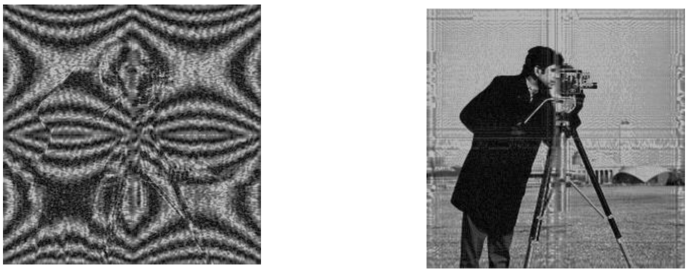


Fig. 4.4 Subimages Decrypted with Correct Keys



(a) **(b)**

Fig. 4.5 Decrypted Image with (a) Wrong Keys (b) Correct Keys

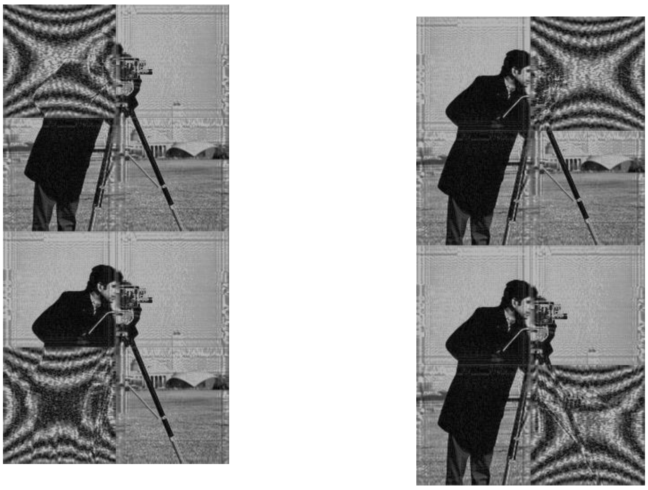


Fig. 4.6 Decrypted Image with Wrong Keys used for Subimages

5. PERFORMANCE ANALYSIS

5.1 Key Space Analysis

The key space is the total number of combinations that can be used in the encryption system. In the proposed technique the keys are made up of three fractional orders and two RPM’s.

Total number of keys used = 5 x 4 = 20

So the size of key space will be $10^{16 \text{ x } 20}$

Assuming precision is 10^{-16}.

Therefore the key space is good and can withstand unauthorized attacks.

5.2 Bits in Use

The number of bits used for the grayscale image (with no compression and neglecting any header information) is given by**:**

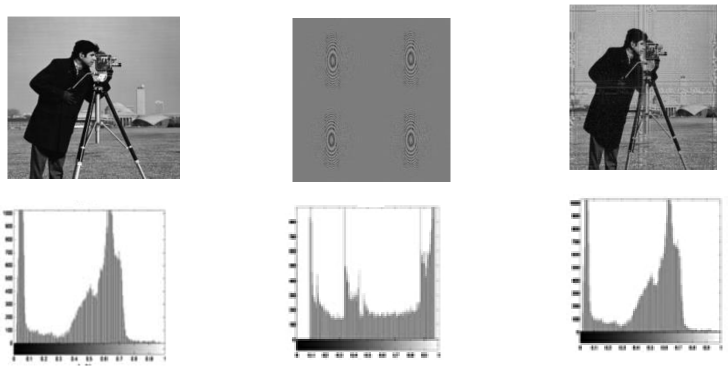
256 x 256 x 1 = 65536 bytes
= 65.536 Kb

In the proposed method it is reduced to:

128 x 128 x 1 = 16384 bytes
= 16.384 Kb

5.3 Histogram Analysis

An image histogram illustrates how pixels in an image are distributed.We have analysed the histograms of the original image,encrypted image, decrypted image. More even the encrypted image histogram higher the safety level of the algorithm .

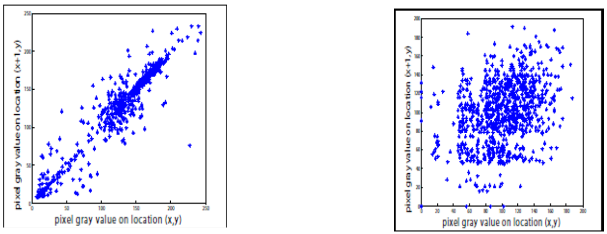


(a) (b) (c)

Fig. 5.1 Histograms of (a) original image (b) encrypted image (c) decrypted image

5.4 Correlation Analysis

In order to examine the correlation property between the adjacent pixel pairs correlation analysis is done. However the adjacent pixels in the original image are highly correlated, there is negligible correlation between the two adjacent pixels in the encrypted image.



(a) (b)

Fig. 5.2 Correlation analysis of (a) encrypted image (b) decrypted image

CONCLUSION

Fractional Fourier transform is the generalization of Fourier transform, it is required to add additional feature to the encryption and decryption process of digital images. A modified approach of dividing the image into separate objects and then applying digital encryption techniques has been presented. It has enhanced the system security as the key space is increased. In the present work the image has been divided into four sub-images which are encrypted independently, each using five keys for encryption thereby increasing total number of keys used to four times the keys used for the encryption of complete image. It reduces the bandwidth requirement for transmission i.e the net bits used for the sub-image to $\left(\frac{1}{4}\right)^{th}$ of that used for the image. The proposed technique can be generalized for N sub-images, increasing the key space for the complete image to N times the number of keys used to encrypt a sub-image. This will also reduce the net bits used to $\left(\frac{1}{N}\right)^{th}$ of the image.

REFERENCES

[1] M.Vilardy, J.E.Calderon, C.O.Torres and L.Mattos, "Digital image phase encryption using fractional fourier transform", Electronics, Robotics and Automotive Mechanics Conference CERMA, 2006.

[2] H. M Ozaktas, Z. Zalevsky and M. A. Kutay, “The fractional Fourier transform with applications in optics and signal processing”, Wiley, 2001.

[3] Min-HungYeh, Soo-Chang Pei, “A method for the discrete fractional Fourier transform computation” IEEE Transactions on Signal Processing, Vol.51, pp.889 – 891, 2003.

[4] Refregier, B.Javedi, “optical image encryption based on input plane and Fourier plane random encoding”, Opt.Lett.20, pp.767-769, 1995.

[5] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain”, Opt. Lett., vol.25, pp. 887- 889,2000.

[6] Ran Tao, Xiang Yi Meng, Yue Wang, “Image encryption with multiorders of fractional Fourier transform”, IEEE Transaction on Information Forensics and Security, vol.5, No.4, 2010.

[7] 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.

[8] Z. Liu and S. Liu, “Randomization of the Fourier transform”, Opt. Lett., vol. 32, pp. 478–480, 2007.

[9] C.Candan, M.A Kutay, and H.M Ozaktas, “The discrete fractional Fourier transform,” IEEE Trans. Signal Process., vol.48, no.5, pp.1329-1337, May 2000.

[10] R. M. May, “Stability and Complexity in Model Ecosystems”, Princeton University.