ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A Novel way of image encrption with piplining pixel scrambling and fractional fourier transform

Sunita Kumari[1] , Pratap Singh Patwal[2]

M. Tech. Scholar, Computer Science & Engineering, IET Group of Institutions, Alwar, India[1]

Professor, Computer Science & Engineering, IET Group of Institutions, Alwar, India[2]

Abstract: A novel way of image encryption based on fractional Fourier transforms (FRFT) and pixel scrambling technique is described and demonstrated in this paper. The idea of pixel scrambling is presented and an implementation to realize the pixel scrambling and decoding is also proposed. Numerical simulation results are given to verify the algorithm, and relative error (RE) between the decoded images and the original image versus the deviation of fractional orders is discussed. Comparing with single FRT encryption, the security using this method for optical image encryption is greatly improved due to the introduction of the pixel scrambling technique.

Keywords: FT, FRFT, Scramble, Encryption

I. INTRODUCTION

According to the cryptography, encryption is a way of transforming any sensitive information using an algorithm (called a cipher) to make it unreadable to anyone except those possessing extraordinary information, more often than not referred as key. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption (i.e., to make it unencrypted). The use of encryption in military applications to facilitate secret communication is known fact. But now it is commonly used in securing data within various kinds of national system. With the evolution of Internet and the increase in the necessity for image transmission, information security and data encryption are becoming more and more important. Encryption systems using Fourier transform have recently caught eyes for the multiple advantages of processing complex two-dimensional data in parallel and transmitting at great speed [1]. Fourier transform is widely used in signal processing system. The fractional Fourier transform (FRFT) is new generation of the conventional Fourier transform with a transform order parameter α, which may be integer or fraction. In every field where Fourier transform is used, the processing effect can be greatly improved by using FRFT. Many researches on data encryption with FRFT have been reported [5–14]. Unnikrishnan et al. [5,6] encoded a primary image to stationary white noise by using two statistically independent random phase masks in fractional Fourier domains. Nishchal et al. [7] proposed a full phase encryption system, where the encrypted image was holographically recorded in a barium titanate crystal and then was decrypted by generating through phase conjugation. Nishchal et al. [10] used FRT in digital holography, that is, the encrypted data and the decryption key were recorded as digital holograms. Full digital technique used in this method enabled digital storage, transmission, and decryption of encrypted data.

Hennelly and Sheridan [11] demonstrated a new method based on random shifting of different sections of the original image in fractional Fourier domains, which shows superior, compared with available methods, at least comparable robustness to blind decryption. Nishchal et al. [14] performed a jigsaw transform with diffractive optical element and a localized fractional Fourier transform on the original image, in which two random phase masks are used to encrypt the image to a stationary white noise. In the Ref. [14], the jigsaw transform index and the number of image segments should be equal. Otherwise, the jigsaw has to be done digitally on the original image. The size of different segments is limited by the diffractive elements manufacture processing and could not be small enough.

A new encryption method based on the fractional Fourier transform and pixel scrambling techniques is proposed in this paper, where FRFT, pixel scrambling and random phase mask are combined and employed for several times. The flexibility of this method is demonstrated both theoretically and by simulation.

II. DEFINITION OF FRFT

FRFT is a generalization of FT [1, 15]. It is not only richer in theory and more flexible in application, but is also not expensive in implementation. It is a powerful tool for the analysis of time-varying signals. With the advent of FRFT and related concepts, it is seen that the properties and applications of the conventional FT are special cases of those of the FRFT. However, in every area where FT and frequency domain concepts are used, there exists the potential for generalization and implementation by using FRFT. Mathematically, α^{th} order FRFT is the α^{th} power of FT operator. Hence α^{th} order FRFT of any signal $s(t) \in L(R^2)$ is given by

$$F^{\alpha}[s(t)] = \int_{-\infty}^{+\infty} s(t)K(\alpha;\omega,t)dt \tag{1}$$

where

$$K(\alpha,\omega,t)=K(\alpha)\exp[(B(\alpha)\omega^2-C(\alpha)\omega t+B(\alpha)t^2)] \tag{2}$$

Is the kernel of F^{α}, α is the fraction, and

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

$$K(\alpha)=\sqrt{\frac{[1-j\cot(\alpha)]}{2\pi}} \quad (3)$$

$$B(\alpha)=\cot(\alpha) \quad (4)$$

$$C(\alpha)=\frac{1}{\sin(\alpha)} \quad (5)$$

$$\alpha=\frac{\pi a}{2} \quad (6)$$

For integer values of α it can be deduced that my fractional Fourier transform repeat itself at an interval of 4 that can be shown as

$$F^{4m+l}[s(t)]=F^{l}[s(t)] \quad (7)$$

where *m* is any integer and *l* can be any real number.

III. PIXEL SCRAMBLING

Pixel scrambling is equal to image division and limited steps of matrix primary transform, so as to displace the position of pixels. For digital image, pixel scrambling is the interchange of gray or RGB value of different pixels. It means that the gray or the RGB value of the point (x, y) is exchanged with that of (x0,y0). One could not obtain any information about the original image from the pixel scrambled image, but the original image can be retrieved by repositioning the disturbed image according to special order.

The principle of pixel scrambling and decoding is depicted in Fig. 1. At first, the division and taxis are applied to the original image, as shown in Fig. 1(a). For simplicity, the image is assumed to be divided into 2x2 subsections and each subsection is numbered. The divided subsections are repositioned relative to one another according to some random permutation. As a result, the partly encrypted image will be gotten, just as shown in Fig. 1(b). During the decryption, the encrypted image is divided and numbered again, as shown in Fig. 1(c). The numbers inside and outside of the brackets are given during the encryption and decryption, respectively. The contrary operations, which have been done during the encryption, ought to be done on Fig.1(c) and the final result is given in Fig. 1(d). Obviously, the encrypted image will be exactly decrypted with inspecting the numbers inside brackets.

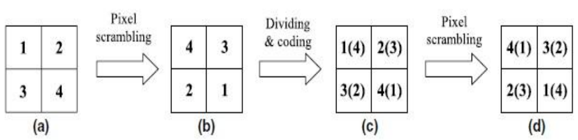

Fig 1 Principle of pixel scrambling and decoding using 2x2 image

IV. PROPOSED IDEA OF IMAGE ENCRYPTION USING FRFT AND PIXEL SRAMBLING

The use of fractional Fourier transform in the image encryption is been implemented in various paper and the pixel scrambling technique is also been developed. But the use of fractional Fourier transform with pixel scrambling technique is unique in a way that it increases the strength of the key by many times which makes the encryption technique stronger. In the proposed method an image is taken which will be used in the encryption will pass through the pixel scrambling block and resulted in an image which itself is encrypted image. Now the two dimensional fractional Fourier transform of this image is taken which will be final encrypted image. To get back the original image at the receiver side the reverse process took place.

Let $R_{n-1}(x,y)$ represent the primary normalized amplitude image to be encrypted , J denotes the pixel scrambling operation [18], which interchanges the pixels according to some random permutation, and the image can be retrieved by repositioning the disturbed image according to the special order. For encryption, the pixel scrambling is applied to the images $R_{n-1}(x,y)$, and then, the scrambled result J_{3n-1} $[R_{n-1}(x,y)]$ will pass through the FRT block as can be seen in Fig 2 and result in $R_n(x,y)$.

Fig 2 Schematic of image encryption

So the final image equation y the above will be

$$R_n(x,y)=F^{\beta}\cdot[F^{\alpha}.\{J_{3n-1}(R_{n-1}(x,y))\}] \quad (8)$$

Now from the Fig 3 as it can be seen that the input image $R_n(x,y)$ will pass through the FRT block followed by pixel decrypting block which will divide the image similarly and again reassemble the pixel in the same permutation as done earlier and resulted in the original image.

So the final image equation at the receiver side will be

$$R_{n-1}(x,y)=J_{3n-1}[F^{-\beta}\cdot\{F^{-\alpha}.R_n(x,y)\}] \quad (9)$$

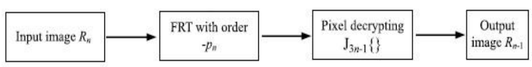

Fig 3 Schematic of single image decryption

V. SIMULATION RESULTS

Computer simulations are performed to verify the proposed encryption technique for image encryption and decryption using MATLAB. Image of college as seen in Fig 4, is serving as primary images to be encrypted with the size of 308x308 pixels.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Fig 4 Original Image

For pixel scrambling, the 308x308 image is divided in to the 14x14 subsections and considering these subsections as an image rearranged according to some permutation. Hence the resulted image after this can be seen in Fig 5.

Fig 5 Pixel scrambled image

Now the order (α, β) which is used in FRFT for the image encryption is as follow *(4.9, 2.4)*. So the image after encryption can be seen in Fig 6**.**

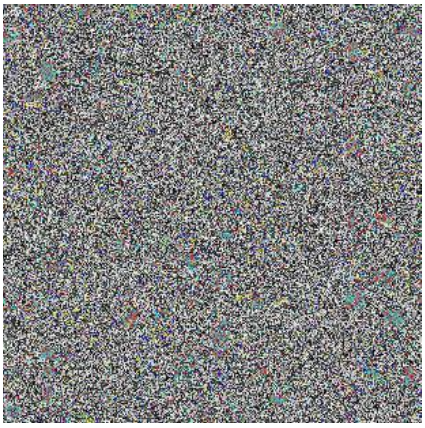

Fig 6 Encrypted image after applying FRFT

To recover back image order $(-\alpha, -\beta)$ of FRFT is (-4.9,-2.4). And hence the image which is decrypted but still the scrambled image can be seen in Fig 7.

Fig 7 Decrypted Images after applying the reverse process

Now to receive the original image back just applies the same pixel scrambling method which was used at the transmitter side. Hence the original image can be seen in Fig 8.

Fig 7 Decrypted Images after applying the reverse process

VI. CONCLUSION

In the proposed encryption method pixel scrambling and order of the fractional Fourier transform served as the key and makes the encryption very efficient. The proposed encryption and decryption is implemented on one image to check the algorithm.

REFERENCES

[1] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," J. Inst. Math. Appl., vol. 25, 1980, pp. 241–265
[2] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using fractional Fourier transform," Opt. Eng. 42, 1583–1588 (2003).
[3] C. C. Shih, "Fractionalization of Fourier transform," Opt. Commun., no. 118, Aug. 1, 1995, pp. 495–498.
[4] G.Unnikrishnan and K. Singh, " Random fractional Fourier domain encoding for optical security," Opt. Eng., vol. 39, 2000, pp. 2853–2859.
[5] Jun LANG , Ran TAO and Yue WANG, "The Generalized Weighted Fractional Fourier Transform and Its Application to Image

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Encryption ," Image and Signal Processing, 2009. CISP '09. 2nd International Congress, IEEE, 978-1-4244-4131-0
[6] Ran Tao, Yi Xin, and YueWang,"Image encryption based on random phase encoding in the fractional Fourier domain "Optical Express-2007,Vol. 15, No. 24
[7] R. Tao, J. Lang, Y. Wang. "Image encryption based on the multiple-parameter fractional Fourier transform," Opt. Lett. vol. 33, 2008, pp. 581-583.
[8] A. Sinha, K. Singh, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes," Opt. Eng. 44, 057001 (2005).
[9] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by random phas encoding in the fractional Fourier domain," Opt. Lett. 25, 887-889 (2000).
[10] N. K. Nishchal, G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption using a localized fractional Fourier transform," Opt. Eng. 42, 3566-3571, (2003).
[11] Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," Opt. Commun. 275, 324–329 (2007).
[12] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, 1995, pp. 767–769.
[13] G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. 30, 1306-1308 (2005).
[14] G. Situ and J. Zhang, "Position multiplexing for multiple-image encryption," J. Opt. A: Pure Appl. Opt. 8, 391 (2006).
[15] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay "The Fractional Fourier Transform with Applications in Optics and Signal Processing" New York: Wiley, 2000.
[16] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase-based encryption using fractional order Fourier domain random phase encoding: Error analysis," Opt.Eng. 43, 2266-2273 (2004).
[17] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J.Opt. Soc. Am. A 16, 1915 (1999).
[18] J. Zhao, H. Lu, X.S. Song, J.F. Li, and Y.H. Ma, " Image encryption based of multistage fractional Fourier transforms and pixel scrambling technique," Opt. Commun. 249, 493-499, (2005).
[19] B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption," Appl. Opt.39, 4117–4130 (2000).
[20] J. Hua, L. Liu, and G. Li, "Extended fractional Fourier transforms," J. Opt. Soc.Am. A 14, 3316-3322 (1997).
[21] A. W. Lohmann, "Image rotation, Wigner rotation, and the fractional Fourier transform," J. Opt. Soc. Am. A 10, 2181- (1993)