Fractional Fourier Transform based Key Exchange for Asymmetric Key Cryptography

ALOKA SINHA
Department of Physics,
IIT Delhi, Hauz Khas,
New Delhi, INDIA – 110016,

Abstract:- Recently several optical encryption techniques have been proposed for two-dimensional data. These techniques use random phase masks, jigsaw transforms, digital signatures, and linear transforms like the Fourier transforms, the fractional Fourier transform and the Fresnel transform. The strength of these encryption techniques is dependent on the size of the key but is strongly limited by the security linked with the exchange of the secret key. We propose a new technique, based on the Diffie-Hellman protocol, in which the key can be exchanged with high security. Fractional Fourier transforms have been used for the secure key transfer. Results of computer simulation are presented to verify the proposed idea and analyse the robustness of the proposed technique.

Key-Words:- Fractional Fourier Transform, Optical encryption, Public key encryption, Diffie-Hellman protocol, Fourier Transform.

1 Introduction

Information security is becoming more and more important with the progress in the exchange of data for electronic commerce. Optical information processing systems have attracted a lot of attention in recent times for information and data security applications because of their inherent parallelism and very high processing speed. Recently, a number of optical security algorithms and optical set ups have been proposed [1, 3-7]

A primary image encryption technique involves a process in which the primary image is encoded with two random phase masks. One mask is placed in the input plane and the other one is placed in the spatial frequency plane. This is known as the double random phase encoding system [1]. Fractional Fourier transforms (FRT) are being used extensively in the field of optical security [2]. Unnikrishnan *et al.* have used the random phase masks in the fractional Fourier domains to encrypt the images [3]. Sinha and Singh have proposed a new technique to encrypt an image by using the digital signature of the image [4]. A new technique based on the jigsaw transform has been recently proposed for image encryption [5]. Another new method of image encryption has been proposed using the random phase mask and the jigsaw encryption in the Fresnel domain [6]. A lens-less optical security system based on the computer generated phase only masks has also been proposed recently [7]. All of these techniques depend on the security of the secret key which has to be transmitted to the recipient for the decryption of the data. The inherent drawback of all these techniques is that they all require secure exchange of keys. Thus, however secure the encryption procedure maybe, they are still susceptible to the key being intercepted during the key transfer process. In this paper, we propose a secure method to exchange the secret keys (random phase mask) required for encryption. Fractional Fourier transform has been used to design an algorithm for the transfer of the key using the Diffie-Hellmann protocol [8].

FRT is the generalization of the conventional Fourier transform in the fractional order [2, 3]. The two-dimensional FRT of a function $f(x,y)$ with a separable kernel can be defined as

$$F^{\alpha_x\alpha_y}[f(x,y)](u,v)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}K_{\alpha_x\alpha_y}(x,y;u,v)f(x,y)dxdy \tag{1}$$

with the kernel

$$K_{\alpha_x\alpha_y}(x,y;u,v)=K_{\alpha_x}(x,u)K_{\alpha_y}(y,v) \tag{2}$$

where

$$K_{\alpha_x}(x,u)=\begin{cases}A_{\phi_x}\exp\left[i\pi\left(x^2\cot\phi_x-2xu\csc\phi_x+u^2\cot\phi_x\right)\right] \text{if } \alpha_x\neq n\pi,\\ \delta(x-u) \text{ if } \alpha_x=2n\pi,\\ \delta(x+u) \text{ if } \alpha_x=(2n+1)\pi,\end{cases} \tag{3}$$

and

$$A_{\phi_x}=\frac{\exp\left[-i\left(\pi\,\mathrm{sgn}(\phi_x)/4-\phi_x/2\right)\right]}{\sqrt{|\sin(\phi_x)|}}$$

where $\phi_x=\alpha_x\pi/2$ is the angle corresponding to the transform along the x-axis. The kernel along the y-axis $K_{\alpha_y}(y,v)$ can be obtained similarly by simply substituting y for x and v for u respectively. FRT will reduce to the conventional Fourier transform when $\alpha_x = \alpha_y = 1$.

The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976 [8]. The protocol allows two users to exchange a secret key over an insecure channel without any prior secrets. The protocol has two system parameters p and g. They are both public and may be used by all the users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p, which is capable of generating every element from 1 to p-1 when multiplied by itself a certain number of times, modulo the prime p.

2 The Proposed Technique

In the proposed technique, FRT, together with the Diffie-Hellmann protocol has been used for key exchange over insecure channels. Let us assume that two persons, A and B, wish to exchange a secret key. First, they agree on a common image (T) to begin with. This starting image is known publicly. Person A secretly chooses two numbers, n_{A1} and n_{A2}, that lie between (0, 1). Similarly, person B secretly chooses two numbers, n_{B1} and n_{B2}, that lie between (0, 1). Person A, then encrypts the image T using the fractional parameters $\{n_{A1}, n_{A2}\}$ to obtain

$$K_A=\mathrm{FRT}^{(n_{A1},n_{A2})}(T). \tag{4}$$

Similarly, person B encrypts the image T using fractional parameters $\{n_{B1}, n_{B2}\}$ to obtain

$$K_B=\mathrm{FRT}^{(n_{B1},n_{B2})}(T). \tag{5}$$

A and B now exchange the encoded images K_A and K_B over an insecure channel. Person A now takes the encrypted image of person B and further performs the FRT using the secret parameters $\{n_{A1}, n_{A2}\}$ to obtain

$$\begin{aligned}K_{AB}&=\mathrm{FRT}^{(n_{A1},n_{A2})}(K_B)\\&=\mathrm{FRT}^{(n_{A1},n_{A2})}\left(\mathrm{FRT}^{(n_{B1},n_{B2})}(T)\right)\\&=\mathrm{FRT}^{(n_{A1}+n_{B1},n_{A2}+n_{B2})}(T).\end{aligned} \tag{6}$$

Meanwhile, person B takes the encrypted image of person A and performs the FRT using his secret parameters $\{n_{B1}, n_{B2}\}$ to obtain

$$\begin{aligned}K_{BA}&=\mathrm{FRT}^{(n_{B1},n_{B2})}(K_B)\\&=\mathrm{FRT}^{(n_{B1},n_{B2})}\left(\mathrm{FRT}^{(n_{A1},n_{A2})}(T)\right)\\&=\mathrm{FRT}^{(n_{B1}+n_{A1},n_{B2}+n_{A2})}(T).\end{aligned} \tag{7}$$

From (6) and (7) it can be seen that $K_{AB} = K_{BA}$, i.e., person A and person B have exchanged their key secretly. The exchanged secret key is $K_{AB} = K_{BA}$, which is not known to an eavesdropper listening in on the insecure channel. The method of exchange of the secret key is highly secure because the exchanged secret key is unknown to either party, i.e., person A or person B prior to the start of the exchange procedure. It gets generated in the process of key exchange. The actual value of the secret key (random phase mask) depends on the random parameters $\{n_{A1}, n_{A2}\}$ chosen by person A and the random

parameters $\{n_{B1}, n_{B2}\}$ chosen by person B independently.

Computer simulations have been done in support of the proposed technique. The primary image chosen for simulations is of "Lena" of size 256 x 256 pixels as shown in Fig. 1. Let person A choose the fractional orders (0.24, 0.47) and person B choose the fractional parameters (0.82, 0.31). Figs. 2(a) and 2(b) represents the encrypted images K_A and K_B. Figs. 3(a) and 3(b) represent the images K_{AB} and K_{BA} after person A and person B have carried out the steps as outlined in Equation (6) and (7). This is the exchanged key. The problem of breaking into the proposed key exchange technique equates to finding K_{AB} (or K_{BA}) from the knowledge of K_A and K_B. That is, finding $\mathrm{FRT}^{(n_{A1}+n_{B1}, n_{A2}+n_{B2})}(\cdot)$ from $\mathrm{FRT}^{(n_{A1}, n_{A2})}(\cdot)$ and $\mathrm{FRT}^{(n_{B1}, n_{B2})}(\cdot)$.

3 Conclusions

In this paper, for the first time a secure key transfer protocol has been proposed that can be carried out optically. This is based on the FRT. The simulation results have shown the validity of this new algorithm. This secure key exchange algorithm in conjunction with the encryption algorithms can be used for a really secure and robust optical encryption technique.

References

[1] P.Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt.Lett.* **20(7),** 767-769 (1995).

[2] H.M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing* (Wiley, Chichester, 2001).

[3] G. Unnikrishnan, J. Joseph and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain," *Opt.Lett.*, **25**, 887-889 (2000).

[4] Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signatures," *Opt. Commun.*, **218**, 229-234 (2003).

[5] B. Hennelly and J.T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* **28** (4), 269- 271 (2003).

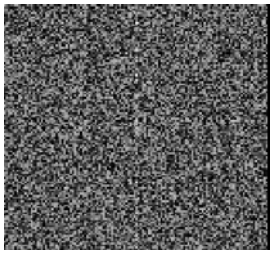
[6] B. M. Hennelly and J.T. Sheridan , "Random phase and jigsaw encryption in the Fresnel domain", *Opt. Eng.* , **43(10),** 2239-2249 (2004).

[7] G. Situ and Jingjuan Zhang, "A lensless optical security system based on computer – generated phase only masks", *Opt. Commun.*, **232**, 115-122(2004).

[8] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, **22** (6), 644, (1976).

Fig. 1 The original image of "Lena" of size 256x256 pixels for encryption.

(a)



(b)

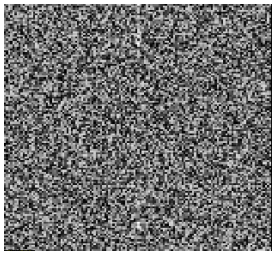
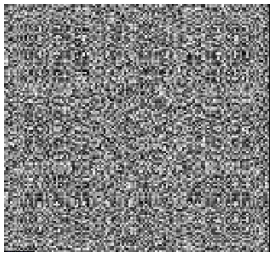


Fig. 2(a) and Fig. 2(b) represent the encrypted images K_A and K_B respectively.

(a)



(b)

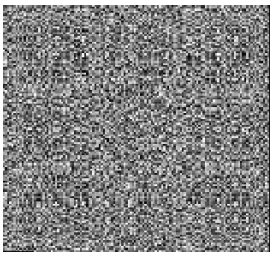


Fig. 3(a) and Fig. 3(b) represent the images K_{AB} and K_{BA} (the exchanged key) after person A and person B have carried out steps outlined in equations (6) and (7) respectively.