Fractional Fourier Transform Based Key Exchange for Optical Asymmetric Key Cryptography

ALOKA SINHA
Department of Physics,
Indian Institute of Technology, Delhi,
Hauz Khas-110016
INDIA
Email: aloka@physics.iitd.ac.in,

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. The Diffie-Hellman protocol allows two users to exchange a secret key over an insecure channel without any prior secrets. 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, cryptography

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 [1-6].

Cryptography is the study or science of secret writing, and a cryptosystem is a system in which either information is transformed into secret writing called ciphertext. Ciphertext is transformed back to the original information called plain text [7-9]. The transformation process just mentioned is controlled by what is called a key. Hence, to transform in either direction, the correct key is needed. Simmons classifies cryptosystems as either symmetric i.e., secret key or asymmetric i.e., public key.

In a secret-key cryptosystem, private conversation between two persons is established by using one key, known to both of them. This key is used for transformation to cipher text as well as transformation back to plain text. A disadvantage of this scheme is the fact that the secrecy of communication depends upon the trustworthiness or reliability of the two persons. Another disadvantage is that in a multi-channel scenario one has to keep a lot of keys secret to maintain private communication with different people.

In a public key cryptosystem, there exist two separate keys known as the enciphering key and the deciphering key. These keys decipher in such a way that, knowing one of the keys, it is computationally infeasible to determine the other key. This concept was first introduced in

1976 by Diffie-Hellman in their seminal paper [10].

The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976 [10]. 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*.

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 [11]. Unnikrishnan *et al.* have used the random phase masks in the fractional Fourier domains to encrypt the images [2]. Sinha and Singh have proposed a new technique to encrypt an image by using the digital signature of the image [3]. A new technique based on the jigsaw transform has been recently proposed for image encryption [4]. Another new method of image encryption has been proposed using the random phase mask and the jigsaw encryption in the Fresnel domain [5]. A lens-less optical security system based on the computer generated phase only masks has also been proposed recently [6]. 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. FRT has been used to design an algorithm for the transfer of the key using the DH protocol [10].

2 Fractional Fourier Transform

FRT is the generalization of the conventional Fourier transform in the fractional order [2, 11]. 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 $\alpha_x = \alpha_y = 1$.

3 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

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

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

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

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

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

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

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

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.

4 Simulation Results

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 $\mathrm{FRT}^{(n_{B1}, n_{B2})}(\cdot)$.

Let an error of Δn in the fractional order cause a large enough error between the actual key (K_{AB}) and the estimated key using the incorrect fractional parameters. In order for the hacker to determine the correct value of n_{A1}, it would require $(2/\Delta n)$ attempts, since n_{A1} can lie in the range (-1, 1). Independently, to determine the correct value of n_{A2}, it would require $(2/\Delta n)$ attempts. Since the correct *combination* of $\{n_{A1}, n_{A2}\}$ is required, the total number of times the hacker has to calculate the FRT will be $(2/\Delta n)\times(2/\Delta n) = (2/\Delta n)^2$. Let the computational requirement to calculate FRT be m. Then, the number of attempts to guess the correct key will be

$$N = m\left(\frac{2}{\Delta n}\right)^2 \quad (8)$$

The computational complexity, m, depends on the size of the image. We know that the computational complexity of FRT is proportional to FFT, which is, at best, O(N log N) where N is the length of the input. For 2D FFT, it will be O($N^2 \log N^2$). Thus, the number of attempts is very large and the method is highly robust to blind decryption.

The mean squared error (MSE) between the decrypted and the original image has also been evaluated to test the performance of the key exchange technique. The MSE is evaluated as a function of the errors in the decrypted fractional orders. If $o(i,j)$ and $r(i,j)$ denote the values of the original and the recovered image at the pixel (i,j), respectively, then the total MSE can be defined as follows:

$$MSE = \|r - o\|^2 = \frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|r(i,j) - o(i,j)\right|^2 \quad (9)$$

where $N \times N$ is the size of the images. In the MSE calculations, each of the results was averaged over 10 trials. We have plotted the MSE versus the error in the fractional order in Fig. 4. It can be seen from the figure that an error of $\Delta n > 0.05$ in the fractional order causes a very high MSE between the actual key (K_{AB}) and the estimated key using incorrect fractional parameters. For a typical image of size 256 x 256 and $\Delta n = 0.05$, the computational requirement is of the order of 10^9 and for an image of size 400 x 600, the computational requirement is of the order of 10^{10}.

5 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, which is an ideal candidate to be implemented optically. 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. Practical applications would include optical digital signature and secure communication over optical channels. This work may be further extended by developing an optical set-up to implement the proposed technique.

References

[1] P.Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, *Optics Letters* Vol.20,No.7, 1995, pp.767-769.

[2] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double random phase encoding in the fractional Fourier domain, *Optics Letters,* Vol.25, No.12, 2000,pp.887-889.

[3] Aloka Sinha ,Kehar Singh, "A technique for image encryption using digital signatures," *Optics Commun*ications, Vol. 218, No.4-6, 2003, pp. 229-234.

[4] B. M. Hennelly, J.T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Optics Letters,*Vol.28, No. 4, 2003, pp.269- 271.

[5] B. M. Hennelly, J.T. Sheridan , "Random phase and jigsaw encryption in the Fresnel domain", *Optical Engineering* , Vol.43, No.10**,** 2004,pp.2239-2249.

[6] G. Situ, J. Zhang, A lensless optical security system based on computer – generated phase only masks, *Optics Communications*, Vol.232, No.1-6, 2004, 115-122.

[7] B. Schneider, *Applied Cryptography*,John Wiley and Sons, 1996.

[8] Kun-Yuan Chao, Ja-Chen Lin, Fault-Tolerant and Non-Expanded Visual Cryptography for Color Images, *WSEAS Transaction on Information Science and Applications*, Vol. 3, No.11, 2006, pp 2184-2191.

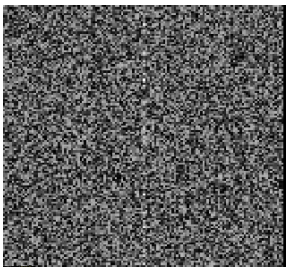
[9] B. Ontiveros, I. Soto, R. Carrasco, A New Cryptography Algorithm using Cab Curves and LDPC for Wireless Communication Systems, *WSEAS Transaction on Mathematics*, Vol. 6, No.2, 2007, pp. 422-425.

[10] W. Diffie, M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol.22, No**.** 6, 1976,644-654.

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

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

(a)



(b)

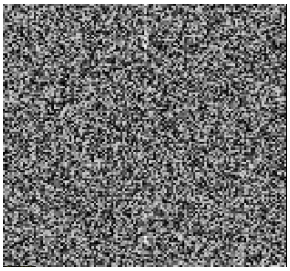
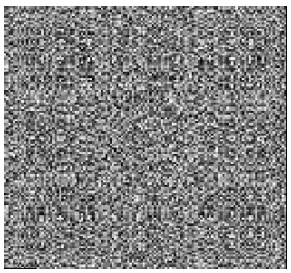


Fig. 2(a) and Fig. 2(b) represent the encrypted images K_A and K_B respectively.

(a)



(b)

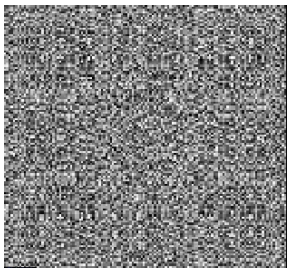


Fig. 3(a) and Fig. 3(b) represent the images K_{AB} and K_{BA} (the exchanged key) after person A and person B have carried out steps outlined in equations (6) and (7) respectively.

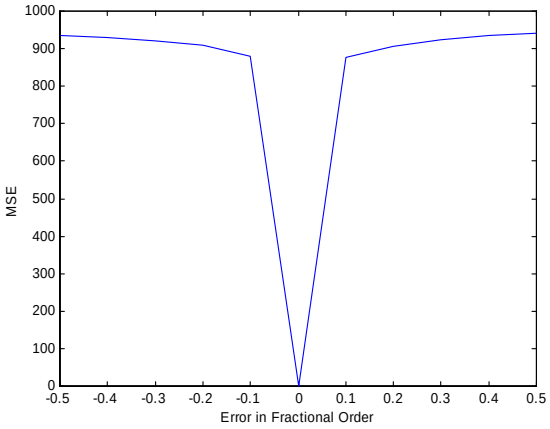


Fig. 4 MSE between the decrypted and the encrypted image as a function of the errors in the fractional parameters in FRT1.