Color Image Encryption and Decryption based on Jigsaw Transform Employed at the Input Plane of a Double Random Phase Encoding System

Ratheesh kumar M [1] Linslal C L [2] V P Mahadhevan Pillai [3] Sudheer Sreedhara Krishna [4]

Department of Optoelectronics
University of Kerala, Kariavattom
Thiruvananthapuram, Kerala, India 695581
ratheeshkumar.m@gmail.com

***Abstract*—In this paper we have demonstrated a simple and secure method to encrypt and decrypt a color image. In the proposed method, the color image is initially encrypted with jigsaw transform and followed by double random phase encryption. The jigsaw transform is employed at the input plane and random phase masks (RPMs) are placed at the Fourier planes. The jigsaw transformed image is Fourier transformed and multiplied with the RPM1 .Inverse transform of this image is performed and multiplied with the RPM2 gives the encrypted image. The jigsaw transform indices of the transformed image and the random phase code of the encrypted image form the keys for the successful retrieval of the data. Encrypting with this technique makes it almost impossible to retrieve the image without using both the right keys. Results of the computer simulation have been presented in support of the proposed idea. Mean square error (MSE) between the decrypted and the original image has also been calculated in support of the technique.**

Keywords- ***Double random phase encryption; Jigsaw transform; Mean square error(MSE) analysis.***

I. INTRODUCTION

In recent years, optical image encryption techniques have become very important in optical information processing. It has some attractive features such as fast computing and parallelism of optics which makes it very useful in the information security systems. A large number of information security systems based on optical techniques have been proposed to protect data from unauthorized use. A well-known technique for information encryption is the double random phase encoding technique proposed by Refregier and Javidi [1], which has been widely used and developed in recent years. This technique uses two statistically independent random phase masks(RPM) 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 domain [9, 10] has been presented by Unnikrishnan et al. [8] and later significant work has been done in this area by other researchers [11–20]. Optical encryption offers several image parameters, e.g. phase, amplitude, color, spatial frequency, polarization, etc., and can be exploited to perform a robust and highly secure encryption.

This paper reports a technique for the encryption and decryption of a color image using jigsaw transform and the random phase encryption method. Jigsaw transform is employed at the input plane and the random phase masks are placed at the Fourier planes. Jigsaw transformed image is Fourier transformed and multiplied with the first RPM .Inverse Fourier transform of this image performed and multiplied with the second RPM. This gives encrypted image.

The MATLAB 7.0 platform has been used to perform the simulations to demonstrate the proposed idea. It is shown that the decrypted image matches with the input image only when the correct keys are used during the process of decryption. To evaluate reliability of the technique, mean square error (MSE) between the decrypted and original image has been calculated.

II. ALGORITHM FOR ENCRYPTION AND DECRYPTION

Encryption process involves the following steps

- The real valued function f(x, y) to be encrypted is jigsaw transformed with some index'b'. [denoted as $J_b\{f(x, y)\}$].
- Fourier transform of the jigsaw transformed image is performed.
- The resultant image is multiplied with RPM, $R_1(u,v)$.
- The inverse transform of the product is performed.
- This image is multiplied with second RPM $R_2(x, y)$ and this gives the complete encrypted image.

Decryption process involves the following steps

- Encrypted image is multiplied with the conjugate of the RPM, $R_2(x, y)$.
- A Fourier transform is carried out.
- Resultant image is multiplied with the conjugate of RPM, $R_1(u, v)$.
- An inverse transform is performed.
- A jigsaw transforms with index –b is performed to get the original image f(x, y).

978-1-4244-7286-4/10/$26.00 ©2010 IEEE

III. DESCRIPTION OF THE METHOD

The proposed 4-f set up (fig.1) can be used to encrypt and decrypt a color image by using jigsaw transform and random phase masks. Let (x,y) and (u,v), denote, respectively the coordinates of input plane and the Fourier transform plane. For encryption, the input image pattern is jigsaw transformed to $J_b\{f(x,y)\}$ and its Fourier transform is performed. The resultant image is multiplied with the RPM, $R_1(u, v)$ at the Fourier plane. The inverse Fourier transform of this image is performed and multiplied with the RPM, $R_2(x, y)$.

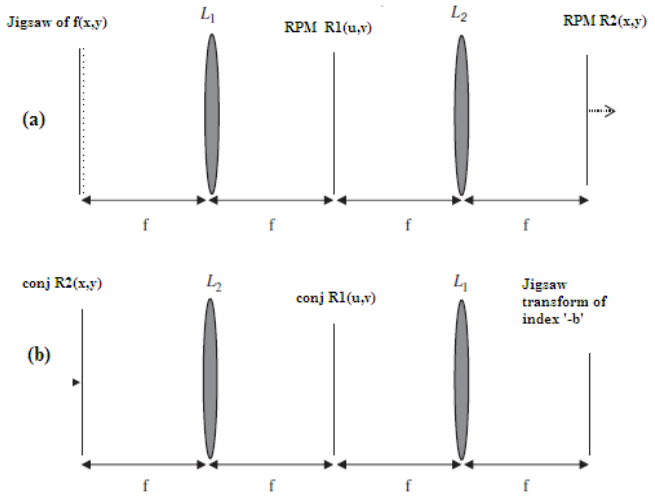

Fig.1 Proposed optical set-up for encryption and decryption. (a) Encryption (b) Decryption; $R_1(u, v)$, $R_2(x, y)$ are RPMs; L1 and L_2 are lenses.

The random phase functions $R_1(u,v)$, $R_2(x,y)$ and $J_b\{f(x,y)\}$ chosen to be statically independent. The functions $R_1(u,v)$and $R_2(x,y)$ are chosen to be the random phase functions and are denoted as $\exp[i\varphi_1(u,v)]$ and $\exp[i\varphi_2(x,y)]$ respectively, with phases uniformly distributed in the interval $[0, 2\pi]$.

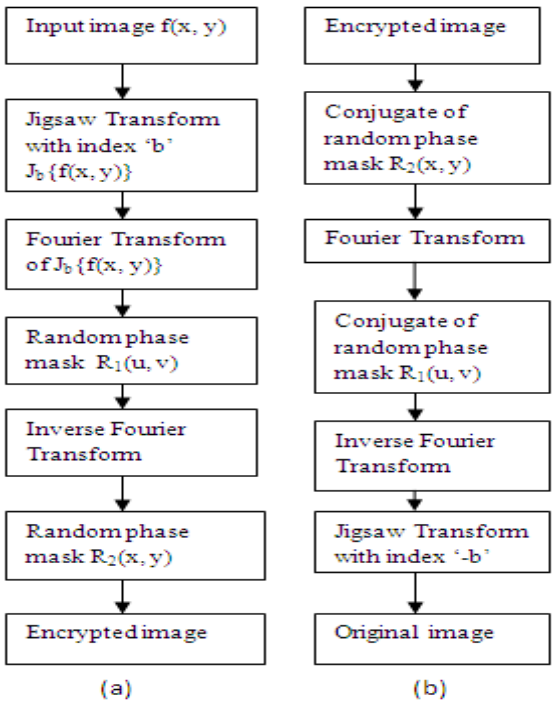

Fig.2 Flowchart of the (a) Encryption (b) Decryption

IV. COMPUTER SIMULATION AND RESULTS

The flowchart of the proposed technique is shown in Fig.2. A color image of size 256x256x3 pixels has been chosen for the study. The MATLAB 7.0 platform has been used for the simulations and demonstration of the proposed idea. To evaluate reliability of the technique, mean square error analysis (MSE) between the decrypted and original image has been done. The computer simulation of the proposed method is shown in Fig.3.

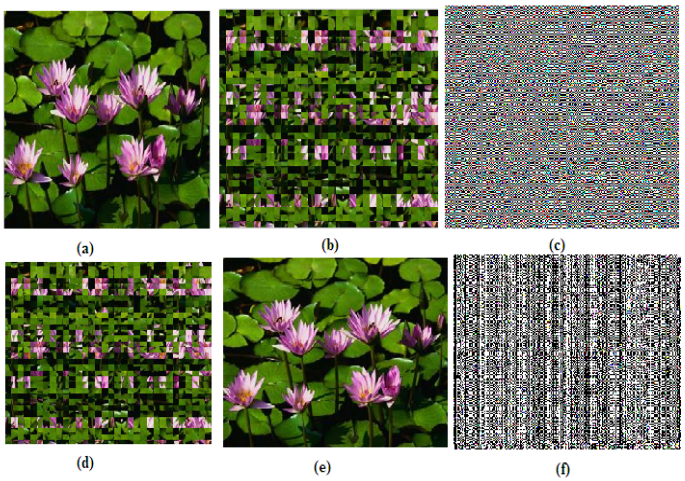

Fig.3 Computer simulation of the encryption and decryption (a) Input color image (b)Jigsaw transformed image(c) Encrypted image using random phase mask (d) Image obtained after conjugate of the RPM is applied. (e) Decrypted image with correct keys (f) Decrypted image with wrong keys.

A color image is used as the input image to the encoding system as in Fig.3(a). Jigsaw transformed image is shown in Fig.3(b). Fourier transformed and random phase encryted image is shown in Fig.3(c). It is shown that the decrypted image matches with the input image only when the correct keys are used during the process of decryption.

In order to study the the robustness of the proposed method mean square error analysis method is used.

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\times\sum_{j=1}^{N}|C(i,j) - f(i,j)|^2$$

In the above expression C (i, j) and f (i, j) represents the encrpted and input image respectively. The MSE between input image and decrypted image with the correct key has been found to be negligible (10^{-27}).

V. CONCLUSION

This paper reports a new method to realize the color image encryption based on jigsaw transform and double random phase encryption technique. The jigsaw transform index and the random phase code of the encrypted image form the keys for the successful retrieval of the image. It is shown that the decrypted image matches with the input image only when the correct keys are used during the process of decryption. Computer simulation results have verified the validity and efficiency of the proposed technique. Mean square error (MSE) between the decrypted and the original image has also been calculated in the support of the proposal.

REFERENCES

[1] Javidi B, editor. Optical and digital techniques for information security. NewYork: Springer; 2004.

[2] Matoba O, Javidi B. Encrypted optical memory system using three-dimensional Keys in the Fresnel domain. Opt Lett 1999; 24:762–4.

[3] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett 2000; 25:887–9.

[4] Joshi Madhusudan, Chandrashakher, Singh K. Color image encryption and decryption using fractional Fourier transform. Opt Commun 2007; 279:35–42.

[5] Liu Z-G, Ahmad MA, Liu S. Image encryption scheme based on the commutation and anti-commutation rules. Opt Commun 2007; 279:285–90.

[6] Singh Madan, Kumar Arvind. Optical encryption and decryption using a sandwich random phase diffuser in the Fourier plane. Opt Eng 2007; 46: 055201-1–6.

[7] Nishchal NK, Joseph J, Singh K. Fully phase encryption using fractional Fourier transforms. Opt Eng 2003; 42:1583–8.

[8] Unnikrishanan G, Joseph J, Singh K. Double random fractional Fourier domain encoding for optical security. Opt Eng 2000; 39:2853–9.

[9] Liu Z-G, Liu S. Double image encryption based on iterative fractional Fourier transform. Opt Commun 2007; 275:324–9.

[10] Singh N, Sinha A. Optical image encryption using fractional Fourier transform and chaos. Opt Laser Eng 2008; 46:117–23.

[11] Liu S, Mi Q, Zhu B. Optical image encryption with multistage and multichannel fractional Fourier domain. Opt Lett 2001; 26:1242–4.

[12] Jin W, Yan C. Optical image encryption based on multichannel fractional Fourier transform and double random phase encoding technique. Optik 2007; 118:38–41.

[13] Nishchal NK, Unnikrishnan G, Joseph J, Singh K. Optical encryption using cascaded extended fractional Fourier transform. Opt Mem Neural Networks 2003; 12:139–45.

[14] Kishk S, Javidi B. Information hiding technique with double phase encoding. Appl Opt 2002; 12:5462–70.

[15] Shi Y, Situ G, Zhang J. Multiple image hiding in the Fresnel domain. Opt Lett 2007; 13:1914–6.

[16] Singh M, Kumar Arvind, Singh K. Multiplexing in optical encryption by using an aperture system and a rotating sandwich random phase diffuser in the Fourier plane. Opt Laser Eng 2008; 46:243–51.

[17] Su W-C, Lin C-H. Three dimensional shifting selectivity of decryption phase mask in a double random phase encoding holographic memory. Opt Commun 2004; 241:29–41.

[18] John R, Joseph J, Singh K. Phase based content addressable holographic data storage with security. J Opt A: Pure Appl Opt 2005; 7:123–8.

[19] Dong L, Xin Z, Ding-Fu Z, Da-Hai L. Study on the influence of the error on the deciphered image in the double random phase encryption system by applying affine cryptography. J Mod Opt 2008; 55:167–76.

[20] Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 2003; 28:269–71.