Optics and Lasers in Engineering 46 (2008) 763–768

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

journal homepage: www.elsevier.com/locate/optlaseng

# Optical security system using jigsaw transforms of the second random phase mask and the encrypted image in a double random phase encoding system

Madan Singh [a], Arvind Kumar [b,*], Kehar Singh [b]

[a] Instruments Design, Development, and Facilities Center, Staff Road, Ambala, Haryana 133 001, India
[b] Department of Physics, Indian Institute of Technology Delhi, New Delhi 110 016, India

ARTICLE INFO

*Article history:*
Received 29 December 2007
Received in revised form
13 March 2008
Accepted 25 April 2008
Available online 24 June 2008

*Keywords:*
Optical encryption
Jigsaw transform
Data security

ABSTRACT

In this paper, we have described a simple and secure double random phase encoding and decoding system to encrypt and decrypt a two-dimensional gray scale image. We have used jigsaw transforms of the second random phase mask and the encrypted image. The random phase mask placed in the Fourier plane is broken into independent non-overlapping segments by applying the jigsaw transform. To make the system more secure, a jigsaw transform on the encrypted image is also carried out. The encrypted image is also broken into independent non-overlapping segments. The jigsaw transform indices of random phase code and 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 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.



## 1. Introduction

Successful encoding and decoding of data in high-capacity storage systems is one of the challenging tasks in order to meet the users' requirements. The double random phase encoding technique [1] has been investigated in the past enabling one to encrypt a primary image into stationary white noise. The encoding is done by use of two statistically independent random phase codes in the input and the Fourier planes with their phases uniformly distributed in the interval $[0, 2\pi]$. Subsequently, various techniques [2–5] have been proposed to encrypt and decrypt the images/data. Recently, a highly secure encryption and decryption system [6] has been investigated using a sandwich diffuser made with two normal speckle patterns in the Fourier plane. Fractional Fourier transform (FrFT) geometry has been used extensively [3,4,7–10] for secure encryption and decryption of the images.

Image encryption technique algorithms that employ multi-channel FrFT domain filtering architecture [11,12] have also been presented. Nishchal et al. [13] have investigated an optical encryption system using cascaded extended FrFT. Double random phase encoding has been used as an information-hiding technique [14,15]. Multiplexing in optical encryption of two-dimensional images, by using apertures and rotation of one of the constituent phase diffusers of a sandwich phase diffuser in the Fourier plane have been investigated by Singh et al. [16].

The effects of three-dimensional shifting selectivity of volume hologram based on random phase encoding with ground glass have also been investigated [17]. John et al. [18] have described a phase-image-based content-addressable holographic data storage with security using random phase in the Fresnel domain. A double random phase encryption technique using affine cryptography [19] has been investigated, in which a study of the influence of key error on the deciphered image has been carried out.

Hennelly and Sheridan [20] have proposed a system to encrypt and decrypt a two-dimensional image using a random shifting, or jigsaw algorithm. To increase the key size a technique has also been developed to encrypt the image by using jigsaw transform and a localized FrFT [21]. An encryption and decryption method [22] has been investigated in which the input image is broken up into the bit planes. In view of the importance of the subject, researches on encryption continue unabated [23–29]. Recently, a possibility of known-plaintext attack on an optical encryption scheme based on double random phase key has been investigated [30], compelling the scientific community to investigate encryption systems to make them more secure. However, it is not desirable to change the input image/data in any form. Instead, the encoding mask and the encrypted image can be manipulated in any way without disturbing the input image.

In this paper, we have presented the results of secure encryption and decryption of a two-dimensional gray scale image

* Corresponding author. Tel.: +91 011 26596547.
*E-mail address:* arvindk_542005@yahoo.co.in (A. Kumar).

0143-8166/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlaseng.2008.04.021

by using the jigsaw transform of the random phase mask (RPM) placed at the Fourier plane as well as the jigsaw transform of the encrypted image. Here, the jigsaw transform indices of the random phase code and the encrypted image act as the keys for the successful retrieval of the input image. Results of 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.

## 2. Algorithm for encryption and decryption

The encryption process involves the following steps:

1. The real-valued input function $f(x, y)$ to be encrypted is multiplied by a RPM $R_1(x, y)$.
2. A Fourier transform of the product is performed.
3. An RPM $R_2(u, v)$, jigsaw transformed with some index 'b' [denoted as $J_b\{R_2(u, v)\}$] is placed in the Fourier transform plane.
4. $J_b\{R_2(u, v)\}$ is multiplied by the Fourier transform of the product of the input function $f(x, y)$ and the RPM $R_1(x, y)$.
5. A Fourier transform of the resultant function is performed to obtain the encrypted image $\psi(x, y)$.
6. A jigsaw transform is performed on the encrypted image $\psi(x, y)$ with some index 'c' to get the jigsaw transformed encrypted image i.e. $J_c\{\psi(x, y)\}$.

The decryption process involves the following steps:

1. A jigsaw transform with index '−c' is performed on $J_c\{\psi(x, y)\}$ to obtain the encrypted image $\psi(x, y)$.
2. An inverse Fourier transform of $\psi(x, y)$ is then carried out.
3. A conjugate of $J_b\{R_2(u, v)\}$ is obtained.
4. The inverse Fourier transform of $\psi(x, y)$ is multiplied with the conjugate of $J_b\{R_2(u, v)\}$.
5. A Fourier transform of the resultant function is performed to obtain the original image $f(x, y)$ denoted by $f_d(x, y)$.

## 3. Description of the method

The proposed 4-f set-up (Fig. 1) may be used to encrypt and decrypt a two-dimensional gray scale image, by using jigsaw transforms of the mask placed in the Fourier plane and the encrypted image in a double random phase encoding system. Let $(x, y)$ and $(u, v)$ denote, respectively, the coordinates in the object and the Fourier transform plane. For encryption, the object pattern $f(x, y)$ is multiplied by a RPM $R_1(x, y)$ placed in the input plane. The Fourier transform of the product of $R_1(x, y)$ is passed through the jiggled version $J_b\{R_2(u, v)\}$ of the RPM $R_2(u, v)$. Here, it should be noted that the jigsaw transform of $R_2(u, v)$ is also a random function.

The random phase functions $R_1(x, y)$, $R_2(u, v)$ and $J_b\{R_2(u, v)\}$ are chosen to be statistically independent. $R_1(x, y)$ and $R_2(u, v)$ are denoted as $\exp[i\phi_1(x, y)]$ and $\exp[i\phi_2(u, v)]$, respectively, with phases uniformly distributed in the interval $[0, 2\pi]$. The encrypted image may be expressed by

$$\Psi(x, y) = \mathrm{FT}[\{\mathrm{FT}[f(x, y)R_1(x, y)]\}\{J_b\{R_2(u, v)\}] \quad (1)$$

The encrypted image $\psi(x, y)$ is also jigsaw transformed and denoted as $J_c\{\psi(x, y)\}$.

A process reverse of encryption is followed to get the decrypted image. First, we obtain the original encrypted image $\psi(x, y)$ after applying the jigsaw transform $J_{-c}\{\psi(x, y)\}$ on the jiggled encrypted image. The decrypted image may be expressed as

$$f_{1d}(x, y) = \mathrm{FT}\{\mathrm{FT}[\Psi(x, y)][\mathrm{Conj}[J_b\{R_2(u, v)\}]]\} \quad (2)$$

## 4. Computer simulation results and discussion

The flowchart of the proposed technique is shown in Fig. 2. A gray scale image 'Lena' of size $256 \times 256$ pixels (Fig. 3(a)) has been chosen for the study. Encryption and decryption were then performed as per the steps in Section 2/flowchart (Fig. 2). For obtaining jigsaw of $R_2(u, v)$, it is broken into 256 subsections each

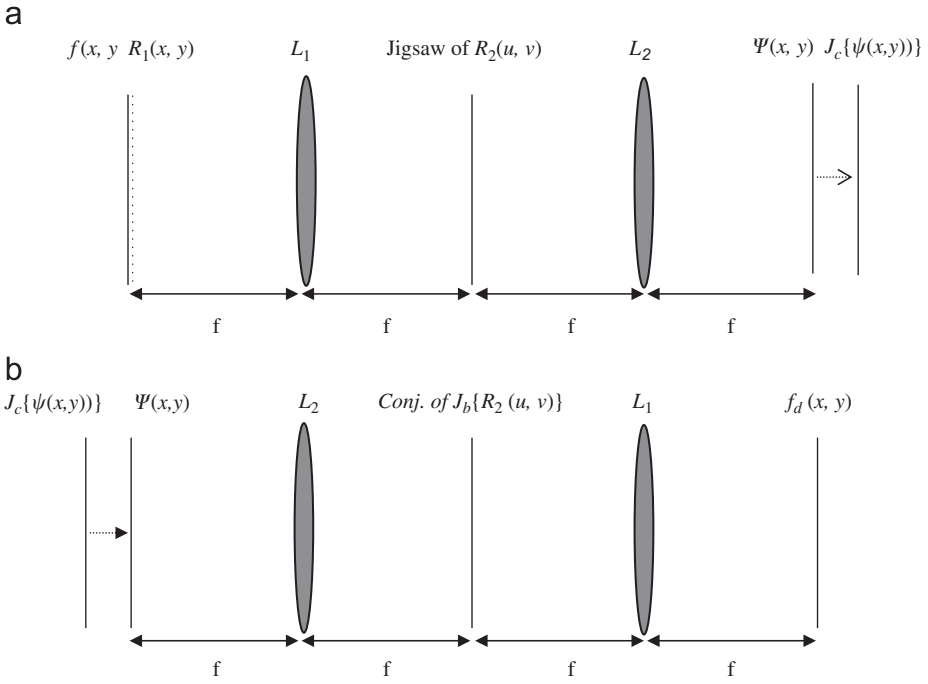


**Fig. 1.** Proposed optical set-up for the encryption and decryption: (a) encryption, (b) decryption; $R_1(x, y)$ and $R_2(u, v)$, RPMs; $J_b\{R_2(u, v)\}$, jigsaw transform of RPM with index 'b'; $L_1$, $L_2$, lenses; $f(x, y)$, input image; $\Psi(x, y)$, encrypted image; $J_c\{\psi(x, y)\}$, jigsaw transform of encrypted image with index 'c'; $f_d(x, y)$, decrypted image.