Optics and Laser Technology 95 (2017) 51–55

Contents lists available at ScienceDirect

Optics and Laser Technology

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

# Optical image encryption using Kronecker product and hybrid phase masks

Ravi Kumar, Basanta Bhaduri *

*Optical Imaging and Image Processing Laboratory, Department of Applied Physics, Indian Institute of Technology (Indian School of Mines) Dhanbad, Jharkhand 826004, India*

ARTICLE INFO

*Article history:*
Received 5 October 2016
Accepted 25 March 2017

*Keywords:*
Kronecker product
Fresnel propagation
Image encryption
Information security

ABSTRACT

In this paper, we propose a new technique for security enhancement in optical image encryption system. In this technique we have used the Kronecker product of two random matrices along with the double random phase encoding (DRPE) scheme in the Fresnel domain for optical image encryption. The phase masks used here are different than the random masks used in conventional DRPE scheme. These hybrid phase masks are generated by using the combination of random phase masks and a secondary image. For encryption, the input image is first randomized and then the DRPE in the Fresnel domain is performed using the hybrid phase masks. Secondly, the Kronecker product of two random matrices is multiplied with the DRPE output to get the final encoded image for transmission. The proposed technique consists of more unknown keys for enhanced security and robust against various attacks. The simulation results along with effects under various attacks are presented in support of the proposed technique.



## 1. Introduction

The advancements in communication technology have prompted new challenges for the security and privacy for image and data transmission. Much research efforts in the direction of development of secure and reliable systems for the information transmission have been initiated. As a result, a large number of encryption techniques have been proposed including optical technology. Due to its unique advantages of parallel processing of two dimensional (2D) image data and capability of hiding data in different dimensions, optical technology is better compared to its electronic counterpart for securing information [1,2]. Many optical encryption techniques have been developed in the past few years [3–23], but the double random phase encoding (DRPE) technique proposed by Réfrégier and Javidi in 1995 [3] is probably the most effective optical encryption technique which has changed the face of this field. In DRPE, the two random phase masks are used to encrypt the primary image using two Fourier transforms [3]. Other methods based on the DRPE architecture are also developed using different transforms such as Fresnel transform [4,5], fractional Fourier transform [6,7] and gyrator transform [8,9]. However, the conventional DRPE technique has some shortcomings (its linearity and symmetry) [10] and can be attacked with some particular methods such as known-plaintext attack (KPA) [11] and chosen cipher-text attack (CPA) [12]. To overcome this problem and enhance the security of the optical system, many alternate techniques such as digital optical stream cipher [13], optical XOR image encryption [14], phase shifting encoding [15], polarization encoding [16,17] are introduced. Recently, image encryption method based on multi-parameter fractional Fourier transform (MPFRFT) is also reported [18,19]. Various other optical techniques for color image encryption are further demonstrated based on DRPE [20,21] and holography, including encryption using wavelength multiplexing [22], lens-less Fresnel transform holograms [23], multidimensional encryption [24], and pure intensity random coding [25].

In this paper, we propose a new technique to enhance the security in traditional DRPE technique by using the Kronecker product (KP) of two random matrices [26–29]. The phase masks used in the proposed technique are different from the random masks used in the conventional DRPE scheme as they are generated by using a secondary image. These hybrid phase masks are generated from the angle of Fourier transform of the product of conventional random phase masks with the secondary image. On the other hand, the two random matrices were used to get the KP of particular order which may have different order [28]. In the proposed method, the image to be encrypted is first randomized and then the DRPE in the Fresnel domain using the hybrid phase masks is performed. After getting the encrypted image from DPRE, it is further multiplied with KP of two random matrices to get the final encoded image for transmission. The proposed technique provides a large number of security keys for optical image encryption which

* Corresponding author.
*E-mail address:* basanta.ism@gmail.com (B. Bhaduri).

http://dx.doi.org/10.1016/j.optlastec.2017.03.041
0030-3992/

includes two hybrid phase masks, distances of Fresnel propagation, along with the randomization operator and the KP of two random matrices. The simulation result depicts the efficiency of the proposed technique and the improvement of security in the system. The proposed technique is also robust to various attacks such noise, occlusion and known-plaintext.

## 2. Theoretical analysis

### 2.1. Fresnel domain DRPE

In our study, we have used the DRPE scheme in the Fresnel domain. The output image after the DRPE can be written as [5],

$$E(\alpha,\beta) = FrT_{d_1}\{FrT_{d_2}\{f(x,y)\cdot\exp[i\Phi(x,y)]\}.\exp[i\Psi(u,v)]\} \quad (1)$$

where $FrT_{d1,2}$ are the Fresnel propagations with distances $d_1$ and $d_2$, respectively, and $\phi(x, y)$ and $\psi(u, v)$ are the random distributions in the range [0,1].

### 2.2. Randomization operator

The randomization operator changes the order of the position of the pixels of an image randomly along a specific dimension [30] and the image becomes scrambled after the operation. The operator holds the pixel locations of image and shakes them in a particular dimension, so that the pixels get shuffled in that dimension only (along either rows or columns) [30].

### 2.3. Hybrid phase mask

The hybrid phase masks are generated using the random phase masks, $P_1$ and $P_2$ in the range [0,1], and the secondary image, $S(x, y)$. $P_1$ or $P_2$ is first multiplied with $S(x, y)$ and the resulting product is then Fourier transformed (FT). The argument of the FT i.e. the phase part of the transformed output is the hybrid phase mask, $M_1$ or $M_2$, respectively as follows,

$$M_{1,2} = Arg\{FT[S(x,y)\cdot P_{1,2}]\} \quad (2)$$

where *FT* is the Fourier transform, *Arg* is the argument of the FT, and $P_{1,2}$ denote the conventional random phase masks.

### 2.4. Kronecker product (KP) of two random matrices

The *KP* of two random matrices A and B is denoted as *Kron*(A, B) or $A \otimes B$ [26,27]. Let $A = [a_{ij}] \in R_{m,n}$ and $B = [b_{ij}] \in R_{p,q}$ where R is set of random numbers, *i, j* are the integers which denote the components of the matrices, *m, n* and *p, q* are the order of matrices A and B, respectively. The KP of A and B is then given by [27]:

$$Kron(A,B) = A\otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \in R_{mp,nq}. \quad (3)$$

For example, if we have A of order $32 \times 32$ and B of $8 \times 8$, then the KP of these two matrices has the order of $256 \times 256$.

Because of several unique properties of the KP [28], it has many applications in various scientific fields like signal processing, image processing, computer vision, linear system, quantum computing etc. [29,31,32]. The KP along with the singular value decomposition (SVD) approximations [33] has been used to develop fast algorithms for image restoration. Further, the KP of two matrices A and B can be computed optically using multiplex imaging setup [34] or holographic parallel processor setup [35].

## 3. Proposed technique

### 3.1. Encoding

The encoding process consists the following steps:

#### 3.1.1. Image randomization

In this step we randomize the primary input image $f(x, y)$ having dimension of $N \times N$ pixel$^2$ to get the $I(x', y')$ as follows [30]:

$$I(x',y') = R\{f(x,y)\}. \quad (4)$$

where, R{.} is the randomization operator.

#### 3.1.2. Fresnel domain DRPE

In this step, we perform the DRPE technique in the Fresnel domain considering $I(x', y')$ as primary image. The two hybrid phase masks, $M_1$ and $M_2$ are used in the encryption process instead of the random phase masks. At the output plane of DRPE, we get the encrypted image, $E(\alpha, \beta)$ as:

$$E(\alpha,\beta) = FrT_{d2}\{FrT_{d1}[I(x',y')\cdot M_1]\cdot M_2\} \quad (5)$$

where $d_1$ and $d_2$ are the propagation distances.

#### 3.1.3. Kronecker product

In the final step, the encrypted image $E(\alpha, \beta)$ is further multiplied with the Kronecker product of two random matrices, A and B, to get the final encoded image, $E'(\alpha, \beta)$ as:

$$E'(\alpha,\beta) = E(\alpha,\beta)\cdot Kron(A,B) \quad (6)$$

### 3.2. Decoding

The decoding process follows the steps given below:

a. First, the encoded image is multiplied with the inverse KP of matrices A and B as:

$$E''(\alpha,\beta) = E'(\alpha,\beta)\cdot Inv\{Kron(A,B)\}. \quad (7)$$

b. $E''(\alpha, \beta)$ is then decrypted using the DRPE technique using complex conjugate of $M_1$ and $M_2$ as:

$$I'(x',y') = IFrT_{d2}\{IFrT_{d1}[E''(\alpha,\beta)]\cdot M_2^*\}\cdot M_1^*. \quad (8)$$

where $IFrT_d$ is the inverse Fresnel propagation of distance $d$ and '$*$' denotes the complex conjugate.

c. Finally, the de-randomization is performed on $I'(x', y')$ to get the final decoded image, $f'(x, y)$.

The block diagram for the proposed technique is show in Fig. 1.

## 4. Results and discussion

### 4.1. Encryption results and key sensitivity analysis

We have implemented the numerical simulation of the proposed technique using MATLAB™ and carried out the effect of the keys on security. Fig. 2(a) shows the cameraman image used as the primary image. The secondary image used to generate the hybrid phase masks are shown in Fig. 2(b) whereas Fig. 2 (c) and (d) show the hybrid phase masks. Fig. 2(e) is the input to the DRPE system after randomizing the primary image shown in Fig. 2(a), and the Kronecker product matrix used for the final encoding is shown in Fig. 2(f). Fig. 2(g) shows the output of the DRPE system and Fig. 2(h) shows the final encoded image, $E'(\alpha, \beta)$, after multiplication with Fig. 2(f) for transmission.

We have decoded the final encoded image, $E'(\alpha, \beta)$ to check the correctness of the technique. Fig. 3 shows the decoding results