Optics & Laser Technology 60 (2014) 1–7

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon

Isha Mehra, Naveen K. Nishchal *

Department of Physics, Indian Institute of Technology Patna Patliputra Colony, Patna 800013, India

ARTICLE INFO

Article history:
Received 24 October 2013
Received in revised form
16 December 2013
Accepted 26 December 2013
Available online 16 January 2014

Keywords:
Image processing
Image encryption
Asymmetric cryptosystem

ABSTRACT

In this paper, a novel optical encryption technique based on two beam interference principle and phase truncation approach is presented. The proposed scheme is compact, highly secure, and suitable for securing multiple images. Simulation results with three different images have been presented. The first two images to be encrypted are encoded into two parts. One is phase-only distribution and other is amplitude mask. The amplitude masks are preserved as decryption keys while phase distribution is used as encryption keys in order to encrypt the third image using phase-truncation approach. The proposed scheme offers higher level of security as it resists the specific attack on asymmetric cryptosystem and is robust against occlusion attack. Also, detailed study has been carried out employing keys which are dependent on and independent of the input image.

1. Introduction

Optical image encryption is a significant research field of information processing because of parallel processing and multi-dimensional nature. The double random phase encoding (*DRPE*) technique is the basic optical encryption scheme, which encodes the phase of the optical wave into a random noise [1,2]. Apart from *DRPE*, different methods based on digital holography [3], polarization [4,5] and interference [6] have also been proposed to enhance the level of information security. Various methods in different optical domains have also been proposed for a secured *DRPE* scheme [7–9]. However, due to linear nature such cryptosystems are often not highly secure. This is because the keys used for encryption are identical to the decryption keys. Also, it is found to be vulnerable against various attacks because of inherent linearity [10]. To overcome such issues, asymmetric cryptosystem has been proposed [11–15]. Such kind of cryptosystem is one of the important tools, which introduces non-linearity and thus makes the system more secure.

Any optical security system cannot be completely secure unless it resists various types of attacks [16–26]. Gopinathan et al. [17] used simulated annealing heuristic algorithm to generate the keys for image decryption. A special attack on phase truncation based encryption has been proposed [20]. This attack is only valid if encryption keys are considered as public keys. Zhang et al. [25] proposed ciphertext-only attack on joint transform correlator (*JTC*) encryption scheme. Recently, we studied hybrid attack on *JTC* architecture with amplitude- and phase-truncation approach [26]. Most of the existing attacks are possible because of the uses of phase retrieval algorithm, such as, Gerchberg–Saxton algorithm [27,28].

In most of the communication techniques, there is a requirement for several users to share the common information simultaneously and also at higher speed. Multiple image encryption schemes could be the potential solution to such requirement. Generally, in multiple image encryptions, two or more images are encoded into a single image using digital [29–34]. Apart from digital means, there are many encryption techniques that have been experimentally demonstrated [35–37]. The drawback which often arises in multiple image encryption schemes is the system's complexity and high computational time. Wang and Zhao [32] reported multiple image encryption method based on Fourier domain nonlinear operations. They designed an encryption unit suitable for securing a single image. For securing multiple images, cascaded encryption units could be employed, which will enhance the computational cost; whether it is implemented digitally or optically. In this paper, we propose a novel optical encryption method using the two beam interference principle and amplitude- and phase truncation approach. The proposed scheme presents an improvement over the method reported by Wang and Zhao [32] in a way that one encryption unit encrypts two different images simultaneously. This means that in Ref. [32], if $n+1$ ($+1$ is for 1st image) images will be encrypted, then by compactness of our scheme $2n+1$ images will be encrypted. Also, instead of Fourier domain, fractional Fourier transform (*FRT*) domain has been used, which not only enhances the key space, but also plays a significant

* Corresponding author: Tel.: +91 612 255 2027; fax: +91 612 227 7383.
E-mail address: nkn@iitp.ac.in (N.K. Nishchal).

0030-3992/$ - see front matter © 2014 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.12.020

role in making the encryption unit compact. We present simulation results with three different images. The proposed encryption unit can also be cascaded in order to secure a large number of images/data.

2. Principle

2.1. Image encryption scheme

The proposed encryption process is shown in Fig. 1(a). Let $f_1(x_1,y_1)$ represent the first image to be encrypted. This input image is encoded into two masks; amplitude mask and phase mask [38]. The complex function can be constructed using an *RPM*,

$$f'(x_1,y_1)=\sqrt{f_1(x_1,y_1)}\exp[i2\pi\phi(x_1,y_1)] \tag{1}$$

where $\varphi(x_1,y_1)$ is random distribution between 0 and 1. This complex distribution can be expressed as the interference of phase mask R_1 and amplitude mask M_1.

$$f'(x_1,y_1)=\exp[iR_1(x,y)]*h_1(x,y,l)+M_1*h_1(x,y,l) \tag{2}$$

where

$$h_1(x,y,l)=\frac{\exp[i2\pi l/\lambda)}{il\lambda}\exp\left[\frac{i\pi}{\lambda l}(x^2+y^2)\right] \tag{3}$$

is the point pulse function of the Fresnel transform. λ is wavelength of the incident light. From Eq. (2) we can write

$$\exp[iR_1(x,y)]+M_1=\Im^{-\alpha}\left\{\frac{\Im^{\alpha}[f'(x_1,y_1)]}{\Im^{\alpha}[h_1(x,y,l)]}\right\} \tag{4}$$

where $\Im^{\alpha}\{..\}$ denote *FRT* of order alpha. Consider

$$\exp[iR_1(x,y)]+M_1=D \tag{5}$$

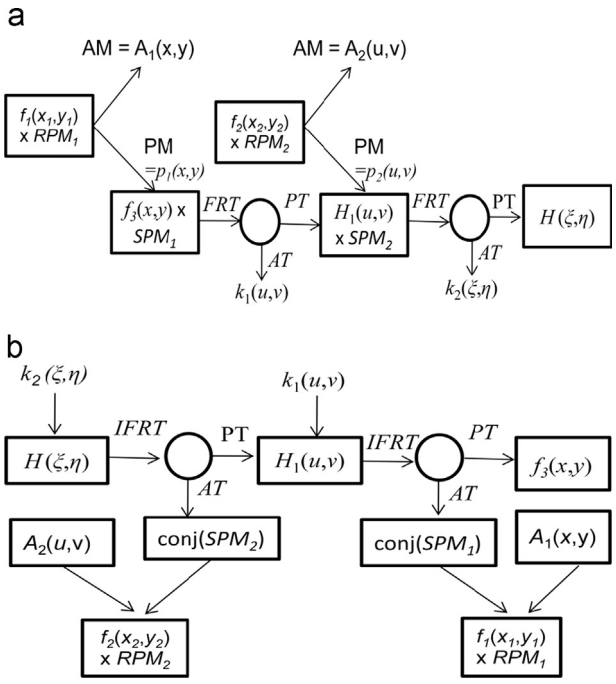

Fig. 1. Block diagrams for (a) image encryption, where three images $f_1(x_1,y_1)$, $f_2(x_2,y_2)$ and $f_3(x,y)$ are used. The first two images $f_1(x_1,y_1)$ and $f_2(x_2,y_2)$ to be encrypted are encoded into two parts. One is phase-only distribution and other is amplitude mask. The amplitude masks are preserved as decryption keys while phase distribution is used as encryption keys in order to encrypt the third image using phase-truncation approach, (b) image decryption using all valid keys.

On solving Eq. (5), phase mask R_1 and amplitude mask M_1 can be written as

$$M_1=\mathrm{Re}(D)+\sqrt{1-\mathrm{Im}^2(D)} \tag{6}$$

$$R_1=\arg[-\sqrt{1-\mathrm{Im}^2(D)}+i\mathrm{Im}(D)] \tag{7}$$

Similarly, the second image $f_2(x_2,y_2)$ to be encrypted is again encoded into two masks; phase mask R_2 and amplitude mask M_2. The phase masks obtained using first two images are used as encryption keys (*EK*) for securing a third image through phase-truncation approach. The third image $f_3(x,y)$ is first bonded with SPM_1 expressed as [39]

$$S(x,y)=t_o\times\ \cos\ \{\pi(x^2+y^2)/\lambda f\} \tag{8}$$

where t_o is a constant, λ is wavelength of light source, and f is the focal length of the zone plate. Then the resultant function is bonded with the first *EK*, $R_1(x,y)$. This function is fractional Fourier transformed with some order α_1.

$$H(u,v)=K\iint f_3(x,y)\times SPM_1(x,y)\times R_1(x,y)\times\exp\left[j\pi\frac{x^2+y^2+u^2+v^2}{\tan\ \alpha_1}-2j\pi\frac{xyuv}{\sin\ \alpha_1}\right]dxdy \tag{9}$$

Here K represents a complex constant. The obtained fractional spectrum is phase-truncated (*PT*) and amplitude-truncated (*AT*).

$$H_1(u,v)=PT\{H(u,v)\} \tag{10}$$

$$k_1(u,v)=AT\{H(u,v)\} \tag{11}$$

The *AT* value is considered as decryption key (*DK*). Now, the obtained real-valued function is further encoded with another SPM_2 and then bonded with the generated phase value, $R_2(u,v)$.

$$M(\xi,\eta)=\Im^{\alpha_2}[H_1(u,v)\times SPM_2(u,v)\times R_2(u,v)] \tag{12}$$

The *AT* and *PT* operations are repeated, which result into *DK* and encrypted image.

$$k_2(\xi,\eta)=AT\{M(\xi,\eta)\} \tag{13}$$

$$H(\xi,\eta)=PT\{M(\xi,\eta)\} \tag{14}$$

where $H(\xi,\eta)$ is the real valued function. Thus, in case of encryption for three images, $H(\xi,\eta)$ is the final encrypted image. This encryption process can be carried out for n number of images without any cross talk. This is because that additive property is not followed in the proposed scheme, which resists cross talk noise.

2.2. Image decryption scheme

The decryption process is shown in Fig. 1(b), which is considered as an inverse process of encryption. The encrypted information, $H(\xi,\eta)$ is bonded with the *DK*, $k(\xi,\eta)$ and then is inverse fractional Fourier transformed. Thus obtained complex value is *PT* operated, which results into a real-valued function, $H_1(u,v)$.

$$H_1(u,v)=PT\{\Im^{-\alpha_2}[H(\xi,\eta)\times k_2(\xi,\eta)]\} \tag{15}$$

The *AT* operated value is given as

$$g(u,v)=AT\{\Im^{-\alpha_2}[H(\xi,\eta)\times k_2(\xi,\eta)]\} \tag{16}$$

Here $g(u,v)$ is nothing but the original product, $R_2(u,v)\times SPM_2(u,v)$. The obtained real-valued function, $H_1(u,v)$ is bonded with the *DK*, $k_1(u,v)$ and its inverse transform is obtained. Finally, the *AT* operated value is given as

$$g_1(x,y)=AT\{\Im^{-\alpha_1}[H_1(u,v)\times k_1(u,v)]\} \tag{17}$$