Optics Communications 347 (2015) 118–122

Contents lists available at ScienceDirect

Optics Communications

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

Phase-only asymmetric encryption based on coherent superposition and phase-truncated Fourier transforms

Bang Cao [a,b], Jun Li [a,b], Zuohua Huang [b,*]

[a] Laboratory of Quantum Engineering and Quantum Materials, Guangzhou 51006, China
[b] School of Physics and Telecommunication, South China Normal University, Guangdong 51006, China

ARTICLE INFO

Article history:
Received 26 January 2015
Received in revised form
4 March 2015
Accepted 6 March 2015
Available online 7 March 2015

Keywords:
Phase-only
Asymmetric
Encryption

ABSTRACT

A phase-only asymmetric encryption (POAE) based on coherent superposition and phase-truncated Fourier transforms is proposed in this paper. An original image can be encrypted into a phase-only mask (POM) by using a random phase mask. Thereafter, the POM is encrypted into an amplitude image via a series of asymmetric operations based on phase-truncated Fourier transforms. Finally, the encrypted result is hidden in a public image. The encryption can be performed digitally, and the decryption can be performed optically or digitally. Simulation results are presented to demonstrate the validity and security of the proposed protocol.

1. Introduction

Since Refregier and Javidi [1] developed double random phase encoding (DRPE), many researchers have proposed a number of methods for optical image security and encryption on the basis of DRPE [2–8]. These methods include the encryption of phase-shifting digital holograms [9–12], encryption by using polarized light [13], and encryption of multiple images [14,15]. However, the DRPE encryption scheme possesses some weaknesses against some common attacks [16–20]. The main weakness lies in its linearity, and the most dangerous attack only requires two known plain images [20]. To remove the linearity of the DRPE, Qin and Peng [21] proposed an asymmetric cryptosystem based on phase-truncated Fourier transforms (PTFTs) by the nonlinear operations of phase truncation, thereby enabling ciphertext to resist some common attacks. Subsequently, a special attack on the PTFTs was proposed to reveal the encrypted information and decryption keys that are generated in the encryption procedure by using public keys and ciphertext [22]. Related studies have shown that phase-only encryption has more security than amplitude or intensity encryption [23,24]. Meng and Cai [25,26] combined DRPE with digital holographic technology to encrypt amplitude images and complete the phase-only encryption. In 2011, Wang and Zhao developed a method to encode an image on the basis of coherent superposition and basic vector operations [27]; however, the encrypted result was not easily transported and stored. As far as we know, the asymmetric segmented phase-only filter has been proposed [28], but phase-only asymmetric encryption (POAE) has not yet been reported.

In this paper, we propose a POAE based on coherent superposition and PTFTs. The decryption keys are different from the ones in the encryption process. In this asymmetric method, an amplitude image can be encrypted into a phase-only mask (POM) by using a random phase mask (RPM), and then the phase truncation and phase reservation of Fourier transforms are used to transform the POM into an amplitude image, which is hidden in a public image. Two random amplitude masks (RAMs) applied to the asymmetric encryption algorithm can be safely used as public keys, whereas the amplitude mask (AM) and phase mask (PM) generated in the encryption procedure are treated as two private decryption keys. Computer simulation results show that the proposed cryptosystem has an effective resistance against some common attacks and the specific attack which is based on a two-step iterative amplitude retrieval approach.

The image encryption and decryption processes are described in Section 2. The validity of this method is verified by computer simulation in Section 3. The algorithms resistance against common attacks and special attacks is analyzed in Section 4. Finally, the conclusions are presented in Section 5.

2. Principle of encryption and decryption

According to the technology of coherent superposition [27], the

* Corresponding author.
E-mail address: zuohuah@163.com (Z. Huang).

http://dx.doi.org/10.1016/j.optcom.2015.03.007
0030-4018/

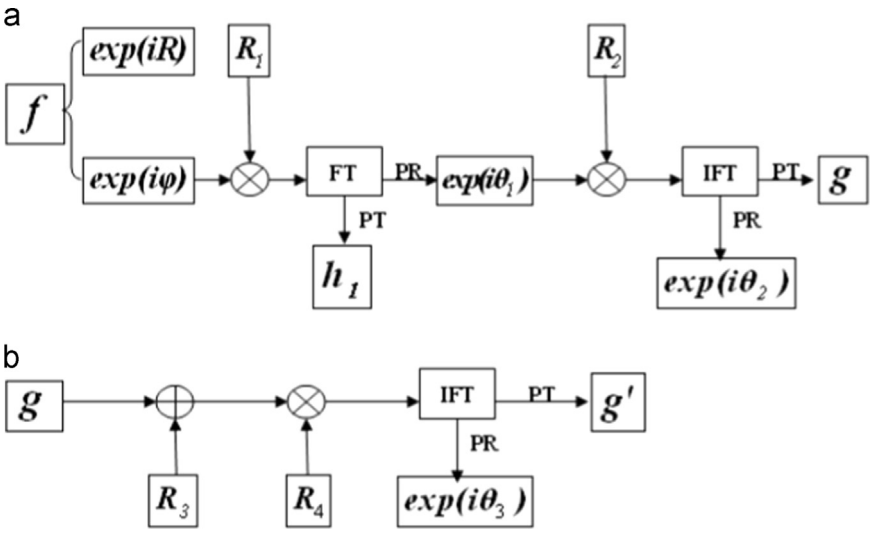

Fig. 1. (a) Flowchart of POAE; (b) process of hiding ciphertext g in a public image g'; h_1 and $\exp(i\theta_2)$ are kept as decryption keys.

plaintext $f(x)$ can be transformed into POM $\exp[i\varphi(x)]$ by using RPM $\exp[iR(x)]$. The POM is expressed as follows:

$$\exp[i\varphi(x)] = \exp\left[iR(x) + i\pi - i\arccos\left(1 - \frac{|f(x)|^2}{2}\right)\right]. \tag{1}$$

The POM employs a pair of independent RAMs, namely, $R_1(x)$ and $R_2(u)$, as asymmetric encryption keys. The mean value and standard deviation of the RAMs cannot be zero. Finally, the result of the encryption is hidden in the public image $g'(x)$ with the aid of AM $R_3(u)$ and PM $R_4(u)$, both of which can be respectively obtained from the following equations:

$$R_3(u) = \mathrm{PT}\{\mathrm{FT}[g_1(x)]\}, \tag{2}$$

$$R_4(u) = \mathrm{PR}\{\mathrm{FT}[g_1(x)]\}, \tag{3}$$

where $g_1(x)$ denotes the carrier image. Operators FT{}, PT{}, and PR{} denote the operator of Fourier transform, the operator of phase truncation, and the operator of phase reservation, respectively. The processes of encryption and image-hiding are illustrated in Fig. 1(a) and (b), respectively.

First, POM is modulated by a RAM $R_1(x)$. The phase truncation and phase reservation are then performed as follows:

$$h_1(\theta_1) = \mathrm{PT}\{\mathrm{FT}[R_1(x)\exp(i\varphi(x))]\}, \tag{4}$$

$$\exp(i\theta_1) = \mathrm{PR}\{\mathrm{FT}[R_1(x)\exp(i\varphi(x))]\}. \tag{5}$$

Second, by using the RAM $R_2(u)$, the result of encryption $g(x)$ can be written as follows:

$$g(x) = \mathrm{PT}\{\mathrm{IFT}[R_2(u)\exp(i\theta_1)]\}, \tag{6}$$

$$\exp(i\theta_2) = \mathrm{PR}\{\mathrm{IFT}[R_2(u)\exp(i\theta_1)]\}, \tag{7}$$

where the operator of IFT{} denotes the inverse Fourier transform, $g(x)$ is the encrypted image, and $g'(x)$ is the public image, which can be given by the following:

$$g'(x) = \mathrm{PT}\{\mathrm{IFT}[R_4(u)(R_3(u) + g(x))]\}, \tag{8}$$

$$\exp(i\theta_3) = \mathrm{PR}\{\mathrm{IFT}[R_4(u)(R_3(u) + g(x))]\}. \tag{9}$$

Thus, we have realized the processes of the POAE based on coherent superposition and PTFTs and the image-hiding technique. $\exp(i\theta_3)$ and $R_3(u)$ can be used as decryption keys from public image to the ciphertext. $h_1(\theta_1)$ and $\exp(i\theta_2)$ are retained as decryption keys from ciphertext to plaintext.

We can retrieve the plaintext from the public image in two steps. The first step is from the public image to the ciphertext and can be written as

$$g(x) = \mathrm{PT}\{\mathrm{FT}[g'(x)\exp(i\theta_3)]\} - R_3(u). \tag{10}$$

The second step, which is from ciphertext to plaintext, is given by following equations:

$$\exp(i\theta_1) = \mathrm{PR}\{\mathrm{FT}[g(x)\exp(i\theta_2)]\}, \tag{11}$$

$$\exp[i\varphi(x)] = \mathrm{PR}\{\mathrm{IFT}[h_1(\theta_1)\exp(i\theta_1)]\}, \tag{12}$$

$$f(x) = |\exp[i\varphi(x)] + \exp[iR(x)]|. \tag{13}$$

The first and second steps from the public image to the plaintext are shown in Fig. 2(a) and (b), respectively.

The phase reservation is implemented with the aid of space-light modulators (SLMs) in the Fourier domain and imaging plane. The reserved-phase POM is then coherently superposed with the RPM in the CCD plane. The sketch of the optical setup for the decryption process of POAE is shown in Fig. 3.

3. Numerical simulation and discussion

Numerical simulations are conducted on MATLAB 7.9 to show the feasibility of the proposed method. In our method, the encrypted result and the key for decryption have the same size as the image to be encoded. A double precision image Lena with a size of 256×256 pixels (Fig. 4(a)) is taken as the plaintext. A double precision image Cameraman is selected as a carrier image (Fig. 4(b)), and the public image, which differs slightly from the carrier image, is shown in Fig. 4(c). The encryption keys are shown in Fig. 4(d)–(f), and (g)–(h) show the private decryption keys.

The difference between Fig. 4(b) and (c) is difficult to detect. Thus, the ciphertext is perfectly hidden in the public image. We can also compute the value of the mean-square error (MSE) between Fig. 4(b) and (c), which is MSE = $6.9000e^{-11}$. The very small value of the MSE indicates that the hiding works well.

4. Analysis of resistance against attacks

To illustrate the high security of our algorithm, we do not focus