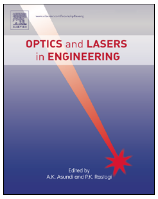
Optics and Lasers in Engineering 78 (2016) 8–16

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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



Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm

Y. Wang, C. Quan*, C.J. Tay

Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 14 July 2015
Received in revised form
28 August 2015
Accepted 22 September 2015

Keywords:
Optical encryption
Asymmetric cryptosystem
Phase retrieval

ABSTRACT

We propose a new asymmetric optical image encryption scheme based on an improved amplitude–phase retrieval algorithm. Using two random phase masks that serve as public encryption keys, an iterative amplitude and phase retrieval process is employed to encode a primary image into a real-valued ciphertext. The private keys generated in the encryption process are used to perform one-way phase modulations. The decryption process is implemented optically using conventional double random phase encoding architecture. Numerical simulations are presented to demonstrate the feasibility and robustness of the proposed system. The results illustrate that the computing efficiency of the proposed method is improved and the number of iterations required is much less than that of the cryptosystem based on the Yang–Gu algorithm.

1. Introduction

The wide spread use of internet has led to remarkable research efforts in the area of information transmission security. In this connection, optical encryption has attracted increasing attention due to its marked characteristics, such as parallel processing and multidimensional capabilities [1–3]. One of the most popular optical encryption techniques, namely, double random phase encoding (DRPE), was first introduced by Refregier and Javidi [4]. In a DRPE system, an image is encoded into a stationary white noise through two statistically independent random phase masks located at the input and Fourier planes. To enlarge the key space and ensure information security, the DRPE algorithm has been extended from Fourier domain to fractional Fourier [5–7] and Fresnel domains [8–10], in which fractional orders and propagation distance are considered as secret keys. However, DRPE-based encryption schemes are linear symmetric cryptosystems, in which decryption keys are identical to encryption keys and they have been found vulnerable to different types of attacks, such as known plaintext and chosen plaintext attacks [11–15]. Some other techniques, such as compressive sensing [16,17], interference [18,19], three-dimensional space [20,21] and nonuniform beam [22,23] are also employed to build secure image encryption schemes.

In recent year, Qin and Peng proposed an asymmetric cryptosystem based on nonlinear phase-truncated Fourier transforms (PTFTs) to render the DRPE scheme nonlinear [24]. This produces a real-value ciphertext with two public keys and a user is able to retrieve the original plaintext using two private keys. Several optical image encryption techniques based on phase-truncation cryptosystem were further developed [25,26]. Owing to the nonlinear operation of the phase truncation, the encryption system is able to achieve a high degree of robustness against existing attacks. However, PTFT-based cryptosystem is still vulnerable to a known public key attack based on iterative amplitude–phase retrieval algorithm [27,28]. Subsequently, techniques, such as amplitude modulation [29] and spherical wave illumination [30], have been proposed to resist known public key attack. Several nonlinear encryption methods based on phase retrieval algorithm [31–33] have been further proposed in recent years. For instance, Rajput and Nishchal presented a Fresnel domain nonlinear image-encryption scheme based on a Gerchberg–Saxton algorithm [31]; Wang et al. proposed a nonlinear image encryption based on a mixture retrieval algorithm [32] and Liu et al. proposed a new encryption scheme based on the Yang–Gu algorithm, in which the public and private key structures are redesigned [33]. However, these methods employ a two-step iterative process and the iteration number for obtaining a high quality image is large due to repetitions in the iteration process. From a computing efficiency point of view, it is always desirable to obtain a high quality image with less iterations and computational time.

In this paper, we propose a new asymmetric optical image encryption scheme based on an improved amplitude–phase retrieval algorithm. The original image and two random phase

* Corresponding author. Tel.: +65 65168089; fax: +65 67791459.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

http://dx.doi.org/10.1016/j.optlaseng.2015.09.008
0143-8166/© 2015 Elsevier Ltd. All rights reserved.

masks (RPMs) function as constraints during the encryption process. Unlike the cryptosystem based on the Yang–Gu algorithm [33], only one iteration process is required in the proposed method and hence the number of iterations and time consumption are reduced significantly. One of the private keys is redesigned and the decryption process is implemented optically based on a linear DRPE scheme. An analysis is conducted to show the robustness of the proposed method against contaminations and attacks. Numerical simulations demonstrate the feasibility and effectiveness of the proposed methods.

2. Theoretical analysis

Recently, Liu et al. proposed a cryptosystem based on the Yang–Gu amplitude–phase retrieval algorithm [33]. The encryption process is conducted in two steps: firstly, the original image is encrypted as an amplitude $g'(u,v)$ using a public key and a binary phase modulation; secondly, the amplitude $g'(u,v)$ is employed as an input in the second iterative process, and a binary phase modulation is generated to obtain a positive ciphertext $C'(x,y)$. The encryption process can be summarized as follows:

$$g(u,v)R_1(u,v)=\mathrm{FT}\{f(x,y)\exp[i\phi(x,y)]\}, \tag{1}$$

$$g'(u,v)=g(u,v)exp[i\pi\gamma_1(u,v)] \tag{2}$$

$$C(x,y)R_2(x,y)=\mathrm{IFT}\{g'(u,v)\exp[i\phi'(u,v)]\}. \tag{3}$$

$$C'(x,y)=C(x,y)\exp[i\pi\gamma_2(x,y)] \tag{4}$$

where FT and IFT represent Fourier transform and inverse Fourier transform respectively, $R_1(u,v)$ and $R_2(x,y)$ represent public random phase keys, $f(x,y)$ represents amplitude of the original image, $g'(u,v)$ and $C'(x,y)$ are unknown amplitudes, $\phi(x,y)$ and $\phi'(u,v)$ are unknown phases to be retrieved. Two private keys $\gamma_1(u,v)$ and $\gamma_2(x,y)$ are generated in the encryption process. Since two steps iterative processes are employed, the iteration number and time consumption is large.

In the proposed amplitude–phase retrieval algorithm, only one iteration process is required. A flow chart of the proposed method is shown in Fig. 1. The two public keys, RPM$_1$ and RPM$_2$, and a plaintext are used as constraints during the iteration process. The proposed encryption process can be describes as follows:

1. A random distribution function $C_1(x,y)$ is assigned as an initial estimation for the ciphertext. At the kth iteration, ciphertext $C_k(x,y)$ is combined with public key RPM$_2$ $R_2(x,y)$ and a Fourier transformed is performed. The amplitude and phase of the spectrum are given by

$$g'_k(u,v)=\mathrm{PT}\{\mathrm{FT}[C_k(x,y)R_2(x,y)]\}, \tag{5}$$

$$\exp[i\phi'_k(u,v)]=\mathrm{PR}\{\mathrm{FT}[C_k(x,y)R_2(x,y)]\}, \tag{6}$$

where PT{} and PR{} denote operators of phase truncation and phase reservation, respectively. Phase truncation retains the amplitude of a complex function but truncates the phase while phase reservation retains the phase and removes the amplitude. Given a spectrum $G(u,v)=|G(u,v)|\exp[i2\pi\varphi(u,v)]$, the phase truncation and the phase reservation can be respectively expressed as: $\mathrm{PT}[G(u,v)]=|G(u,v)|$ and $\mathrm{PR}[G(u,v)]=\exp[i2\pi\varphi(u,v)]$.

2. Amplitude function $g'_k(u,v)$ as shown in Eq. (5) is multiplied by public key RPM$_1$ $R_1(u,v)$ and a private phase modulation $\exp(i\pi\gamma_{1,k-1})$ ($\gamma_{1,0}$ is initialized to 0), and an inverse Fourier transform is performed. The amplitude and phase of the spectrum are then given by

$$f_k(x,y)=\mathrm{PT}\{\mathrm{IFT}[g'_k(u,v)\cdot R_1(u,v)\exp(i\pi\gamma_{1,k-1}(u,v))]\}, \tag{7}$$

$$\exp[i\phi_k(x,y)=\mathrm{PR}\{\mathrm{IFT}[g'_k(u,v)\cdot R_1(u,v)\exp(i\pi\gamma_{1,k-1}(u,v))]\}, \tag{8}$$

3. The phase function $\exp[i\phi_k(x,y)]$ given by Eq. (8) is multiplied by plaintext $f(x,y)$ and a Fourier transform is performed

$$F_k(u,v)=FT\{f(x,y)\exp[i\phi_k(x,y)]\}, \tag{9}$$

4. The spectrum $F_k(u,v)$ is multiplied by a complex conjugate RPM$_1$ $R_1^*(x,y)$ to obtain the real part $g_k(u,v)$

$$g_k(u,v)=\mathrm{Re}\{F_k(u,v)\cdot R_1^*(u,v)\}, \tag{10}$$

The amplitude $g_k(u,v)$ contains both positive and negative values. In order to obtain the actual amplitude, a one-way binary phase modulation $\exp[j\pi\gamma_{1,k}(u,v)]$ is introduced. Private modulation $\gamma_{1,k}(u,v)$ is generated using the following equation:

$$\gamma_{1,k}(u,v)=\begin{cases}1 & g_k(u,v)<0\\ 0 & g_k(u,v)>0\end{cases} \tag{11}$$

The actual amplitude is given by

$$g''_k(u,v)=g_k(u,v)\exp(i\pi\gamma_{1,k}(u,v)), \tag{12}$$

5. The function $g''_k(u,v)$ is then multiplied by the phase function $\exp[i\phi'_k(u,v)]$ shown in Eq. (6) and an inverse Fourier transform

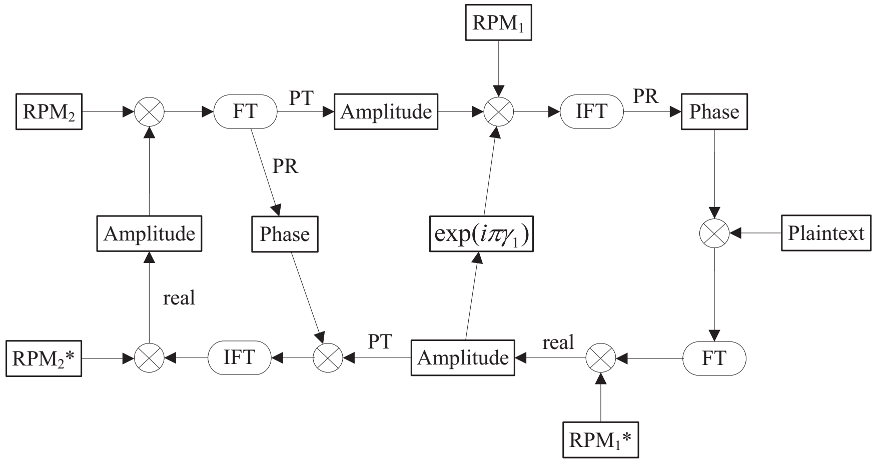


Fig. 1. Flowchart of the proposed encryption process.