Optics and Lasers in Engineering 107 (2018) 142–148

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Specific attack and security enhancement to optical image cryptosystem based on two random masks and interference

Y. Xiong, A. He, C. Quan*

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

ARTICLE INFO

Keywords:
Specific attack
Phase-truncated Fourier-transform-based encoding
Security enhancement

ABSTRACT

In this paper, we evaluate the security of an amplitude-phase retrieval attack free encryption scheme based on two random masks and interference. In the proposed cryptosystem, two phase-only masks (POMs) are generated from two random images using interference technique. The POMs are then used as encryption keys in a phase-truncated Fourier transform (PTFT) based encryption scheme. Compared to traditional PTFT-based cryptosystem, the security of the encryption scheme is improved by integrating the interference technique. Consequently, the scheme is immune to some attacks. We proposed a specific attack based on a phase retrieval algorithm with median filtering to break the cryptosystem. Numerical simulation results show that the cryptosystem is vulnerable to the proposed attack. Moreover, based on the proposed attack and the existing cryptosystem, full phase encoding technique is added to the previous cryptosystem to enhance the security.

1. Introduction

With the wide spread use of Internet, information transmission security has drawn increasing attention. In this connection, due to inherent capability of arbitrary selection of optical parameters and high speed parallel processing of multi-dimensional signal, optical encryption techniques have been widely employed in information processing filed [1,2]. The most pioneering work in optical image encryption filed is the double random phase encoding (DRPE) proposed by Refregier and Javidi [3]. With help of a classical DRPE scheme, an image is encoded into a stationary white noise through two statistically independent random phase masks (RPMs) located at the input and frequency planes, respectively. Since then, the DRPE-based encryption algorithm has been extended from Fourier domain to fractional Fourier [4–6], Fresnel [7,8], gyrator [9,10], fractional Mellin domains [11,12]. In these cryptosystems, additional parameters can be used as private keys to enlarge the key space and ensure information security.

In recent years, numerous works have demonstrated that the DRPE-based cryptosystems are vulnerable to some attacks due to inherent linearity [13–18]. To render the DRPE scheme nonlinear, Qin and Peng proposed an asymmetric cryptosystem based on nonlinear phase-truncated Fourier transforms (PTFTs) [19]. Owing to the nonlinearity of the phase truncation, the encryption system is immune to common attacks which DRPE-based cryptosystems are vulnerable to. However, PTFT-based cryptosystem is found to be vulnerable to special attacks based on iterative amplitude-phase retrieval algorithm [20,21]. Subsequently, various nonlinear encryption methods [22–26] have been further proposed. These methods employ an iterative process which would decrease the computational efficiency. Image encryption techniques based on chaos [27–29] and holography [30] with good performance have also been reported. An interference-based encryption scheme has been proposed by Zhang and Wang [31]. In this cryptosystem, a plaintext is encrypted into two phase-only masks (POMs) with no iterative process. However, interference-based cryptosystems have been found that partial information of the plaintext can be recognized visually due to silhouette problem. To overcome this issue, several optical image encryption schemes based on interference have been proposed [32–34].

Recently, Sui and Zhou et al. proposed an amplitude-phase retrieval attack free encryption scheme based on PTFTs and interference [35]. In this scheme, the POMs used as encryption keys are generated by an interference structure with two RPMs. Subsequently, a plaintext is encrypted to the real-valued ciphertext by using the PTFTs with encryption keys. The encryption process is nonlinear and no iterative calculation is involved, while the decryption process is linear and can be implemented with the 4*f* optical system. Compared to the original PTFT-based cryptosystem, only one RPM is set as the public key, and the decryption keys are generated by an interference structure, which improve the security of cryptosystem. In addition, since the interference technique is used to generate two encryption keys rather than encrypt a plaintext, the silhouette problem of interference-based encryption scheme can be avoided elaborately.

* Corresponding author.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

https://doi.org/10.1016/j.optlaseng.2018.03.023
Received 13 December 2017; Received in revised form 1 March 2018; Accepted 20 March 2018

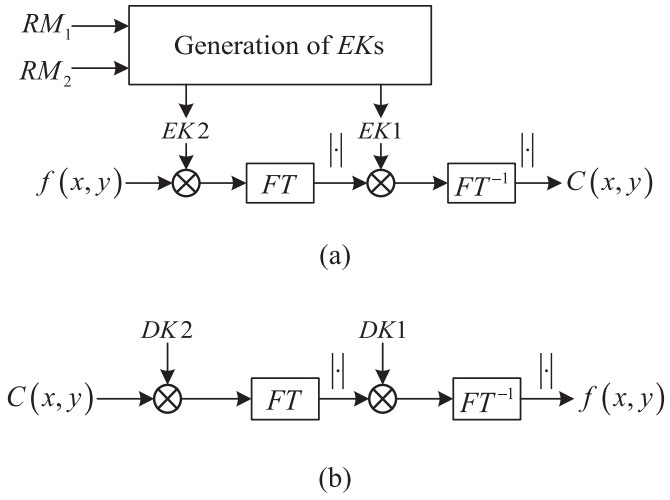

Fig. 1. Schematic diagram of (a) encryption process, (b) decryption process in Ref. [35].

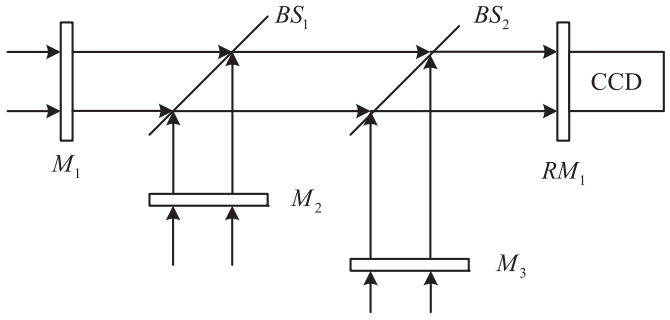

Fig. 2. Optical relationship between M_1, M_2, M_3 and RM_1 in Ref. [35].

In this paper, we will evaluate the security of an optical image cryptosystem based on PTFT and interference. Then, we will show how the cryptosystem is vulnerable to our proposed specific attack and how a plaintext can be retrieved by using only a ciphertext. Based on cryptanalysis of the existing cryptosystem, we will propose a security-enhanced cryptosystem by combining full phase encoding with the existing cryptosystem.

2. Image encryption scheme based on two random masks and interference

The process of the amplitude-phase retrieval attack free encryption scheme is shown in Fig. 1. $f(x, y)$ denotes the intensity distribution of the plaintext, RM_1, RM_2 represent two statistically independent random masks (*RMs*) whose values are uniformly distributed in [0, 1], $EK1$ and $EK2$ are two encryption keys generated by an interference technique. RM_2 is set as the only public key. The optical setting for the interference technique is shown in Fig. 2. Three coherent parallel light beams modulated by three POMs, M_1, M_2 and M_3, are combined by two beam splitters. These beams interfere mutually and generate random image RM_1, which can be recorded by a CCD. M_3 is generated by public key RM_2 as follows:

$$M_3 = 2\pi RM_2 \tag{1}$$

The relationship between M_1, M_2, M_3 and RM_1 can be expresses as:

$$RM_1 = \exp(iM_1) * h(x, y; l_1) + \exp(iM_2) * h(x, y; l_2) + \exp(iM_3) * h(x, y; l_3) \tag{2}$$

where variables l_1, l_2 and l_3 represent the distances between three POMs and the output plane, respectively. For simplicity, distances are set as same value l. Variables x and y are indices of image plane. The symbol $*$ denotes the convolution operation, function $h(x, y; l)$ is the point pulse function of the Fresnel transform:

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

where λ is the wavelength of the incident light. Employing the convolution theorem on Eq. (2), a simple deduction can be obtained and given as:

$$D = \exp(iM_1) + \exp(iM_2) = FT^{-1}\left\{\frac{FT(RM_1) - FT[\exp(iM_3)]FT[h(x, y; l)]}{FT[h(x, y; l)]}\right\} \tag{4}$$

where function D is a resultant vector, $FT\{\cdot\}$ and $FT^{-1}\{\cdot\}$ denote a forward and inverse Fourier transform, respectively. Subsequently, two masks M_1 and M_2 can be given as:

$$M_1 = \arg(D) - \cos^{-1}(|D|/2) \tag{5}$$

$$M_2 = \arg[D - \exp(iM_1)] \tag{6}$$

where $\arg\{\cdot\}$ and $|\cdot|$ return a phase angle and an amplitude of a complex number, respectively, and $\cos^{-1}$ denotes an inverse cosine operation. Finally, two encryption keys $EK1(m, n)$ and $EK2(x, y)$ are given by

$$EK1(m, n) = \exp[iM_1(m, n)] \tag{7}$$

$$EK2(x, y) = \exp[iM_2(x, y)] \tag{8}$$

where variables m and n are indices of Fourier domain. Based on PTFT encryption scheme shown in Fig. 1, a final encrypted image $C(x, y)$ is expressed as:

$$C(x, y) = \left|FT^{-1}\{|FT[f(x, y)EK2(x, y)]|EK1(m, n)\}\right| \tag{9}$$

In the cryptosystem, RM_1 is an auxiliary random mask to generate M_1 and M_2, which means that it is not necessary to record RM_1. In the decryption process, using two decryption keys $DK2(x, y)$ and $DK1(m, n)$ generated in encryption process, a decrypted image $f'(x, y)$ can be expressed as

$$f'(x, y) = \left|FT^{-1}\{|FT[C(x, y)DK2(x, y)]|DK1(m, n)\}\right| \tag{10}$$

where $DK1(m, n)$ and $DK2(x, y)$ are given by:

$$DK1(m, n) = PR\{FT[f(x, y)EK2(x, y)]\} \tag{11}$$

$$DK2(x, y) = PR\left\{FT^{-1}[|FT[f(x, y)EK2(x, y)]|EK1(m, n)]\right\} \tag{12}$$

where $PR\{\cdot\}$ is a phase-reserved operation.

3. Specific attack on cryptosystem based on two random masks and interference

Cracking a security system means finding the value of keys with some knowledge about the input and corresponding output of the system. According to the Kerckhoffs' principle [36], everything about the cryptosystem, except the keys, is public knowledge. In this section, we analysis the security of the encryption scheme, and show how this optical encryption scheme can be vulnerable to a ciphertext-only attack (COA) based on phase retrieval algorithm.

The authors of Ref. [35] claimed that since only RM_2 is employed as the public key, it is impossible to retrieval two encryption keys ($EK1$, $EK2$) with this unique constraint. In fact, since the two encryption keys are generated by interference technique, they are not independent. Based on this analysis, we try to retrieve RM_1, which is used as a random image and not recorded in the encryption process, with the help of the public key RM_2. Employing RM_2 and the retrieved RM_1, two encryption keys can be generated, and a retrieved plaintext can be obtained.