Optics and Lasers in Engineering 86 (2016) 1–10

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Amplitude-phase retrieval attack free image encryption based on two random masks and interference

Sui Liansheng *, Zhou bei, Wang Zhanmin, Sun qindong

School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China

ARTICLE INFO

Article history:
Received 10 December 2015
Received in revised form
21 March 2016
Accepted 27 April 2016
Available online 13 May 2016

Keywords:
Specific attack
Phase-truncated Fourier-transform-based encoding
Interference

ABSTRACT

An amplitude-phase retrieval attack free encryption scheme is proposed by using two random masks, where one is considered as the random image and other as the public key. Initially, the random image is encrypted to two phase-only masks based on interference technique with the help of the public key. These two phase-only masks are real-valued functions and used as the encryption keys. Then, the plain image is encrypted to the ciphertext with the white noise distribution by using the phase-truncated Fourier-transform-based encoding scheme with the previous encryption keys. The encryption process is nonlinear in which no iterative calculation is involved, while the decryption process is linear which can be easily implemented with the 4*f* optical system. Moreover, less constraints makes the specific attack unusable. Simulation results are given to verify the feasibility and robustness of the proposed encryption scheme.

1. Introduction

Due to inherent capability of arbitrary selection of optical parameters and high speed parallel processing of multi-dimensional signal, optical techniques have been widely employed in information processing fields such as image security applications. Currently, though numerous optical methods such as coherent diffractive imaging [1], integral imaging [2], ghost imaging [3], photon-counting [4], polarized light encoding [5], interferometer [6] and compressive sensing [7] have been employed for different applications including image encryption and watermarking, the most pioneering work is the double random phase encoding (DRPE) proposed in [8]. With the help of DRPE, the plain image is encrypted to the ciphertext with stationary white noise distribution by using two random phase masks (RPMs), where one is placed in the input plane and another in the frequency plane. Up to now, the encryption schemes based on Fourier transform (FT) [9] or discrete cosine transform (DCT) [10] have been extended into different domains such as fractional Fourier transform (FrFT) [11], Fresnel transform (FrT) [12], gyrator transform (GT) [13,14], fractional angular transform [15], fractional random transform [16] and fractional Mellin transform (FrMT) [17], in which the additional parameters can be used as secret keys. In Ref. [18], the authors have analyzed numerous kinds of optical encryption methods and different applications and predicted some future trend.

However, recent works have demonstrated that the DRPE based cryptosystems are vulnerable to some kinds of attacks due to inherent linearity [19,20]. To overcome these weaknesses, a variety of nonlinear encryption schemes have been proposed subsequently. Among them, the diffusion or confusion encoding architecture based on different chaotic maps has widely applied into different optical cryptosystems [21–23], which makes the encryption or decryption process more complicated. Additionally, the most attracting method based on the phase-truncated Fourier transforms (PTFTs) is proposed, in which the linearity of DRPE is removed thoroughly [24]. Unfortunately, Wang and Zhao [25] reported a specific attack that can reveal the hiding information of ciphertext encrypted by using PTFTs. In the process of attack, a two-step iterative amplitude-phase retrieval process is exploited while the encryption keys are considered as public keys. Most recently, Wang and Zhao [26] proposed an amplitude-phase retrieval attack free cryptosystem based on PTFTs, which makes the specific attack unusable due to lack of enough constraints. In the process of encryption, two PTFTs are employed. Initially, a random amplitude mask (RAM) is encrypted by using the first PTFTs with two random phase masks (RPMs) as public keys, in which two fake keys are generated. Then, the plain image is encrypted to the ciphertext by using the second PTFTs with two fake keys as encryption keys. Though this method has a high level of robustness, it is not straightforward, and more masks including two random phase masks (RPMs) and one random amplitude mask (RAM) are indispensable, which makes the encoding architecture more complicated.

Since Zhang and Wang [27] proposed an interference based

* Corresponding author.
E-mail address: liudua2010@gmail.com (S. Liansheng).

http://dx.doi.org/10.1016/j.optlaseng.2016.04.026
0143-8166/

scheme to encrypt a plain image into two phase-only masks (POMs) with no iterative calculations, various POM-based schemes are designed to implement image encryption optically [28–35]. In order to eliminate the inherent problem that the silhouette information of the plain image can be recognized visually by making use of one mask, some approaches have been suggested by adding additional transformation or using larger number of POMs. Kumar et al. [36] proposed an interference-based optical encryption scheme to overcome the silhouette problem with non iterative process, in which the jigsaw transformation is employed in a single step. Wang [37] reported a simple method to resolve the problem, in which the information of the plain image is smoothed away by using the modulation of a random POM. Wang and Zhao [38] suggested a very compact method to remove the problem, where the information of the plain image is hidden into three POMs. But it is still possible that the remnant information of the plain image can be recognized by using two of these POMs.

In this paper, an amplitude-phase retrieval attack free encryption scheme is proposed to resist against the specific attack by using two random masks. First, two randomly generated masks are input into the cryptosystem, where one is used as the random image and other as the public key. By using interference method with the help of the public key, the random image is encrypted to form into two POMs that are employed as the encryption keys in the subsequent encryption process. Second, the plain image is encrypted to the real-valued ciphertext by using the PTFTs with these encryption keys. Simultaneously, two decryption keys that are relative to the plain image are engendered, which makes the proposed scheme has high robustness against potential attacks such as chosen plain attack. To the best of our knowledge, this is the first report on integrating the interference technique with the PTFTs based cryptosystem in the field of optical image encryption. Because the POMs generated by using interference are used as the encryption keys which cannot be accessed by the unauthorized users, the proposed scheme can avoid the silhouette problem of interference-based encryption scheme elaborately. Different from the modified PTFTs based scheme proposed in [26], only two random masks are used to generate the encryption keys, which makes the cryptosystem has more security. Finally, numerical simulation results are presented to demonstrate the feasibility and effectiveness of the proposed scheme.

The rest of this article is organized as follows. In Section 2, the encryption and decryption processes are introduced in detail. In Section 3, numerical simulation results and security analysis are given. Finally, the conclusion is given in Section 4.

2. Encryption and decryption process

The diagram of the encryption process is shown as Fig. 1(a). Let the function $f(x, y)$ denotes the intensity distribution of the plain image, and RM_1, RM_2 represent two statistically independent random masks (RMs), respectively, which values are randomly distributed in the interval [0, 1].

Initially, two random masks RM_1 and RM_2 are input into the generation process of the encryption keys (EKs), in which two POMs denoted as M_1 and M_2 are engendered based on interference. In this process, RM_1 is considered as the intensity distribution of random image and RM_2 is used as public key to form the POM M_3, which is expressed as

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

Two encryption keys EK_1 and EK_2 that are used to encrypt the plain image based on PTFTs are generated as

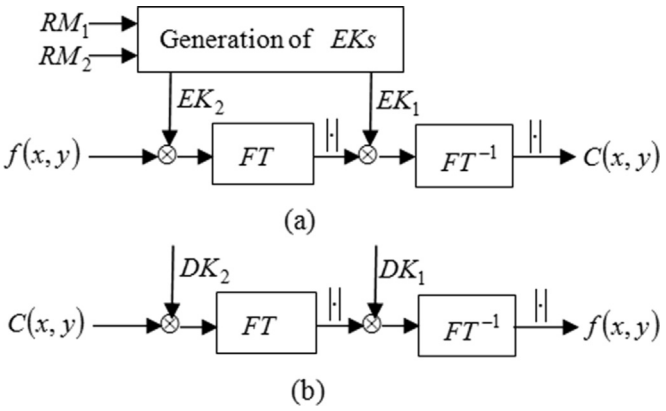

Fig.1. Diagram of (a) encryption and (b) decryption.

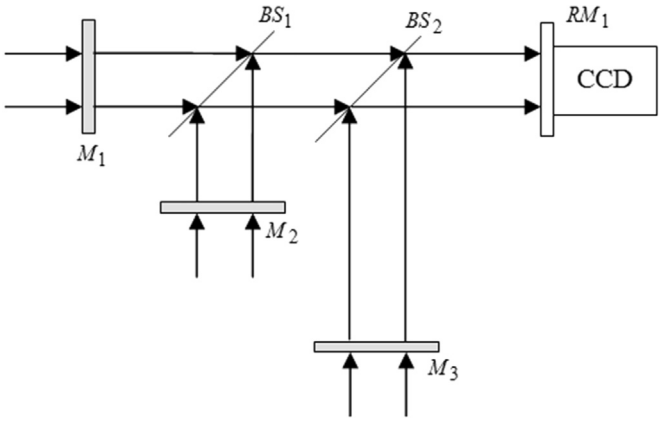

Fig. 2. Optical relationship between M_1,M_2, M_3 and RM_1.

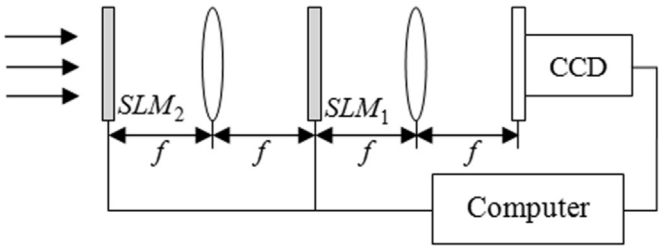

Fig.3. Optical setup of the decryption process.

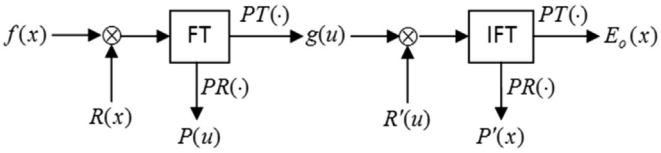

Fig.4. Diagram of the encryption process proposed in Ref. [24].

$$EK_1 = \exp(jM_1), \tag{2}$$

$$EK_2 = \exp(jM_2). \tag{3}$$

The optical relationship between M_1, M_2, M_3 and random image RM_1 is schematically shown in Fig. 2. Three coherent parallel light beams modulated by M_1, M_2 and M_3, respectively, are combined by two beam splitters. Thus three beams interfere mutually and generate random image RM_1, which can be received by the intensity detector such as CCD. Notably, RM_1 is an auxiliary random function to generate M_1 and M_2, which means that it is not necessary to record RM_1.