Optics Communications 328 (2014) 67–72

Contents lists available at ScienceDirect

Optics Communications

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

Optical image encryption via reverse engineering of a modified amplitude-phase retrieval-based attack

Xiaogang Wang*, Chaoqing Dai, Junlang Chen

School of Sciences, Zhejiang A & F University, Lin'an, Zhejiang Province 311300, China

ARTICLE INFO

Article history:
Received 8 March 2014
Received in revised form
8 April 2014
Accepted 23 April 2014
Available online 9 May 2014

Keywords:
Optical encryption
Amplitude-phase retrieval
Phase truncation
Attack

ABSTRACT

By reverse-engineering the modified amplitude-phase retrieval-based attack that has deciphered the phase-truncated double random phase encoding scheme, we proposed a new cryptosystem to encode a target image into a preselected fake image using a modified phase retrieval algorithm under the framework of phase-truncated double random phase encoding. With two private keys that are generated during the encryption, the decryption can be optically realized using a classical linear double random phase encoding method. The proposed cryptosystem has immunity against the recently proposed specific attack and the new attack based on a modified amplitude-phase retrieval algorithm. Numerical results are presented to demonstrate the validity and good performance of our proposed algorithm.

1. Introduction

Over the past two decades, optical security techniques have been proposed to secure and decrypt information based on double random phase encoding (DRPE) [1], phase retrieval algorithm [2–5], diffractive imaging [6,7], ghost imaging [8,9], etc. Among them, the classical DRPE scheme has spawned many variation techniques by combining different optical transforms [10–17]. In these variation techniques, different optical transforms are used for encryption and encryption keys are required to retrieve the original information, i. e., the encryption process is the same as its decryption process and the encryption key is identical to the decryption too. This complete symmetry is changed in the phase-truncated DRPE system based on phase-truncated Fourier transforms (PFFTs) with security enhancement [18]. However, a few weaknesses have started to appear in some recent investigations on the security of phase-truncated DRPE [19]. When the two encryption keys are compromised or regarded as public keys, this phase-truncated DRPE scheme is vulnerable to a specific attack method based on a cascade amplitude-phase retrieval algorithm, which can be regarded as an extended application of phase retrieval algorithm that has been successfully applied in crystallography [20]. Subsequently, several new phase-truncated encryption techniques have been explored to improve safety and have drawn considerable attention from researchers for their nonlinear property [21–28].

An attack on the security of a cryptosystem is usually undertaken to test the effectiveness of the security and to highlight any areas of weakness, but it can also be used for encryption and security enhancement. Recently, Rajput and Nishchal have proposed an information security scheme based on modified Gerchberg–Saxton algorithm and the concept of known plaintext attack under the framework of linear DRPE [26]. Based on the idea of the specific attack, nonlinear optical cryptosystems in Fourier domain [27] and Fresnel domain [28] have also been proposed by employing a cascaded Yang–Gu (or Gerchberg–Saxton) algorithm, which comprises two iteration processes with high consumed computations and cumulative error.

Very recently, we have proposed a new method of attack to decipher the nonlinear phase-truncated DRPE scheme based on a modified amplitude-phase retrieval algorithm [29]. The total number of iterations by using this method is much less than that by the specific attack, where the amplitude-phase retrieval algorithm has been applied twice. In this paper, we develop a new cryptosystem by reverse-engineering the modified amplitude-phase retrieval-based attack. Different from the phase-retrieval-based algorithms using classical linear double random phase encoding [3–5], here we encode a target image into a preselected fake image by using a modified amplitude-phase retrieval algorithm under the framework of phase-truncated double random phase encoding. In addition, the random phase masks applied for encryption can be treated as public keys in our method. Each iteration of the modified amplitude-phase retrieval algorithm involves four cascaded phase-truncated Fourier transforms and inverse Fourier transforms. With two asymmetric private keys that are generated during the encryption, the decryption can be optically realized using the classical linear double random phase encoding method.

* Corresponding author.
E-mail address: wxg1201@163.com (X. Wang).

http://dx.doi.org/10.1016/j.optcom.2014.04.059
0030-4018/© 2014 Elsevier B.V. All rights reserved.

In Section 2, we describe the principle of encoding an original image into a fake image by reverse-engineering the recently proposed modified amplitude-phase retrieval-based attack. In Section 3, the feasibility and security of this method are verified by computer simulations. Some conclusions are finally presented in Section 4.

2. Principle

As illustrated in Fig. 1, the encryption can be realized by single application of a modified amplitude-phase retrieval algorithm that reduces the consumed computations and cumulative error. Differing from conventional linear DRPE-based and phase-truncated DRPE-based encryption schemes [1,10–18,21–28], the target image (original image) here is encoded into a fake image, which is another preselected image used to avoid arousing the curiosity of the grabbers who desire to recover it or simply destroy it. The two grayscale images shown in Fig. 1 are just used for illustration.

Hereinafter, we use one-dimensional coordinate for notational simplicity. Let the functions $I(x)$, $R(x)$ and $R'(u)$ represent the original image, two statistically independent random phase masks, where x and u are coordinates of the input plane and Fourier plane, respectively. $E(x)$, $P(x)$ and $P'(u)$ are the encrypted result and the two asymmetric private keys generated in the encryption process. The original image can be faithfully recovered only in the case that two private keys and the encrypted result, i.e., an approximation of a fake image, are available for authorized receivers.

The optical setup of linear DRPE is used for decryption. The encrypted image is located at the input plane of the optical processor, as shown in Fig. 2. An intensity-sensitive device such as a CCD camera can be used to record the distribution of intensity in the output plane of the decryption system since the primary image is real and positive. The decrypted image, i.e., the square root of the distribution of intensity, can be written as follows:

$$D(x) = \mathrm{PT}\{\mathrm{IFT}[\mathrm{FT}[E(x)P(x)] \cdot P'(u)]\} \tag{1}$$

where the operators FT[], IFT[]and PT{} denote the Fourier transform, the inverse Fourier transform and phase truncation, respectively. Phase truncation on a complex function here means retaining the amplitude part of the function but truncating its phase part.

Now we show how to produce the three components $E(x)$, $P(x)$ and $P'(u)$ in Eq. (1) by reverse-engineering the modified amplitude-phase retrieval-based attack under the framework of phase-truncated DRPE [29]. The flowchart of the algorithm is shown in Fig. 3, where the target image and the fake image are two constraints for iterations and the symbol $\otimes$ represents multiplication. For convenience, the iteration process is divided into two parts, i.e., encryption unit (EU) and decryption unit (DU). In the first iteration, the two public keys are used as two initial encryption phase keys (EPKs). During each iteration of the algorithm, two DPKs are generated in EU and are used in decryption unit (DU) to produce the EPKs for the next iteration. At the end of the iteration process, the target image $I(x)$ is finally encoded into an amplitude image $E(x)$ through EU.

In the kth ($k = 1, 2, 3, \ldots$) iteration, the amplitude distribution in the Fourier plane in EU can be written as follows:

$$g_k(u) = \mathrm{PT}\{\mathrm{FT}[I(x)R_k(x)]\} \tag{2}$$

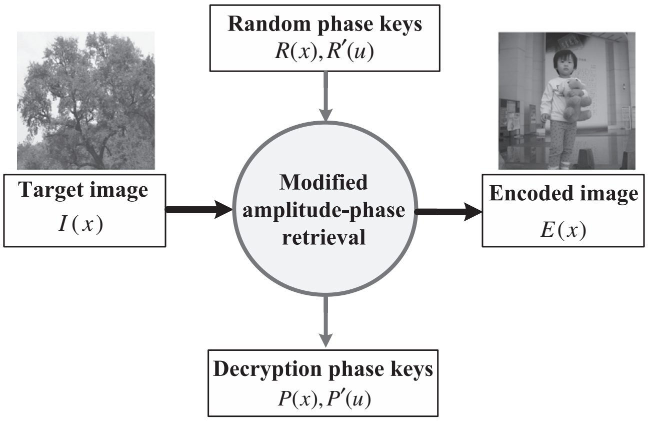

Fig. 1. Synoptic diagram of the encryption system.

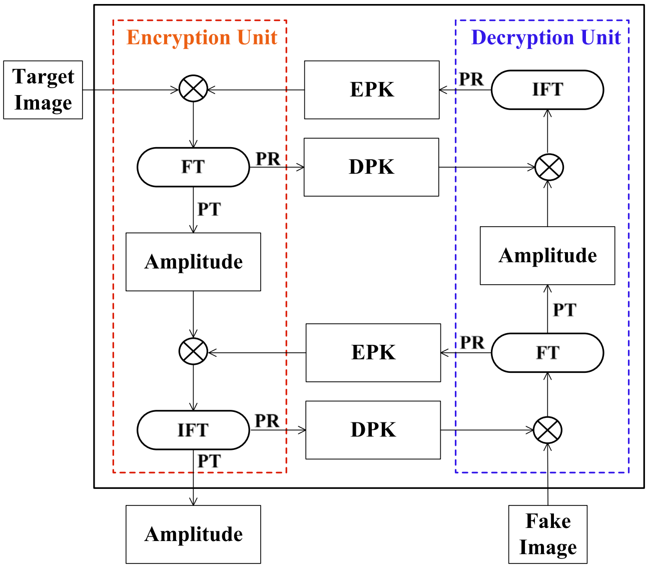

Fig. 3. Flowchart of the modified amplitude-phase retrieval algorithm based on phase-truncated DRPE architecture. EPK: encryption phase key; DPK: decryption phase key.

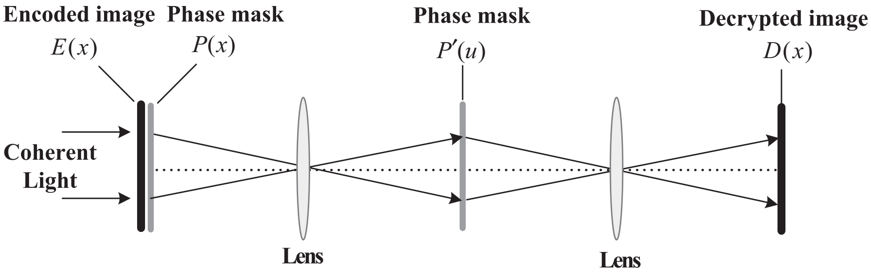

Fig. 2. Optical system for decryption.