Optics Communications 317 (2014) 7–12

Contents lists available at ScienceDirect

Optics Communications

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

A hybrid attack on 'double images encryption method with resistance against the specific attack based on an asymmetric algorithm'

Deng Xiaopeng

Department of Physics and Information Engineering, Huaihua University, Huaihua 418008, China

ARTICLE INFO

Article history:
Received 3 September 2013
Received in revised form
15 November 2013
Accepted 29 November 2013
Available online 13 December 2013

Keywords:
Optical information processing
Image encryption
Hybrid attack
Iteration

ABSTRACT

A hybrid attack method, which is based on an iteration process and the decisive role of phase in the propagation process of light, is proposed to break the double image encryption system based on a nonlinear algorithm. The whole attack process contains three steps. First, an approximate value of the encoded image is achieved by using the phase retrieval algorithm when the encryption key, placed in the Fourier spectrum plane, and the ciphertext are used as the two constraints. Then, an approximate value of the joint power spectrum (JPS) is obtained based on the result of the first step. Finally, two approximate values of the original images are obtained by the use of the approximate value of the JPS and other two encryption keys. The simulation results show that the hybrid attack is valid and the cryptosystem is vulnerable to this attack.

1. Introduction

With the rapid development of modern communication techniques and computer network techniques information security has become an important issue. Optical image encryption technology is an attractive alternative in information security owing to its inherent ability of multiple parameters and parallel operation. Various optical image encryption methods have been proposed [1–13] since the double random phase encoding technology was reported by Refregier and Javidi [13]. However, to be the best our knowledge, most of these encoding methods belong to the linear symmetric encrypting system, in which the encryption key is the same as the decryption key. From the point of view of cryptography, the linear encrypting system would suffer from several problems such as all kinds of attacks. In order to overcome these problems, a nonlinear cryptosystem based on phase-truncated Fourier transforms (PTFTs) was proposed by Qin and Peng [11]. And then some nonlinear cryptosystem methods based on PTFTs have been proposed [14–20]. Although the nonlinear cryptosystem has very high robustness against existing attacks owing to the nonlinear operation of phase truncation, the PTFT-based encoding system recently has been found to be vulnerable to a specific attack based on the iterative Fourier transforms [21]. To avoid the specific attack and realize double-image encryption, Wang and Zhao proposed a double-image encryption technique based on a nonlinear algorithm, in which the encryption process is different from the decryption and the encryption keys are also different from the decryption keys [22]. In this nonlinear encrypting method, phase truncation of a joint Fourier transform is used to transform two images into a noise image in the encryption process [22]. The authors claimed that the cryptosystem has a high level of robustness against some common attacks, including brute force attacks, known plaintext attack and known encryption key attack [22]. However, the cryptosystem will still be placed into a more exposed and vulnerable position if one tries to use the encryption keys to recover the plaintexts.

In this paper, we propose a hybrid attack method to try to reveal the encrypted information based on an iteration process and the decisive role of phase in the propagation process of light [23]. In the attack method discussed in this paper, an approximate value of the encoded image is first achieved by using the phase retrieval algorithm when the encryption key, placed in the Fourier spectrum plane, and the ciphertext are used as the two constraints. Then, an approximate value of the joint power spectrum (JPS) is obtained based on the approximate value of the encoded image. Finally, two approximate values of the original images are obtained by the use of the approximate value of the JPS and other two encryption keys. Unfortunately, the simulation results show that the cryptosystem is vulnerable to this attack. Because the whole attack process contains two different attack ways, we refer to this as a hybrid attack. In the following sections, we will show how the cryptosystem is vulnerable to the hybrid attack. It is worth pointing out that in this paper the three phrases "asymmetric algorithm", "public key", and "private key", which appear in Refs. [11,21,22], have been changed to the three phrases "nonlinear algorithm", "encryption key", and "decryption key", respectively, the purpose of which is to avoid confusion because the cryptosystems mentioned in Refs. [11,21,22] are not real asymmetric cryptosystems.

E-mail address: dxpzqh@163.com

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.11.055

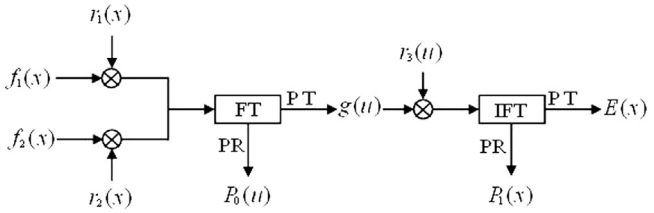

Fig. 1. Flowchart of the double images encryption based on nonlinear algorithm.

2. Double images encryption based on a nonlinear algorithm

First, let us briefly review the double images encryption based on a nonlinear algorithm [22], the encrypting process can be shown in Fig. 1. Two original images $f_1(x)$, $f_2(x)$ that located in the position $(a_1,0)$, $(-a_1,0)$ are combined with $r_1(x)$ and $r_2(x)$, respectively. Thus the input image can be expressed as

$$f(x)=[f_1(x)\times r_1(x)]*\delta(x-a_1)+[f_2(x)\times r_2(x)]*\delta(x+a_1), \tag{1}$$

where $r_1(x)$ and $r_2(x)$ are two random phase masks, and the symbol $*$ denotes convolution operation. After the operation of joint Fourier transform, the Fourier spectrum $FT[f(x)]$ can be obtained. Then by performing phase truncation in the Fourier domain, the amplitude part and phase part can be separated from the Fourier spectrum and expressed as

$$g(u)=PT\{FT[f(x)]\}, \tag{2}$$

$$P_0(u)=PR\{FT[f(x)]\}, \tag{3}$$

where the operators $PT\{\bullet\}$, $FT\{\bullet\}$ and $PR\{\bullet\}$ denote phase truncation, Fourier transform and phase reservation, respectively [22].

By the same way, the final encrypting image $E(x)$ and its phase part $P_1(x)$ can be written as

$$E(x)=PT\{IFT[g(u)\cdot r_3(u)]\}, \tag{4}$$

$$P_1(x)=PR\{IFT[g(u)\times r_3(u)]\}, \tag{5}$$

where $IFT\{\bullet\}$ denotes inverse Fourier transform and $r_3(u)$ is another random phase mask.

It is can be seen from the above encrypting process that the encrypted images can be recovered if we use $P_1(x)$ and $P_0(x)$ as decryption keys. It also can be seen that the position parameter a_1 and $r_1(x)$, $r_2(x)$ and $r_3(u)$ (encryption keys) are not required for a correct decryption.

As mentioned in Ref. [22], the double images encrypting system can resist some common attacks, such as brute force attacks, known plaintext and chosen plaintext attacks because the cryptosystem is based on a nonlinear algorithm. Meanwhile, the cryptosystem also can resist the special attack because there are two primary images rather than one image in the input plane [22]. However, the cryptosystem will still be placed into a more exposed and vulnerable position if one tries to use the following attack to recover the plaintexts.

3. A hybrid attack on 'the double images encryption scheme based on a nonlinear algorithm'

The flowchart of the hybrid attacking algorithm is shown in Fig. 2. The hybrid attack can be described as the following three steps. The first step is to access $g'(u)$, which is an approximate value of the encoded image $g(u)$, by using the encryption key $r_3(u)$ and the ciphertext $E(x)$ based on the phase retrieval algorithm. The second step is to calculate $g'^2(u)$ which is an approximate value of the JPS. The third step is obtain the approximate values of the original images by using the approximate value $g'^2(u)$ of the JPS and other two encryption keys $r_1(x)$ and $r_2(x)$. In the following section, we will describe the three steps in detail.

Similar to the special attack discussed in Ref. [21], an iteration process is used to achieve the aim of the first step, where the encryption key $r_3(u)$ and the ciphertext $E(x)$ are used as the constraints in the input and output planes, respectively. After n rounds of iterations, an approximate value $g'(u)$ of the encoded image $g(u)$ can be obtained. The second step is to calculate $g'^2(u)$ which is an approximate value of the JPS. Because $g'(u)$ is an approximate value of $g(u)$, the approximate value $g'^2(u)$ of the JPS can be approximately expressed as

$$\begin{aligned} g'^2(u)\approx g^2(u)=&|F_1(u)*R_1(u)|^2+|F_2(u)*R_2(u)|^2\\ &+[F_1(u)*R_1(u)]^*[F_2(u)*R_2(u)]\exp(4\pi j a_1 u)\\ &+[F_1(u)*R_1(u)][F_2(u)*R_2(u)]^*\exp(-4\pi j a_1 u), \end{aligned} \tag{6}$$

where the superscript * denotes the complex conjugate, and $F_1(u)$, $F_2(u)$, $R_1(u)$ and $R_2(u)$ are the Fourier transformations of $f_1(x)$, $f_2(x)$, $r_1(x)$ and $r_2(x)$, respectively. It can be seen from (6) that the above expression actually represents the ciphertext of the joint transform correlator cryptosystem if $f_1(x)$ (or $f_2(x)$) is a constant [2]. In such a case, $f_1(x)$ (or $f_2(x)$) can be easily recovered by using the public key $r_2(x)$ (or $r_1(x)$) as the decrypting key [2]. Although here $f_1(x)$ and $f_2(x)$ are not constants, we can still approximately recover $f_1(x)$ and $f_2(x)$ respectively with the encryption key $r_2(x)$ and $r_1(x)$ as the decryption keys. The detailed analyses are as follows.

As we known, the Fourier frequency spectrum of the positive image is usually more concentrated, and the phase plays a decisive role in the propagation process of light [23]. So the Fourier transformation of $f_1(x)r_1(x)$(or $f_2(x)r_2(x)$) is mainly determined by $r_1(x)$ (or $r_2(x)$) if $f_1(x)$ and $f_2(x)$ are positive functions. Thus, we can obtain the following two approximate expressions

$$F_1(u)*R_1(u)\approx\delta(u)*R_1(u)=R_1(u), \tag{7}$$

$$F_2(u)*R_2(u)\approx\delta(u)*R_2(u)=R_2(u). \tag{8}$$

In order to recover $f_1(x)$, the encryption key $r_2(x)$ is placed in the centre of the input plane of the $4f$ system and Fourier transformed. And then the Fourier transformation of $r_2(x)$ is multiplied with Eq. (6) in Fourier plane to get the filtered result

$$\begin{aligned} g'^2(u)R_2(u)\approx g^2(u)R_2(u)=&\{|F_1(u)*R_1(u)|^2+|F_2(u)*R_2(u)|^2\}R_2(u)\\ &+R_2(u)[F_1(u)*R_1(u)]^*[F_2(u)*R_2(u)]\exp(4\pi j a_1 u)\\ &+R_2(u)[F_1(u)*R_1(u)][F_2(u)*R_2(u)]^*\exp(-4\pi j a_1 u). \end{aligned} \tag{9}$$

According to Eq. (8), the third term in Eq. (9) can be approximately rewritten as

$$\begin{aligned} g_3(u)\approx g'_3(u)&=R_2(u)[F_1(u)*R_1(u)]R^*{}_2(u)\exp(-4\pi j a_1 u)\\ &=F_1(u)*R_1(u)\exp(-4\pi j a_1 u). \end{aligned} \tag{10}$$

After the operation of inverse Fourier transform, an approximation of $f_1(x)$ can be obtained and expressed as

$$f'_1(x)\approx IFT[g'_3(u)]=|[f_1(x)r_1(x)]\otimes\delta(x-2a)|=f_1(x-2a). \tag{11}$$

By the same way, an approximation of $f_2(x)$ can be obtained by using the other encryption key $r_1(x)$ and expressed as

$$f'_2(x)\approx|[f_2(x)r_2(x)]\otimes\delta(x+2a)|=f_2(x+2a). \tag{12}$$

It can be seen from the above analyses that the two original images can be approximately recovered by the hybrid attack if an attacker knows the three encryption keys and the ciphertext.