Optik 126 (2015) 2832–2838

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A hybrid two-step attack on double-images nonlinear cryptosystem using phase truncation operation

Xiangling Ding[a,b], Guangyi Chen[c], Gaobo Yang[a,*]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha Hunan 410082, PR China
[b] Department of Physics and Information Engineering, Huaihua University, Huaihua 418008, China
[c] College of Information Science and Technology, Hunan Agricultural University, Changsha 410128, China

ARTICLE INFO

Article history:
Received 21 May 2014
Accepted 2 July 2015

Keywords:
Hybrid two-step attack
Iterative algorithm
Nonlinear cryptosystem
Phase truncation operation

ABSTRACT

In this paper, a hybrid two-step attack strategy is proposed to break the double-images nonlinear encryption system using phase truncation operation. The attack process is composed of two steps. First, an iterative algorithm is exploited to obtain an approximate value of the encoded image when the ciphertext and the encryption key are placed on the input plane and the output plane, respectively. Second, two approximate values of the original images are achieved by the use of decryption key, which is generated by another two encryption keys. Simulation results show that the proposed hybrid attack strategy can effectively attack the existing double-images nonlinear cryptosystem.

1. Introduction

Over the last few decades, many optical cryptosystems based on the double random phase encoding technique (DRPE) [1], which is first presented by Refregier and Javidi in 1995, have been proposed, such as Fresnel encryption system [2], fractional Fourier-transform encryption system [3], and extended fractional Fourier-transform encryption system [4], etc [5,6]. However, some simulations and verifications on the DRPE have revealed that it is fragile to various attacks, such as the known plaintext attack [7], chosen plaintext attack [8] and chosen ciphertext attack [9], simply because DRPE belongs to the category of linear cryptosystems. In order to resist these attacks, Wan and Peng have recently proposed a nonlinear cryptosystem based on phase-truncated Fourier transforms (PTFTs) to remove the linearity of DRPE by the nonlinear operation of phase truncation [10]. It can achieve high robustness against existing attacks owing to the nonlinear operation of phase truncation. However, it still has been found to be vulnerable to specific attack based on the iterative Fourier transforms [11]. Meanwhile, several security-enhanced encryption schemes have been proposed to resist against the above-mentioned attack [12–16]. In a recent enhancement nonlinear cryptosystem, Wang et al. have proposed a double-images nonlinear encryption scheme, in which the encryption process is quite different from the decryption and the encrypting keys are different from the decrypting keys as well [12]. It is reported that the nonlinear cryptosystem has a strong robustness against some common attacks, such as the known plaintext attack, chosen plaintext attack and chosen ciphertext attack [12]. Thus, there is no doubt that proposing attacks on the double-images nonlinear cryptosystem can have great significance. Then, we observe that the double-images nonlinear cryptosystem is not as robust and secure as it describes, especially it is vulnerable to a hybrid two-step attack.

In this paper, a hybrid two-step strategy is proposed to retrieve the original double-images information based on an iterative algorithm and the decryption key. The attack process consists of two steps: an approximate value of the enciphering image is achieved in the first step by using the iterative algorithm when the ciphertext and the encryption key are place on the input and the output plane, respectively. Two approximate values of the original images are obtained in the second step by using the decryption key, which is generated by another two encryption keys. Please note that the cryptosystems mentioned in Refs. [10–16] belong to the nonlinear encryption system even though they are not real asymmetric cryptosystems. To avoid confusing, the three keywords “asymmetric system”, “public key”, and “private key” in Refs. [10–16] are replaced with “nonlinear system”, “encryption key”, and “decryption key”, respectively.

The rest paper is organized as follows: Section 2 briefly introduces the double-images nonlinear encryption scheme based on phase truncation operation; Section 3 discusses the hybrid two-step attack on the double-images nonlinear cryptosystem.

* Corresponding author. Fax: +86 0731 88821341.
E-mail address: yanggaobo@hnu.edu.cn (G. Yang).

http://dx.doi.org/10.1016/j.ijleo.2015.07.004
0030-4026/

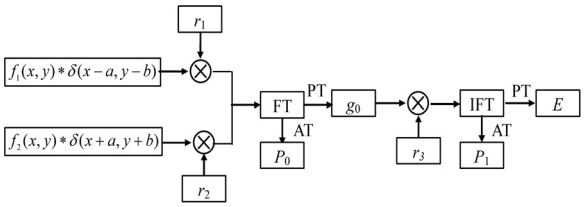

Fig. 1. Flowchart of encryption process with the double-images nonlinear encryption scheme.

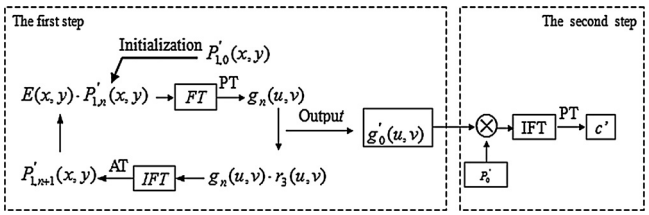

Fig. 2. Flowchart of hybrid two-step attack process.

Simulation results are presented in Section 4 and we conclude this paper in Section 5.

2. Double-images nonlinear encryption scheme based on phase truncation operation

The encryption process of double-images nonlinear encryption [12] is shown in Fig. 1, where the symbol $\otimes$ and $*$ represent the multiplication operation and the convolution operation, respectively. Let $f_1(x, y)$ and $f_2(x, y)$ be two original image to be encrypted, $r_1(x, y) = \exp[j\mu_1(x, y)]$, $r_2(x, y) = \exp[j\mu_2(x, y)]$ and $r_3(u, v) = \exp[j\mu_3(u, v)]$ are three random phase encryption keys where $\mu_1(x, y)$, $\mu_2(x, y)$ and $\mu_3(u, v)$ are white sequences statistically independent in the interval $[0, 2\pi]$. Two original images $f_1(x, y)$ and $f_2(x, y)$, which located in the position (a, b) and $(-a, -b)$ of the same plane along the axis x and the axis y, are combined with two different random phase encryption keys $r_1(x, y)$ and $r_2(x, y)$, respectively, into a gray image. Thus the input information can be expressed as:

$$f(x,y) = [f_1(x,y)\cdot r_1(x,y)] * \delta(x-a, y-b) + [f_2(x,y)\cdot r_2(x,y)] * \delta(x+a, y+b) \quad (1)$$

where the symbol $*$ represents the convolution operation.

Through Fourier transform and nonlinear operation of phase-truncation, the amplitude part and phase part can be achieved from the Fourier spectrum and described as

$$g_0(u,v) = \mathrm{PT}\left\{\mathrm{FT}[f(x,y)]\right\} \quad (2)$$

$$P_0(u,v) = \mathrm{AT}\left\{\mathrm{FT}[f(x,y)]\right\} \quad (3)$$

where $\mathrm{PT}\{\bullet\}$, $\mathrm{AT}\{\bullet\}$ and $\mathrm{FT}\{\bullet\}$ denote phase-truncation, amplitude-truncation and Fourier transform, respectively.

In the same way, the final ciphertext $E(x, y)$ and its phase part can be obtained by the following step

$$E(x,y) = \mathrm{PT}\left\{IFT[g_0(u,v)\cdot r_3(u,v)]\right\} \quad (4)$$

$$P_1(x,y) = \mathrm{AT}\left\{\mathrm{IFT}[g_0(u,v)\cdot r_3(u,v)]\right\} \quad (5)$$

where $\mathrm{IFT}\{\bullet\}$ denotes inverse Fourier transform and $R_3(u, v)$ is another random phase encryption key.

Seen from above encryption process, the decrypted result can be deciphered by using the decryption keys $P_1(x, y)$ and $P_0(u, v)$. The process can be depicted as follows

$$g_0(u,v) = \mathrm{PT}\left\{FT[E(x,y)\cdot P_1(x,y)]\right\} \quad (6)$$

$$c(x,y) = \mathrm{PT}\left\{\mathrm{IFT}[g_0(u,v)\cdot P_0(u,v)]\right\} \quad (7)$$

where $c(x, y)$ contains the information of the two primary images and can be described as $f_1(x, y) * \delta(x - a, y - b) + f_2(x, y) * \delta(x + a, y + b)$. Furthermore, two primary images can be extracted from the decrypted result.

As mentioned in [12], the double-images nonlinear encryption system can resist several attacks, such as: brute force attack, chosen plaintext attacks, known public key attack and known plaintext attack because of the nonlinear phase-truncated Fourier transform. Meanwhile, the cryptosystem can also resist the iterative attack [11] because there are two primary images rather than one image in the input plane. However, it will be demonstrated that the double-images nonlinear cryptosystem is vulnerable to a hybrid two-step attack in the following section.

3. A hybrid two-step attack on the double-images nonlinear cryptosystem

The flowchart of the attack process is shown in Fig. 2, where the symbol $\otimes$ represents the multiplication operation. It can be completed by a two-step approach which can be described as follows: the first step is to access $g'_0(u, v)$ which is an estimate of $g_0(u, v)$ by using an encryption key $R_3(u, v)$ and the ciphertext $E(x, y)$ based on iterative algorithm, and the second step is to achieve estimate double-images $c'(x, y)$ of the original double-images $c(x, y)$ by using $g'_0(u, v)$ and decryption key $P'_0(u, v)$, generated by another two encryption keys $r_1(x, y)$ and $r_2(x, y)$ that are used in

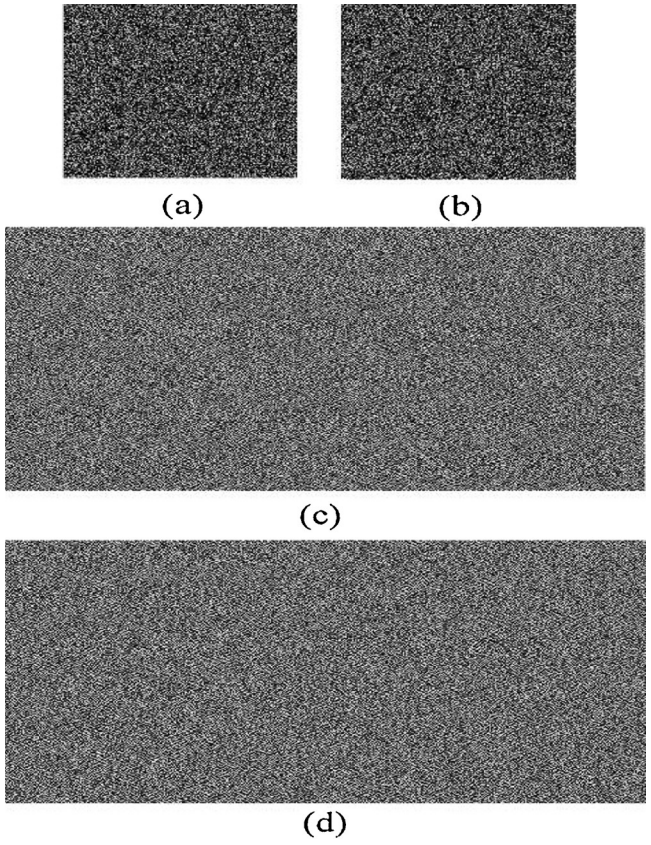

Fig. 3. The phase part of three encryption keys (a) $R_1(x, y)$; (b) $R_2(x, y)$; (c) $R_3(u, v)$ and the phase part of the decryption key (d) $P'_0(u, v)$.