Optics Communications 346 (2015) 141–148

Contents lists available at ScienceDirect

Optics Communications

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

A simple public-key attack on phase-truncation-based double-images encryption system

Xiangling Ding [a,b], Gaobo Yang [a,*], Dajiang He [b]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan 410082, PR China
[b] The Key Laboratory of Intelligent Control Technology for Ecological Agriculture in Wuling Mountain Areas of Hunan Province, HuaiHua University, Huaihua, Hunan 418008, PR China

ARTICLE INFO

Article history:
Received 17 December 2014
Received in revised form
5 February 2015
Accepted 7 February 2015
Available online 14 February 2015

Keywords:
Public-key attack
Optical security
Nonlinear cryptosystem
Phase truncation operation

ABSTRACT

Phase-truncation based double-images cryptosystem can avoid the iterative Fourier transforms and realize double-images encryption. In this paper, a simple public-key attack is proposed to break this cryptosystem by using arbitrary position parameters and three public keys. The attack process is composed of two steps. Firstly, the decryption keys are simply generated with the help of arbitrary position parameters and the three public keys. Secondly, the two approximate values of the original images are obtained by using the generated decryption keys. Moreover, the proposed public-key attack is different from the existing attacks. It is not sensitive to position parameters of the double-images and the computing efficiency is also much better. Computer simulation results further prove its vulnerability.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Since the double random phase encoding technology was reported by Refregier and Javidi in 1995 [1], various optical cryptosystems for information security have been proposed then. These optical encryption algorithms cover many field such as Fresnel [2,3], fractional Fourier [4,5], and Fresnel diffraction [6]. However, some simulations and verifications on most of these encoding algorithms had revealed that they are prone to some attacks. These attacks include the known plaintext attack [7], the chosen plaintext attack [8] and the chosen ciphertext attack [9]. In order to overcome these attacks, Qin and Peng proposed a nonlinear cryptosystem based on the phase truncation [10]. This technique can achieve high robustness of the system against aforementioned attacks, but still it has been found to be fragile to the specific attack based on the iterative Fourier transforms [11]. Subsequently, some enhanced encryption techniques [12–16] have been proposed to avoid the specific attack. In these techniques, there is a double-images nonlinear encryption technique presented by Wang et al [12]. It was reported that two primary images were transformed into a noisy image by phase truncation of a joint Fourier transform. Although the authors claimed that the cryptosystem has a high level of robustness against some common attacks, a hybrid attack method [17] is proposed to break down the double-images encryption system. In this attack method, it needs a lot of time to be accomplished in the first step by using the amplitude-phase retrieval algorithm and also employs the original position parameters in the third step by using the joint power spectrum. Therefore, a new attack method, which does not need the original position parameters and the computation-intensive amplitude-phase retrieval algorithm, is worthy of further investigation.

In this paper, we propose a simple public-key attack strategy on phase-truncation-based double-images cryptosystem to retrieve the main information of the double-images. The attack process consists of two steps. In the first step, two decryption keys are simply generated by the three public keys using arbitrary position parameters. The approximate values of the original double-images are obtained in the second step by using the two decryption keys generated in the first step. Compared to the hybrid attack method [17], the new attack method does not need the original position parameters and the computing efficiency is much better due to not applying the amplitude-phase retrieval algorithm. Particularly, arbitrary position parameters could also result into a recognizable recovered image. Moreover, because the attack process is as the same as the decryption process of the double-images nonlinear cryptosystem, it can be easily implemented in optics. Numerical simulations are demonstrated to show the feasibility and effectiveness of the new method of attack.

2. Double-images nonlinear cryptosystem based on phase truncation operation

The flowchart of the double-images nonlinear cryptosystem [12] is shown in Fig. 1, where the symbol ⊗ and ∗ represent the

* Corresponding author.
E-mail address: yanggaobo@hnu.edu.cn (G. Yang).

http://dx.doi.org/10.1016/j.optcom.2015.02.014
0030-4018/© 2015 Elsevier B.V. All rights reserved.

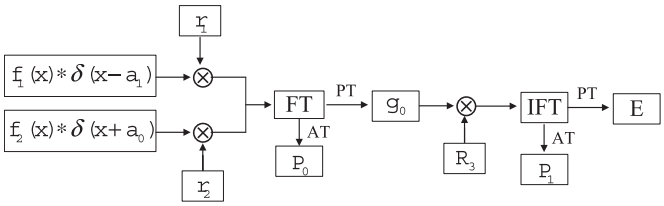

Fig. 1. Flowchart of the double-images encryption scheme.

multiplication operation and the convolution operation, respectively. For the sake of simplicity, one-dimensional notation is used to illustrate this concept. Let $f_1(x)$ and $f_2(x)$ be two original images to be encrypted, $r_1(x) = \exp[j\mu_1(x)]$, $r_2(x) = \exp[j\mu_2(x)]$ and $R_3(x) = \exp[j\mu_3(x)]$ are three public keys where $\mu_1(x)$, $\mu_2(x)$ and $\mu_3(x)$ are white sequences statistically independent in the interval $[0, 2\pi]$, FT{•} the operator of Fourier transform, IFT{•} the operator of inverse Fourier transform, PT{•} the operator of phase truncation, which means only the amplitude part of the Fourier spectrum is retained while the phase part of the spectrum is truncated, and AT{•} the operator of amplitude truncation, which means only the phase part of the Fourier spectrum is retained while the amplitude part of the spectrum is truncated. Let a Fourier transformation be $F(u) = \mathrm{FT}[f(x)] = |F(u)|\exp(i2\pi\phi(u))$, the phase truncation and the amplitude truncation can be respectively expressed as $\mathrm{PT}[F(u)] = |F(u)|$ and $\mathrm{AT}[F(u)] = \exp(i2\pi\phi(u))$ [10]. Two original images $f_1(x)$ and $f_2(x)$, which located in the position (a_0 and $-a_0$) of the same plane along the x-axis, are combined with two different public keys ($r_1(x)$ and $r_2(x)$) respectively into a gray image. Thus the input information can be expressed as

$$f(x) = [f_1(x)\cdot r_1(x)]_*\delta(x - a_0) + [f_2(x)\cdot r_2(x)]_*\delta(x + a_0) \quad (1)$$

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

$$g_0(u) = \mathrm{PT}\{\mathrm{FT}[f(x)]\} \quad (2)$$

$$P_0(u) = \mathrm{AT}\{\mathrm{FT}[f(x)]\} \quad (3)$$

In the same way, the final ciphertext $E(x)$ and its phase part can be obtained through the following steps:

$$E(x) = \mathrm{PT}\{\mathrm{IFT}[g_0(u)\cdot R_3(u)]\} \quad (4)$$

$$P_1(x) = \mathrm{AT}\{\mathrm{IFT}[g_0(u)\cdot R_3(u)]\} \quad (5)$$

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

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

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

where $c(x)$ contains the information of the two primary images

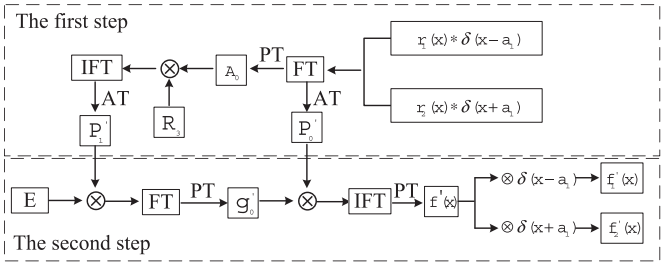

Fig. 2. The block diagram of the public-key attack process.

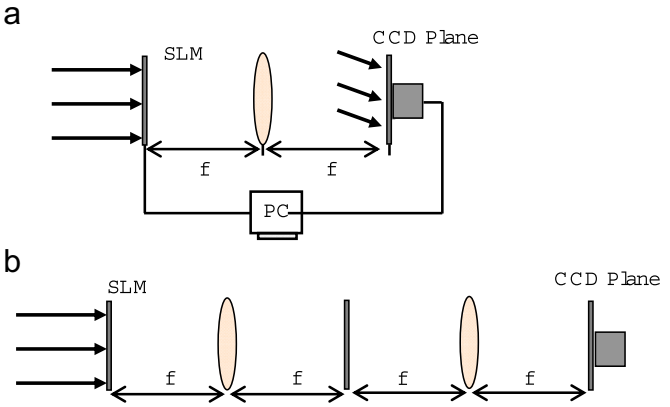

Fig. 3. Optical (a) decryption keys generation setups and (b) crack setups of the public-key attack process.

and can be described as $f_1(x)_*\delta(x - a_0) + f_2(x)_*\delta(x + a_0)$. Furthermore, with position multiplexing technique [6] two primary images can be extracted from the decrypted result.

As mentioned in [12], the double-images nonlinear cryptosystem can resist several attacks such as brute force attack, chosen plaintext attack and known plaintext attack because of the nonlinear phase-truncated Fourier transform. Meanwhile, the cryptosystem can also resist the specific 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 public-key attack in the below following section.

3. A simple public-key attack on the double-images nonlinear cryptosystem

The block diagram of the attack process is shown in Fig. 2. It can be completed by a two-step approach which can be described as follows: the first step employs two arbitrary position parameters (a_1 and $-a_1$) and the three public keys ($r_1(x)$, $r_2(x)$ and $R_3(x)$) to obtain two decryption keys $P_0(u)$ and $P_1(x)$. The second step is to achieve the approximate values of the original double-images by using the two generated decryption keys $P_0(u)$ and $P_1(x)$. In the following paragraphs, we will explain the two steps in detail.

The first step can be accomplished by using two arbitrary position parameters (a_1 and $-a_1$) and the three public keys ($r_1(x)$, $r_2(x)$ and $R_3(x)$) to obtain two decryption keys $P_0(u)$ and $P_1(x)$. Note that the position (a_1 and $-a_1$) are different from the original position (a_0 and $-a_0$), which used in the encryption process of the double-images cryptosystem. Firstly, the two public keys ($r_1(x)$ and $r_2(x)$) are located in the arbitrary position (a_1 and $-a_1$) respectively to form a composite image. Secondly, through employing the Fourier-transform, the phase-truncation operation and the amplitude-truncation operation on the composite image, the decryption key $P_0(u)$ and the amplitude part $A_0(u)$ can be obtained as follows:

$$P_0(u) = \mathrm{AT}\{\mathrm{FT}[r_1(x)_*\delta(x - a_1) + r_2(x)_*\delta(x + a_1)]\} \quad (8)$$

$$A_0(u) = \mathrm{PT}\{\mathrm{FT}[r_1(x)_*\delta(x - a_1) + r_2(x)_*\delta(x + a_1)]\} \quad (9)$$

Finally, the amplitude part $A_0(u)$ is bonded with the third public key $R_3(x)$, and its inverse Fourier transform is obtained. This spectrum is divided into an amplitude and phase part then. Its phase part is used as another decryption key $P_1(x)$ and it can be expressed as follows:

$$P_1(x) = \mathrm{AT}\{\mathrm{IFT}[A_0(u)\cdot R_3(u)]\} \quad (10)$$

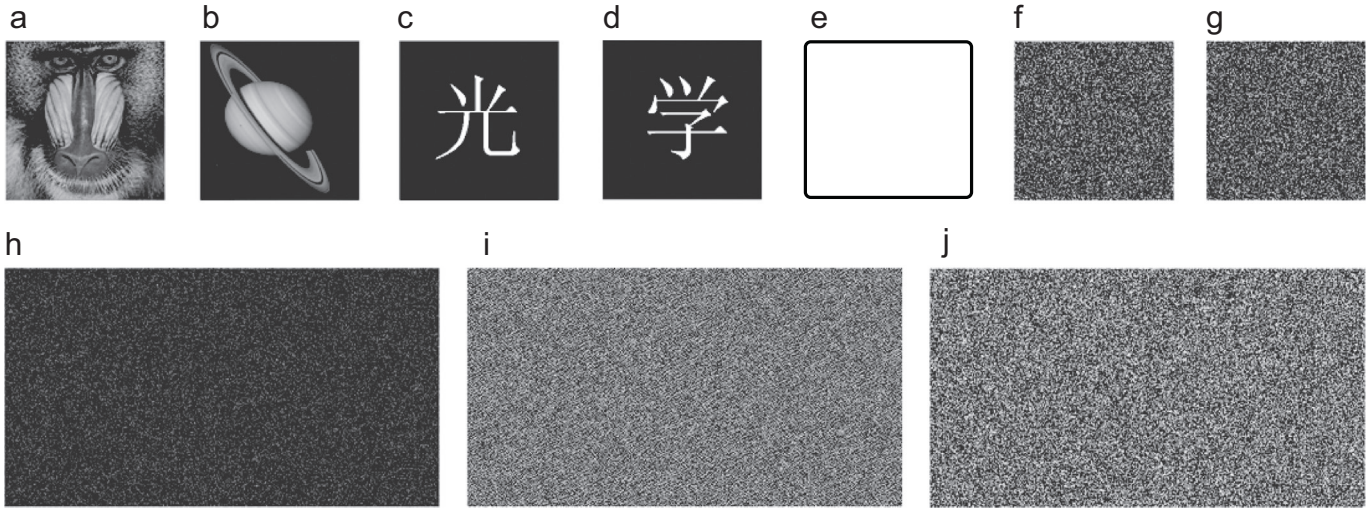

Fig. 4. (a), (b) gray-scale image; (c), (d) binary image; (e) a fixed value image; the phase part of three encryption keys (f) ; (g) ; (h) and the phase part of the two decryption key (i) ; (j).

The second step, which is as the same as the decryption process of the double-images nonlinear cryptosystem, is to achieve the approximate values of the original double-images by using the generated decryption keys ($P_0(u)$ and $P_1(x)$). After substituting $P_1'(x)$ for $P_1(x)$ and $P_0'(u)$ for $P_0(u)$ in Eqs. (6) and (7) respectively, we can achieve the approximate encoded result $g_0'(u)$ and the approximate attacked result as presented below:

$$g_0'(u) = \mathrm{PT}\{\mathrm{FT}[E(x)\cdot P_1'(x)]\} \tag{11}$$

$$c'(x) = \mathrm{PT}\{\mathrm{IFT}[g_0'(u)\cdot P_0'(u)]\} \tag{12}$$

Subsequently, through substituting Eq. (4) into Eq. (11), we can obtain

$$g_0'(u) \approx \mathrm{PT}(\mathrm{FT}\{\mathrm{PT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))\cdot P_1'(x)\}) \tag{13}$$

Further, Eq. (13) can be rewritten as

$$g_0'(u) \approx \mathrm{PT}\left(\mathrm{FT}\left\{\mathrm{PT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))\cdot \mathrm{AT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))\cdot \frac{1}{\mathrm{AT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))}\cdot P_1'(x)\right\}\right) \tag{14}$$

Because $\mathrm{IFT}(g_0(u)\cdot R_3(u)) = \mathrm{AT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))\cdot \mathrm{PT}(\mathrm{IFT}(g_0(u)\cdot R_3(u)))$ and Eq. (5), the relationship between $g_0'(u)$ and $g_0(u)$ can be derived from Eq. (14) as follows:

$$g_0'(u) \approx \mathrm{PT}(\mathrm{FT}\{\mathrm{IFT}[g_0(u)\cdot R_3(u)]\cdot W_1(x)\}) \tag{15}$$

where $W_1(x)$ is an error-function given by

$$W_1(x) = \frac{P_1'(x)}{P_1(x)} = \frac{\mathrm{AT}\{\mathrm{IFT}[A_0(u)\cdot R_3(u)]\}}{\mathrm{AT}\{\mathrm{IFT}[g_0(u)\cdot R_3(u)]\}} \tag{16}$$

Through analyzing the relationship between $g_0'(u)$ and $g_0(u)$, we can then obtain that when $W_1(x)$ is close to 1, $g_0'(u) \approx g_0(u)$. In order to derive the relationship between the approximate values of the original double-images after the crack process and the original double-images, we firstly assume that $g_0'(u) \approx g_0(u)$ and the reason for which will be discussed in the next paragraphs. Therefore, Eq. (12) can be rewritten as

$$c'(x) = \mathrm{PT}\{\mathrm{IFT}[g_0(u)\cdot P_0'(u)]\} \tag{17}$$

Then, we substitute Eq. (2) into Eq. (17) and obtain the following:

$$c'(x) = \mathrm{PT}\{\mathrm{IFT}[\mathrm{PT}(\mathrm{FT}(f(x)))\cdot P_0'(u)]\} \tag{18}$$

Also, Eq. (18) can be rewritten as

$$c'(x) = \mathrm{PT}\left\{\mathrm{IFT}[\mathrm{PT}(\mathrm{FT}(f(x)))\cdot \mathrm{AT}(\mathrm{FT}(f(x)))\cdot \frac{1}{\mathrm{AT}(\mathrm{FT}(f(x)))}\cdot P_0'(u)]\right\} \tag{19}$$

Then we substitute $\mathrm{FT}(f(x)) = \mathrm{PT}(\mathrm{FT}(f(x)))\cdot \mathrm{AT}(\mathrm{FT}(f(x)))$ and Eq. (3) into Eq. (10) to obtain the below equation:

$$c'(x) \approx \mathrm{PT}(\mathrm{IFT}\{\mathrm{FT}[f(x)]\cdot W_2(u)\}) \tag{20}$$

where $W_2(u)$ is an error-function given by

$$W_2(u) = \frac{P_0'(u)}{P_0(u)} = \frac{\mathrm{AT}\{\mathrm{FT}[r_1(x)*\delta(x-a_1) + r_2(x)*\delta(x+a_1)]\}}{\mathrm{AT}\{\mathrm{FT}[[f_1(x)\cdot r_1(x)]*\delta(x-a_0) + [f_2(x)\cdot r_2(x)]*\delta(x+a_0)]\}} \tag{21}$$

When $W_2(u) \approx 1$, the relationship between the attack result and the original double-images can be inferred as follows:

$$c'(x) \approx \mathrm{PT}(\mathrm{IFT}\{\mathrm{FT}[f(x)]\cdot W_2(u)\}) \approx \mathrm{PT}(\mathrm{IFT}\{\mathrm{FT}[f(x)]\cdot 1\}) = \mathrm{PT}(f(x)) = c(x) \tag{22}$$

Further analysis about the relationship between $g_0'(u)$ and $g_0(u)$ and the relationship between $c'(x)$ and $c(x)$ are discussed as following below:

As described in Ref. [18], the Fourier frequency spectrum is usually more concentrated, and the phase part plays a more important role for reconstructing an image. Therefore $A_0(u)\cdot R_3(u)$, $g_0(u)\cdot R_3(u)$, $f_1(x)\cdot r_1(x)$ and $f_2(x)\cdot r_2(x)$ are dominated by $R_3(u)$, $R_3(u)$, $r_1(x)$ and $r_2(x)$ respectively when the Fourier frequency spectrum ($A_0(u)$ and $g_0(u)$) are concentrated and original images ($f_1(x)$ and $f_2(x)$) belong to the non-negative images. Then, we can obtain four approximate values as follows:

$$\mathrm{IFT}[A_0(u)\cdot R_3(u)] \approx \delta(x)*r_3(x) \approx r_3(x) \tag{23}$$

$$\mathrm{IFT}[g_0(u)\cdot R_3(u)] \approx \delta(x)*r_3(x) \approx r_3(x) \tag{24}$$

$$\mathrm{FT}[f_1(x)\cdot r_1(x)] = F_1(u)*R_1(u) \approx \delta(u)*R_1(u) \approx R_1(u) \tag{25}$$

$$\mathrm{FT}[f_2(x)\cdot r_2(x)] = F_2(u)*R_2(u) \approx \delta(u)*R_2(u) \approx R_2(u) \tag{26}$$

From this we can infer that $W_1(x)$ is close to 1 because of

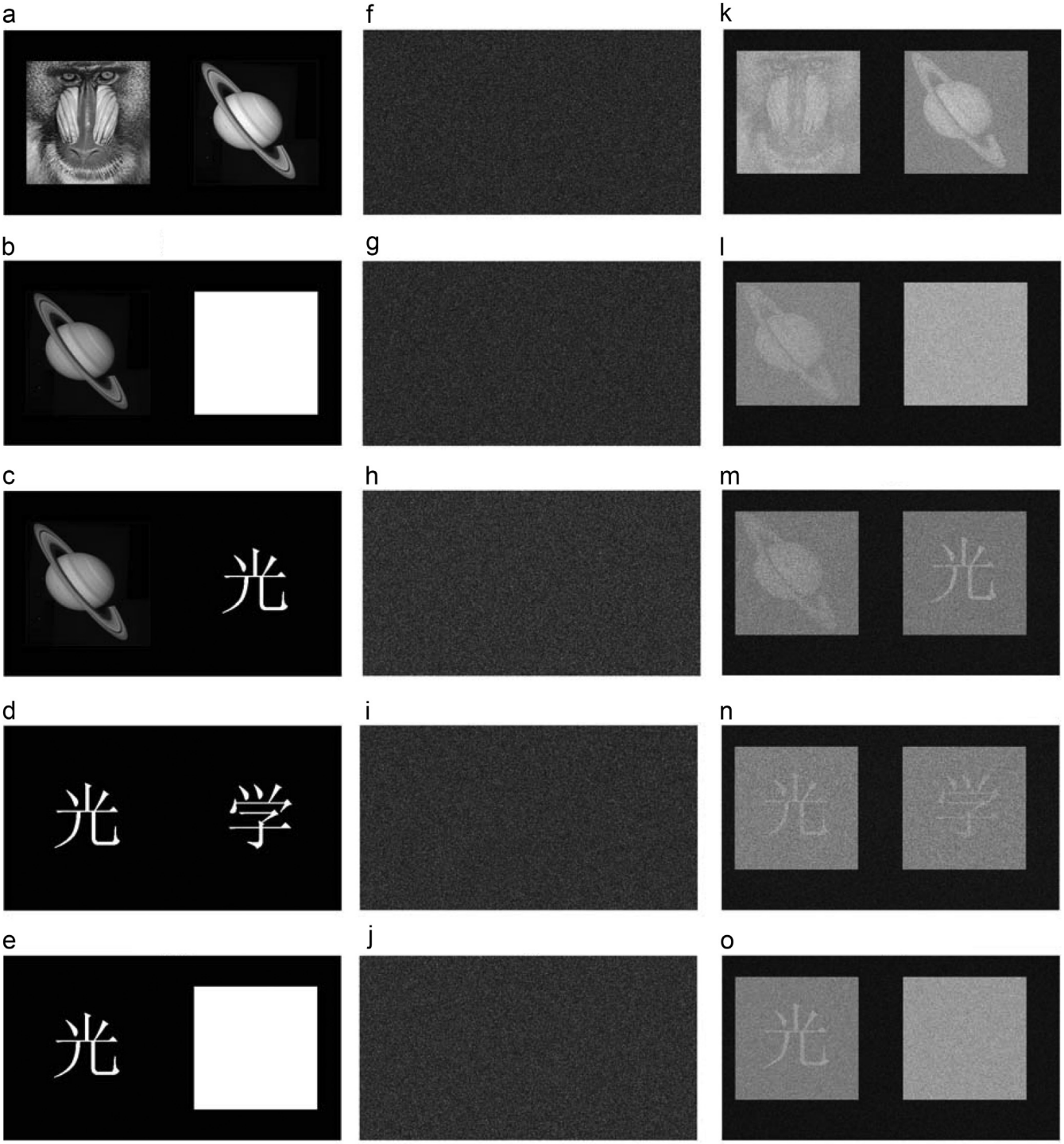

Fig. 5. (a)–(e) five cases of double-images; (f)–(j) the corresponding ciphertexts to (a)–(e); (k)–(o) the corresponding attack results.

$\mathrm{IFT}[A_0(u)\cdot R_3(u)] \approx \mathrm{IFT}[g_0(u)\cdot R_3(u)]$ and then $g_0'(u) \approx \mathrm{PT}(\mathrm{FT}\{\mathrm{IFT}[g_0(u)\cdot R_3(u)]\cdot 1\}) = \mathrm{PT}[g_0(u)\cdot R_3(u)] = g_0(u)$. That is, we obtain a good encoded result $g_0'(u)$ [19]. Meanwhile, $\mathrm{FT}[[f_1(x)\cdot r_1(x)]_*\delta(x-a_0)+[f_2(x)\cdot r_2(x)]_*\delta(x+a_0)] \approx \mathrm{FT}[r_1(x)_*\delta(x-a_0)+r_2(x)_*\delta(x+a_0)]$, $\mathrm{FT}[r_1(x)_*\delta(x-a_1)+r_{2*}\delta(x+a_1)] = \mathrm{FT}[r_1(x)_*\delta(x-a_0)]\cdot\delta(x-a_1+a_0)+\mathrm{FT}[r_2(x)_*\delta(x+a_0)]\cdot\delta(x+a_1-a_0)$. Therefore, it can be deduced from above that $R_1(u)$ and $R_2(u)$ in the $W_2(u)$ have the position offset of (a_1-a_0) and $-(a_1-a_0)$ respectively, and then the position offset propagate to the Fourier operation result of $c(x)$, which result into the position of $f_1(x)$ from a_0 to a_1 and the position of $f_2(x)$ from $-a_0$ to $-a_1$. Finally, as the same as the last step of the double-images decryption process, with position multiplexing technique [6] and two arbitrary positions (a_1 and $-a_1$) the main information of two primary images ($f_1(x)$ and $f_2(x)$) can be easily extracted from the attack result $c'(x)$.

From the attack processes as discussed above, it can be seen that the two original primary images can be approximately obtained when the attacker has intercepted and captured the ciphertext and the three public keys. Meanwhile, compare to [17], our proposed attack method does not require the original position

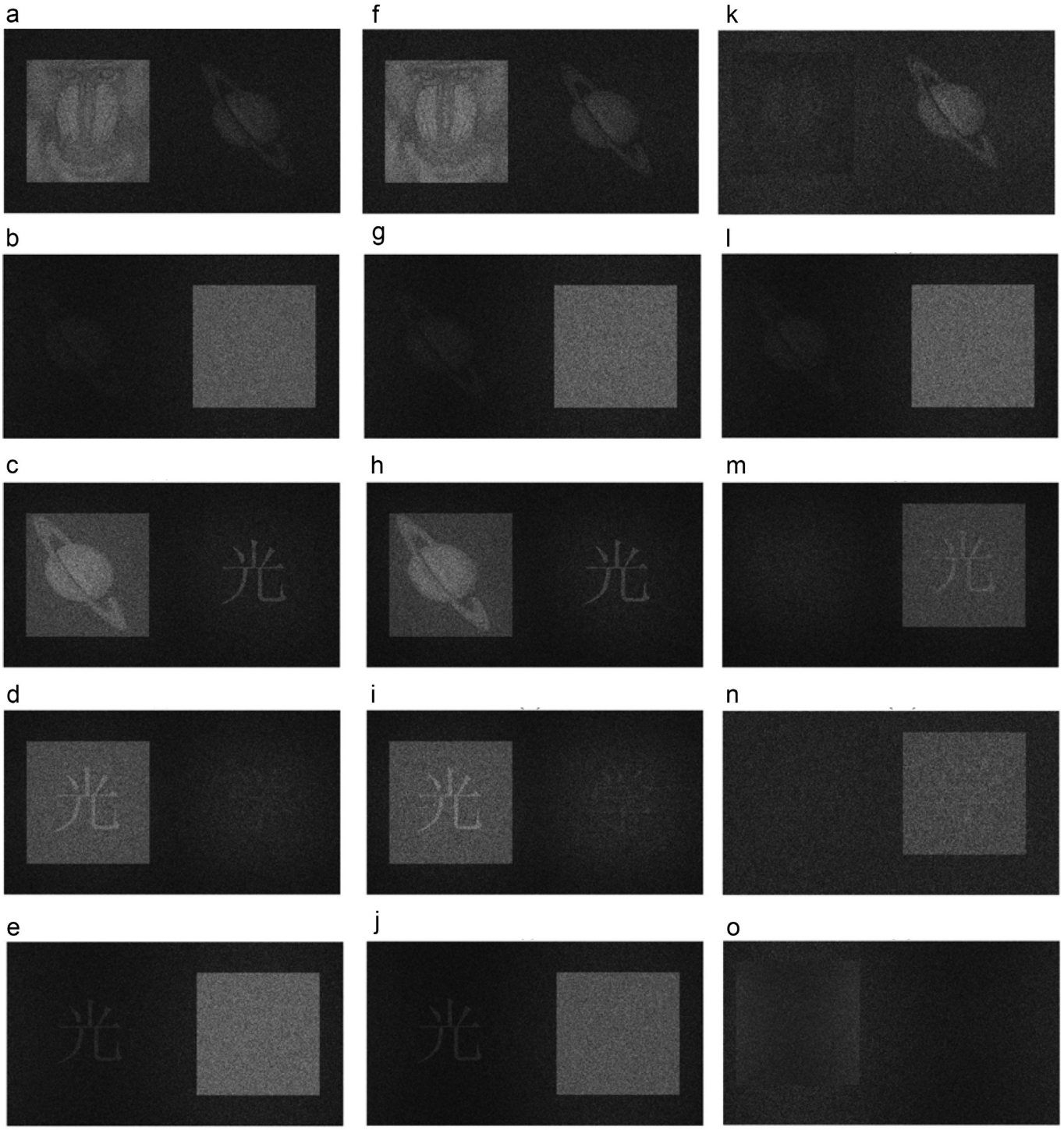

Fig. 6. The cracked results of the hybrid attack (a)–(e) with original position parameters and iteration number is 30; (f)–(j) with original position parameters and iteration number is 300; (k)–(o) with arbitrary position parameters and iteration number is 300.

(a_0 and $-a_0$) and the algorithmic complexity and time consumption is much better than by [17], which has an iteration loop. In addition, it can be easily implemented in optics compared to [17].

It is worth to note that this attack can not only be implemented digitally, but can also possibly be implemented in optics with the help of some optoelectronic devices shown in Fig. 3, where SLM is a space-light modulator. The SLM and CCD plane are controlled by a computer. The generation process of the decryption keys is shown in Fig. 3(a). Firstly, the two public keys ($r_1(x)$ and $r_2(x)$), which are located in the arbitrary position (a_1 and $-a_1$), are displayed on the SLM. Secondly, the SLM are illuminated by a monochromatic light. Thirdly, the encoding image $A_0(u)$ is recorded by the CCD camera in the focal plane. In order to obtain the decryption keys, we just repeat the above operations with the encoding image $A_0(u)$ multiplied by $R_3(u)$ as input image displayed on the SLM and also illuminated by a monochromatic light. For the condition of the first step of the attack process, a reference beam should be split from the light source to record the decryption keys $P_0(u)$ and $P_1(x)$ by interferometry. The process of the optical crack is shown in Fig. 3(b). Firstly, the ciphertext $E_1(x)$ is

Table 1
The MSE values between the recovered double-images and the original double-images using the hybrid attack algorithm [17].

Method	MSE				
	Case 1	Case 2	Case 3	Case 4	Case 5
[17] with iteration 30 and original position	0.0743	0.4246	0.1269	0.2202	0.4434
[17] with iteration 300 and original position	0.0704	0.4003	0.1115	0.2127	0.4053
[17] with iteration 300 and arbitrary position	0.1171	0.5029	0.2196	0.3773	0.5366

Table 2
Comparison of computational times between the new attack method and the hybrid attack algorithm [17].

Method	The computational time				
	Case 1	Case 2	Case 3	Case 4	Case 5
The new attack method	0.429	0.432	0.438	0.425	0.417
[17] with iteration 30 and original position	3.211	3.156	3.279	3.129	3.521
[17] with iteration 300 and original position	30.595	28.258	29.294	30.254	30.461
[17] with iteration 300 and arbitrary position	29.313	29.044	30.068	29.680	29.635

multiplied by the first decryption key $P_1(x)$ and then displayed on the SLM. Secondly, the multiplied result is illuminated by a monochromatic light. Thirdly, the approximate encoding image $g_0'(u)$ is recorded by the CCD plane. For the attack result, we just repeat the above operations with $g_0'(u)$ multiplied by $P_0'(u)$ as the input image displayed on the SLM and also illuminated by a monochromatic light. Finally, two primary images can be extracted from approximate attack result in the computer. However, because of the current resource limitation in our laboratory, we just made some numerical simulations to verify the feasibility and effectiveness of the proposed method.

4. Numerical simulations and discussion

To verify the effectiveness of the proposed attack technique, simulation experiments are performed with Matlab 7.8 and Intel Pentium(R) G630 2.70 GHz, RAM 2GB. Three types of normalized images, two gray-scale images (128 128 pixels), "Lion" and "Saturn", two binary images of a Chinese character (128 128 pixels) and a fixed value image (128 128 pixels), are used for double-images encryption, as shown in Fig. 4(a)–(e). In order to meet the needs of the calculation and data displaying, the background image, composed of the two images $f_1(x)$ and $f_2(x)$, is a centered and zero-padded image (150 512 pixels). Note that the original parameters ($-a_0$ and a_0) are set as -160 and 160, respectively. At the beginning, we arbitrarily set position parameters ($-a_1$ and a_1) as -180 and 140 respectively. And then, through executing the first step of the public-key attack method by using three public keys shown in Fig. 4(f)–(h) and arbitrary position parameters, we can then obtain the decryption keys $P_0'(u)$ and $P_1'(x)$ as shown in Fig. 4 (i) and (j). Next, with the above three types of images, five cases of double-images can be considered with the above three types of images to verify the validity of the proposed attack: (1) two images are all gray-scale image; (2) one image is gray-scale image, the other is binary image; (3) one image is gray-scale image, the other is assumed to have fixed values; (4) two images are all binary image; (5) one image is binary image, the other is assumed to have fixed values.

In the proposed attack, the mean-square-error (MSE) is used to measure the similarity between the original double-images and the recovered one, calculated by the following equation:

$$\mathrm{MSE} = \frac{1}{L}\sum_{i=1}^{L}(f_i - |f_i'|)^2 \tag{27}$$

where L and f_i' denote the number of pixels and the estimate of f_i, respectively.

In the following test, five cases of double-images are shown in Fig. 5(a)–(e). The corresponding ciphertexts are shown in Fig. 5(f)–(j). In order to verify the validity of this new attack method, we will try to recover the approximate double-images from their

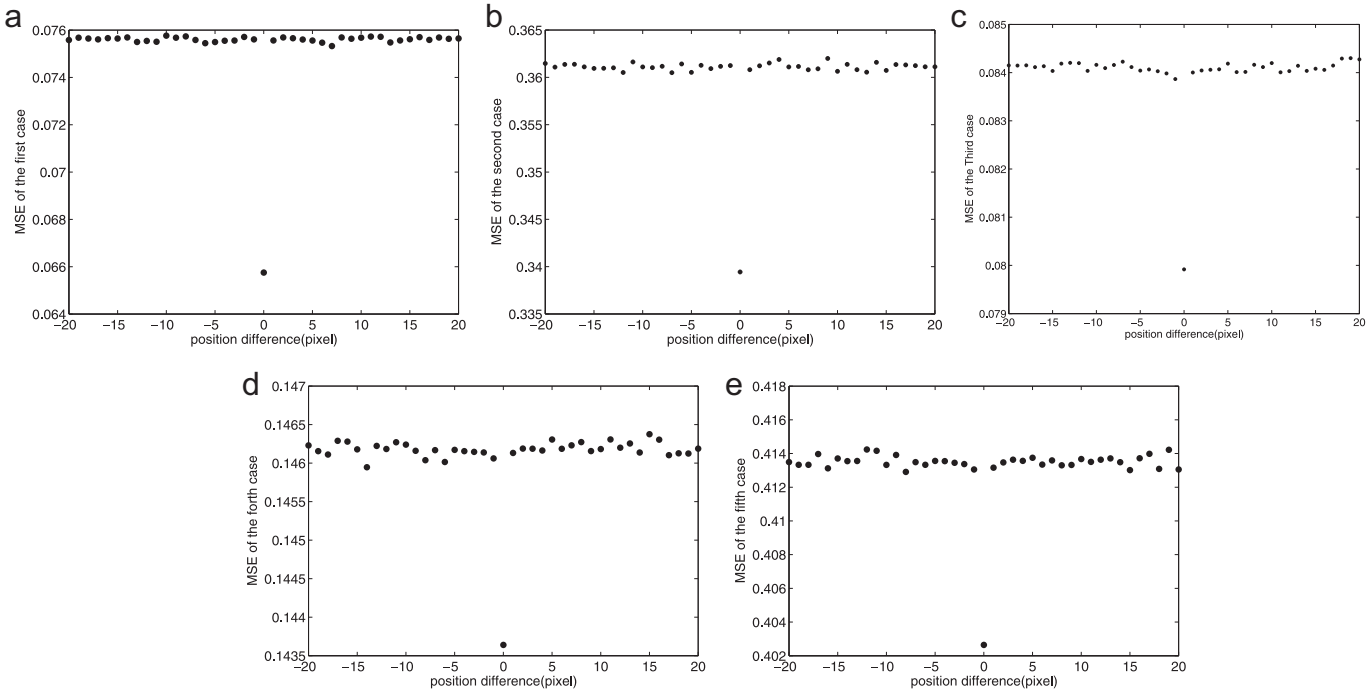

Fig. 7. The MSE values versus position difference using the new attack method.

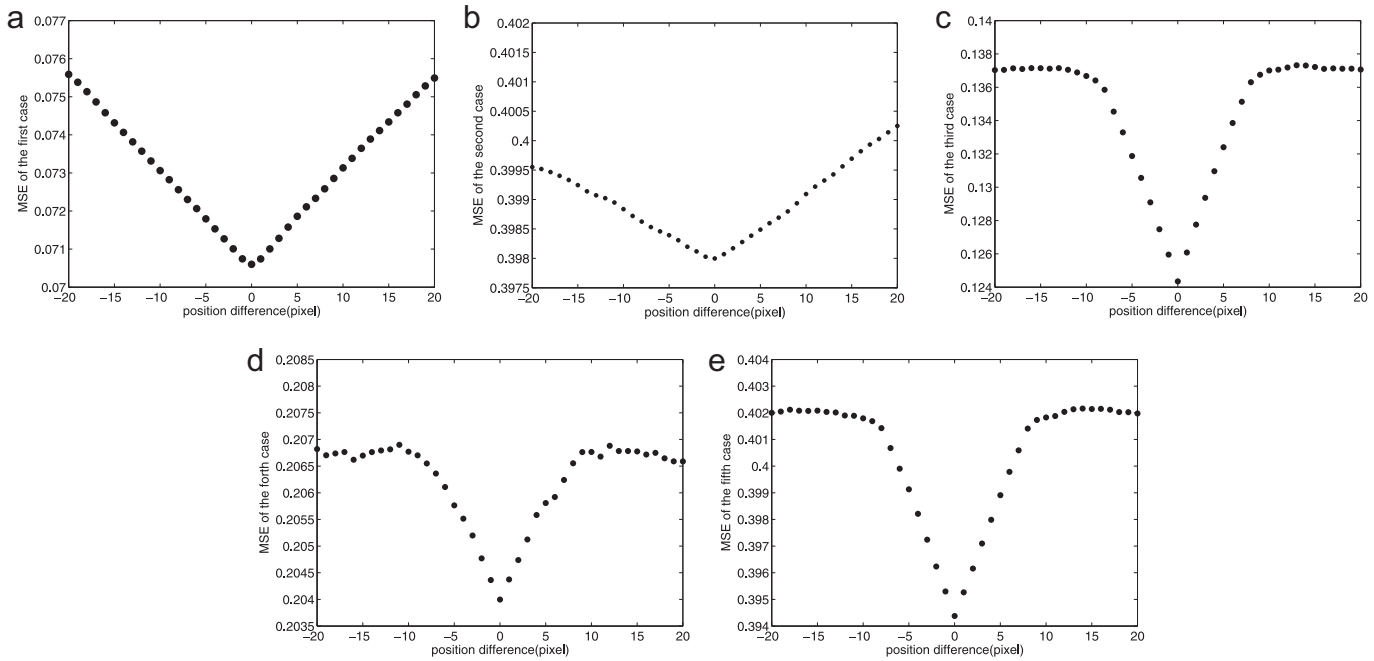

Fig. 8. The MSE values versus position difference using the hybrid attack algorithm.

corresponding ciphertexts respectively with the two generated decryption keys $P_0(u)$ and $P_1(x)$. Fig. 5(k)–(o) shows the cracked double-images corresponding to five cases of double-images, respectively. The corresponding values of MSE between Fig. 5(k)–(o) and the original double-images are 0.0751, 0.3408, 0.0841, 0.1434, and 0.4121, respectively. It can be found that although the cracked double-images are not clean, they can still provide enough information for recognition. Meanwhile, it means that the double-images nonlinear encryption based on phase truncation operation is vulnerable to the proposed attack method.

In this section, the method of the hybrid attack method [17] is also used to break the double-images cryptosystem for comparison. Let us recover five cases of double-images with original position parameters ($-a_0$ and a_0) first. The iteration numbers in the first step are set as 30 and 300, respectively. The corresponding recovered double-images are shown in Fig. 6(a)–(e) and (f)–(j), respectively. The values of MSE between the original double-images and the recovered one are represented in the first row and the second row of Table 1, respectively. Although the hybrid attack can obtain better recovered double-images by using greater iteration number in the first step, the new attack method whereby arbitrary position parameters could also result into a recognizable decoded double-images with a smaller value of MSE. Likewise, the recovered five cases of double-images with arbitrary position parameters ($-a_1$ and a_1) are also be simulated using the hybrid attack, as shown in Fig. 6(k)–(o). Note that the iteration number in the first step is still set as 300. The corresponding MSE values are displayed in the third row of Table 1. It is illustrated that with the arbitrary position parameters the hybrid attack method could not crack all five cases of double-images except for the case 1, case 2 and case 3, in which only part of information can be recognized. Meanwhile, it is obviously that the performance of the proposed method would be superior in attack time compare to that of the hybrid attack method, which has an iteration loop. The total computational time of the new attack and the hybrid attack algorithm required during simulation in five cases of double-images are shown in Table 2. All the simulation results illustrate that the performance of the new attack method is better than that of the hybrid attack method. Since the hybrid attack method has the iteration process and the original position parameters, but the new attack method does not need the iteration process and the original position parameters and also does not decrease the quality of recovery.

It is clearly seen from the above simulated result that with the arbitrary position parameters, the approximate double-images will be obtained by the new attack method . Therefore, it is necessary to study the sensitivity of the attack results with the operation position parameters. We shift the operating position of one image of the double-images in the attack process from the original position a_0, which was used in the encryption process, with Δa(1 pixels) , while the original position of another image of the double-images is fixed. The corresponding MSE values between the attack result with the different position and the original double-images, as the function of the position difference Δa, are shown in Fig. 7(a)–(e). Note that the corresponding MSE values in Fig. 7 are plotted with the dot graph because of the variation of the position of the image in one pixel. It can be seen from Fig. 7 that the MSE values of five cases of double-images stable fluctuate at 0.0748, 0.362, 0.0842, 0.1462 and 0.4135, respectively. That is, Fig. 7 indicates that although the position of the double-images changes, the corresponding MSE values maintain almost unchanged. In comparison to the new attack method, the sensitivity of the attack results with the operation position parameters for the hybrid attack algorithm should also be studied the same way. The corresponding MSE values between the attack result with the different position and the original double-images, as the function of the position difference Δa, are shown in Fig. 8(a)–(e). It indicates that the MSE values increase as $|\Delta a|$ increases. The above results fully show that the cracked result of the new attack method is more stable than by that of the hybrid attack algorithm as $|\Delta a|$ increases. That is, the hybrid attack algorithm is sensitive to the different position parameters, but the new attack method is not sensitive to the different position parameters. All of the simulation results illustrate that when the attacker does not know the original position parameters, a better cracked result can be achieved by the new attack method compared to the hybrid attack algorithm.

5. Conclusions

In summary, we have described a simple public-key attack strategy to crack the double-images nonlinear encryption technique. The main information of five cases of double-images can be obtained from its ciphertext, the arbitrary position parameters and the three public keys without any iterative operation. Compared to the hybrid attack method, the computing efficiency of the proposed attack algorithm is much better due to not using the amplitude-phase retrieval algorithm. Particularly, arbitrary position parameters could also result into a better recognizable recovered image. In addition, unlike the existing attack methods, our proposed attack method can be easily implemented in optics. The simulation results show that with arbitrary position parameters the public-key attack is valid and the double-images nonlinear cryptosystem is vulnerable to this attack.

Acknowledgments

The authors would like to extend sincere appreciation to the referees for their valuable comments and suggestions to improve this paper. The authors also appreciate the nice help from Mrs. Moses Odero John because he helps us a lot in improving the English usage. This work was supported by Key Laboratory of Intelligent Control Technology for Ecological Agriculture in Wuling Mountain Areas of Hunan Province, the project of the Educational Commission of Hunan Province of China under Grant 13C715.

References

[1] P. Refregier, B. Javidi, Opt. Lett. 20 (1995) 767.
[2] G. Situ, J. Zhang, Opt. Lett. 29 (2004) 1584.
[3] Y. Wang, C. Quan, C.J. Tay, Opt. Commun. 330 (2014) 91.
[4] B. Hennelly, J.T. Sheridan, Opt. Lett. 28 (2003) 269.
[5] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. 25 (2000) 887.
[6] L. Chen, D. Zhao, Opt. Express 14 (2006) 8552.
[7] X. Peng, P. Zhang, H. Wei, B. Yu, Opt. Lett. 31 (2006) 1044.
[8] X. Peng, H. Wei, P. Zhang, Opt. Lett. 31 (2006) 3261.
[9] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.
[10] W. Qin, X. Peng, Opt. Lett. 35 (2010) 118.
[11] X. Wang, D. Zhao, Opt. Commun. 285 (2012) 1078.
[12] X. Wang, D. Zhao, Opt. Express 20 (2012) 11994.
[13] M.R. Abuturab, Opt. Lasers Eng. 58 (2014) 39.
[14] L.S. Sui, K.K. Duan, J.L. Liang, Opt. Lasers Eng. 62 (2014) 139.
[15] W. Liu, Z. Liu, S. Liu, Opt. Lett. 38 (2013) 1651.
[16] X. Ding, X. Deng, K. Song, G. Chen, Appl. Opt. 52 (2013) 467.
[17] X. Deng, Opt. Commun. 317 (2014) 7.
[18] Y. Shapiro, M. Porat, Proc. IEEE 2 (1997) 773.
[19] W. Qin, X. Peng, X. Meng, B. Gao, Opt. Eng. 50 (2011) 080501.