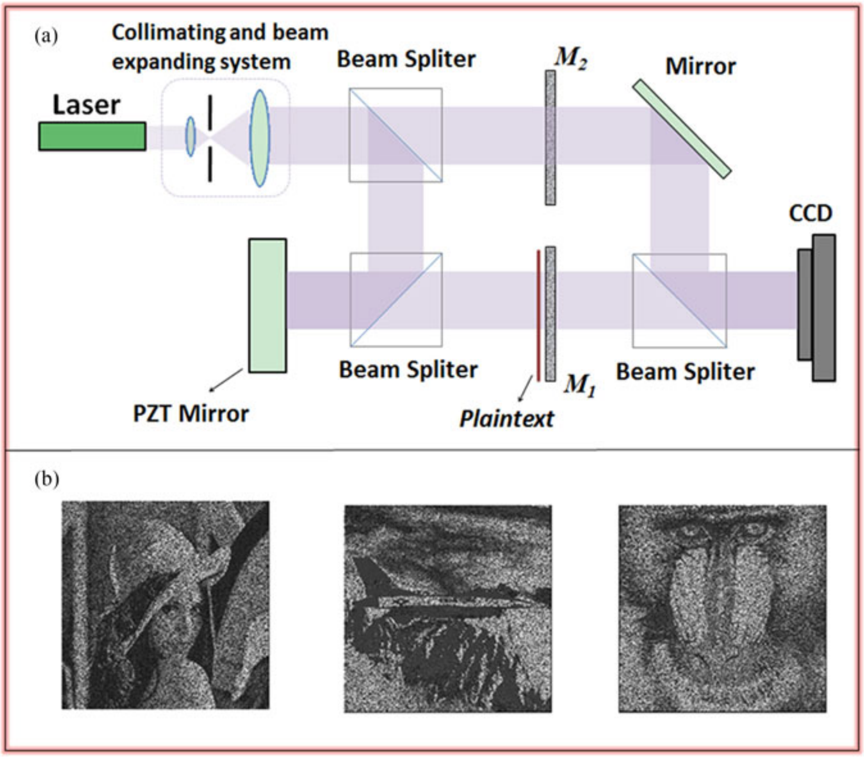
IEEE Photonics Journal
An IEEE Photonics Society Publication

Ciphertext-Only Attack on Phase-Shifting Interferometery-Based Encryption

Volume 9, Number 5, October 2017

Tuo Li
Zongcheng Miao
Yishi Shi



DOI: 10.1109/JPHOT.2017.2743060
1943-0655 © 2017 IEEE

Ciphertext-Only Attack on Phase-Shifting Interferometery-Based Encryption

Tuo Li,[1] Zongcheng Miao,[1] and Yishi Shi[2, 3]

[1]School of Science, Xijing University, Xi’an 710123, China
[2]College of Opto-Electronics, University of Chinese Academy of Sciences,
Beijing 100049, China
[3]Academy of Opto-Electronics, Chinese Academy of Sciences, Beijing 100094, China

DOI:10.1109/JPHOT.2017.2743060

Manuscript received June 13, 2017; revised August 14, 2017; accepted August 18, 2017. Date of publication August 29, 2017; date of current version September 11, 2017. This work was supported by the National Natural Science Foundation of China under Grant 61575197, K. C. Wong Education Foundation; Fusion Foundation of Research and Education, Chinese Academy of Sciences; Youth Innovation Promotion Association CAS. Corresponding author: Yishi Shi (e-mail: optsys@gmail.com).

Abstract: The phase-shifting interferometry-based (PSI-based) encryption is one of most typical optical encryption systems. In this paper, we demonstrate a new approach to ciphertext-only attack (COA) on PSI-based encryption, revealing that there is serious security risk in PSI-based encryption. With the proposed COA approach, an opponent can crack the ciphertexts directly without use of the keys of the system. This demonstration, as far as our best knowledge, shows the PSI technique is vulnerable to COA for the first time. A series of attack results are shown to demonstrate the feasibility and robustness of the attack method. Our study reveals a critical security issue that should be taken in to account when designing an optical information security system.

Index Terms: Ciphertext-only attack, phase-shifting interferometery-based encryption.

1. Introduction

Optical encryption has raised many researcher’s interests owing to its inherent capability for parallel processing [1]. Since the double random phase encoding (DRPE) was proposed [2], a number of researchers focus on it and give massive extensions, such as the DRPE scheme in different domains [3]–[5], the joint transformation correlator (JTC) encryption [6]–[8] and multiple-image encryption [9]–[11], and the PSI-based encryption [12]–[20], etc [21]–[22]. During these extensions, the PSI-based cryptosytem is one of most typical encryption methods which has been demonstrated experimentally due to its convenience to perform accurate alignment. However, as any other encryption systems, the PSI-based encryption could be claimed to be security and widely used in the practical use only if it is able to endure the attacks of various cryptanalysis methods. Dependent on the type of information available, typical cryptoanalysis methods can be categorized as the chosen-ciphertext attack (CCA) [23], the chosen-plaintext attack (CPA) [24]–[26], the known-plaintext attack (KPA) [27]–[30], the ciphertext-only attack (COA) [31]–[33]. Among these, the COA is the most challenging one as it requires the least knowledge about the encryption machine. Therefore, an encryption method is generally said to be not secure at all if it is vulnerable to COA, as any plaintext encrypted by it will be disclosed by properly analyzing the corresponding ciphertext alone [33].

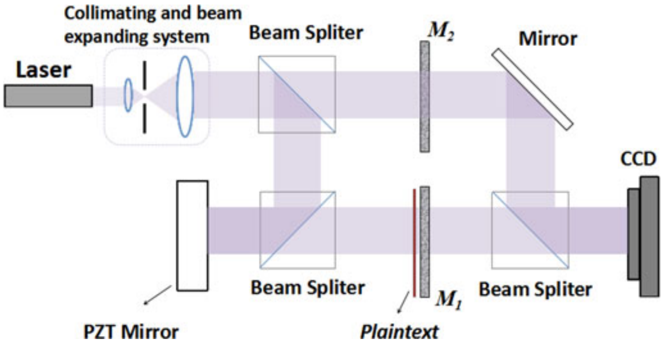


Fig. 1. Scheme of PSI-based cryptosystem. M_1 and M_2 are the random phase key.

In this paper, we demonstrate that the PSI-based encryption is vulnerable to the COA. We note that the previous work has reported a CPA and KPA method [34]–[35]. But compared with CPA and KPA, it relies on a strong assumption that the some additional resources or prior knowledge should be known, for example, some plaintext-ciphertexts pairs. These conditions are often hard to satisfy in practical situations [32]. Alternatively, the approach we employed in the present COA works without the need to have a prior knowledge about the support of plaintext image. To the best of our knowledge, it is the first demonstration of COA to the PSI-based method. Our study reveals a critical security risk that should be taken into account when designing an optical information security problems.

2. Theoretical Analysis

2.1 Principle of Proposed PSI Cryptosystem

Here, we concisely review the PSI-based encryption system. Among the existing PSI-based cryptosystem, some applies four-step PSI [12], and three-step [13] or two-step [14]–[15], etc. In fact, the basic principle of these schemes is similar. Therefore, the four-step PSI method is taken as an example and briefly describe the PSI-based cryptosystem. Fig. 1 shows the scheme of PSI-based cryptosystem. The system is based on Mach-Zehnder interferometer architecture. A random phase mask M_1 is attached to the plaintext in the object beam, and another random phase mask M_2 is placed at a variable position in the reference arm. The phase shifting setup (for example PZT mirror) located in the reference beam is to provide 0, $-\pi/2$, $-\pi/$ and $-3\pi/2$ phase-shifting. In this way, four corresponding interferograms with different phase-shifting values are captured in turn by the detector. Note that Fig. 1 is just a principle scheme of the PSI-based cryptosystem. In the practical PSI-based cryptosystem, the physical map of PSI-based cryptosystem can be made more compatible and the spatial light modulator can be applied to upload the plaintext efficiency [15].

Assume that $P(x, y)$ is the plaintext to be encrypted and M_1 is the random phase key attached to the plaintext. Then, the complex amplitude distribution of the object beam on the CCD plane is:

$$U_O(x, y) = FrT_{\lambda, z_1}\left\{P(x, y)\cdot \exp\left(i\phi_1(x, y)\right)\right\} \tag{1}$$

where $FrT_{\lambda, z_1}\{\bullet\}$ denotes the Fresnel diffraction with the illumination wavelength of λ and the distance z_1. $\phi_1(x, y)$ represents the phase distribution of random key M_1. Since the M_2 is placed at z from the CCD plane, the complex amplitude distribution of the reference beam on the detector plane is:

$$U_R(x, y, \alpha) = \exp(i\alpha)\cdot FrT_{\lambda, z_2}\left\{\exp\left[i\phi_2(x', y')\right]\right\} \tag{2}$$

where $FrT_{\lambda, Z_2}\{\bullet\}$ denotes the Fresnel diffraction with the illumination wavelength of λ and the distance of z_2. α is the relative phase shift value by the PZT mirror. $\phi_2(x', y')$ is the random phase distribution of the phase-only mask M_2. Let $U_O = A_O \exp[j\phi_o(x, y)]$, $U_R = A_R \exp[j\phi_R(x, y) + \alpha]$. Note that α is the relative phase shift values by the PZT mirror. Then the encrypted interferograms recoded by the CCD camera is given by (3):

$$\begin{aligned} I(x, y; \alpha) &= |U_O(x, y) + U_R(x, y; \alpha)|^2 \\ &= [A_O(x, y)]^2 + [A_R(x, y)]^2 + 2A_O(x, y) A_R(x, y) cos[\phi_o(x, y) - \phi_R(x, y) - \alpha] \end{aligned} \tag{3}$$

Till now, the encryption is finished. Since the method of processing the encrypted interferograms $I(x, y, \alpha)$ by PSI method is non-uniqueness, the plaintext $P(x, y)$ can be obtained by (4) [13]:

$$P(x, y) = \left|FT^{-1}\left\{B_E(x, y)/A_R(x, y) \cdot \exp(\phi_E - \phi_R)\right\}\right| \tag{4}$$

where $\phi_\mathrm{E}(x, y)$ and $B_\mathrm{E}(x, y)$ in (4) can be obtained by using (5) and (6), respectively:

$$\phi_E(x, y) = \arctan\left[\frac{I(x, y; -3\pi/2) - I(x, y; -\pi/2)}{I(x, y; 0) - I(x, y; -\pi)}\right] \tag{5}$$

$$B_E(x, y) = \frac{1}{4}\frac{I(x, y; 0) - I(x, y; -\pi)}{\cos[\phi_o(x, y) - \phi_R(x, y)]} \tag{6}$$

From (5) and (6), we can see that ϕ_E and B_E can be obtained by the interferegrams, which are known resources. The plaintext can be acquired immediately if A_R and $\phi_\mathrm{R}(x, y)$ are known according to (4). However, if the A_R and $\phi_\mathrm{R}(x, y)$ are not known, the plaintext cannot be obtained directly. In the next section, we will show that how to breach the system by the proposed COA method in the case that A_R and $\phi_\mathrm{R}(x, y)$ are unknown.

2.2 Principle of Proposed COA

We proposed a new approach to COA on PSI-based cryptosystem. For the COA method, it is assumed that the phase keys M_1 and M_2 is unknown. The target of attackers is how to retrieve the plaintexts from the ciphertexts directly without use of the keys. Here, we show the principle of the proposed COA method. Assume that attackers intercept three ciphertexts $\{C_1, C_2, C_3\}$ (which are easy to be acquired with the four corresponding encrypted interferograms by PSI-technique). According to the principle of PSI-based cryptosystem:

$$\begin{aligned} A_{O1}\exp(j\phi_{O1}) + A_R\exp(j\phi_R) &= C_1 \\ A_{O2}\exp(j\phi_{O2}) + A_R\exp(j\phi_R) &= C_2 \\ A_{O3}\exp(j\phi_{O3}) + A_R\exp(j\phi_R) &= C_3 \end{aligned} \tag{7}$$

Construct the equation group by applying the (7):

$$\begin{aligned} a_{11}A_{O1}\exp(j\phi_{O1}) + a_{12}A_{O2}\exp(j\phi_{O2}) + a_{13}A_{O3}\exp(j\phi_{O3} &= a_1 + jb_1 \\ a_{21}A_{O1}\exp(j\phi_{O1}) + a_{22}A_{O2}\exp(j\phi_{O2}) + a_{23}A_{O3}\exp(j\phi_{O3}) &= a_2 + jb_2 \\ a_{31}A_{O1}\exp(j\phi_{O1}) + a_{32}A_{O2}\exp(j\phi_{O2}) + a_{33}A_{O3}\exp(j\phi_{O3}) &= a_3 + jb_3 \end{aligned} \tag{8}$$

where the ciphertext C_1, C_2 and C_3 are equal to $C_1 = a_1 + jb_1$, $C_2 = a_2 + jb_2$ and $C_3 = a_3 + jb_3$, respectively. When constructing the equation group shown in (8), the value of the coefficients $(a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33})$ can be arbitrary chosen only if it meets the condition: $a_{11} + a_{12} + a_{13} = 0$, $a_{21} + a_{22} + a_{23} = 0$, $a_{31} + a_{32} + a_{33} = 0$.

Equation (8) can be decomposed to (9) and (10). Equation (9) is shown as follows:

$$\begin{aligned} a_{11}A_{O1}\cos(\phi_{O1}) + a_{12}A_{O2}\cos(\phi_{O2}) + a_{13}A_{O3}\cos(\phi_{O3}) &= a_1 \\ a_{21}A_{O1}\cos(\phi_{O1}) + a_{22}A_{O2}\cos(\phi_{O2}) + a_{23}A_{O3}\cos(\phi_{O3}) &= a_2 \\ a_{31}A_{O1}\cos(\phi_{O1}) + a_{32}A_{O2}\cos(\phi_{O2}) + a_{33}A_{O3}\cos(\phi_{O3}) &= a_3 \end{aligned} \tag{9}$$

Equation (10) is shown as follows:

$$\begin{aligned} a_{11}A_{O1}\sin(\phi_{O1}) + a_{12}A_{O2}\sin(\phi_{O2}) + a_{13}A_{O3}\sin(\phi_{O3}) = b_2 \\ a_{21}A_{O1}\sin(\phi_{O1}) + a_{22}A_{O2}\sin(\phi_{O2}) + a_{23}A_{O3}\sin(\phi_{O3}) = b_2 \\ a_{31}A_{O1}\sin(\phi_{O1}) + a_{32}A_{O3}\sin(\phi_{O3}) + a_{33}A_{O3}\sin(\phi_{O3}) = b_2 \end{aligned} \tag{10}$$

Let $A_{O1}\cos(\phi_1) = x_1$, $A_{O2}\cos(\phi_2) = x_2$, $A_{O3}\cos(\phi_3) = x_3$, (9) can be written as:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = a_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = a_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = a_3 \end{aligned} \tag{11}$$

The (11) can be changed into:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{12}$$

Equation (12) can be written as:

$$Ax = a \tag{13}$$

where $A = [a_{11}, a_{12}, a_{13}; a_{21}, a_{22}, a_{33}; a_{31}, a_{32}, a_{33}]$, $x = [x_1, x_2, x_3]$, and $a = [a_1, a_2, a_3]$.

To prevent the determinant of matrix $det(A) = 0$, we introduce a perturbation matrix δ which meets the condition that $det(\delta) \neq 0$.

$$(A + \delta)\, x' = a \tag{14}$$

By solving the linear equations, we can obtain $x' = [x_1', x_2', x_3']$. Because the matrix δ is a perturbation matrix, there is the equation:

$$x \approx x' \tag{15}$$

To ensure the (15), the elements of perturbation matrix δ should be small enough and satisfies the condition $|\delta_{ij}| < 0.005|a_{ij}|$ $(i, j = 1, 2, 3)$. δ_{ij} and a_{ij} represent the elements of matrix A and δ, respectively.

Let $\sin(j\phi_1) = y_1$, $\sin(j\phi_2) = y_2$, $\sin(j\phi_3) = y_3$, (10) can be written as:

$$Ay = b \tag{16}$$

where $y = [y_1, y_2, y_3]$, and $b = [b_1, b_2, b_3]$.

In the similar way, to prevent the determinant of matrix $\det(A) = 0$, we introduce a perturbation matrix δ which meets the condition that $\det(\delta) \neq 0$.

$$(A + \delta)\, y' = b \tag{17}$$

By solving the equation, we can obtain $y' = [y_1', y_2', y_3']$. Because matrix δ is a perturbation matrix of matrix A, there is the equation:

$$y \approx y' \tag{18}$$

According to (1)–(18), there are:

$$\begin{aligned} P_1(x, y) \approx P_1{}'(x, y) = \left| IFrT_{\lambda, z_1}\left\{x_1' + jy_1'\right\}\right| \\ P_2(x, y) \approx P_2'(x, y) = \left| IFrT_{\lambda, z_1}\left\{x_2' + jy_2'\right\}\right| \\ P_3(x, y) \approx P_3'(x, y) = \left| IFrT_{\lambda, z_1}\left\{x_3' + jy_3'\right\}\right| \end{aligned} \tag{19}$$

where $IFrT\{\bullet\}$ represents the inverse Fresnel transform, $P_1(x, y)$, $P_2(x, y)$, and $P_3(x, y)$ are the original plaintexts, $P_1'(x, y)$, $P_2'(x, y)$, and $P_3'(x, y)$ stand for the cracked plaintexts obtained by the proposed COA. Till now, the proposed COA is finished.

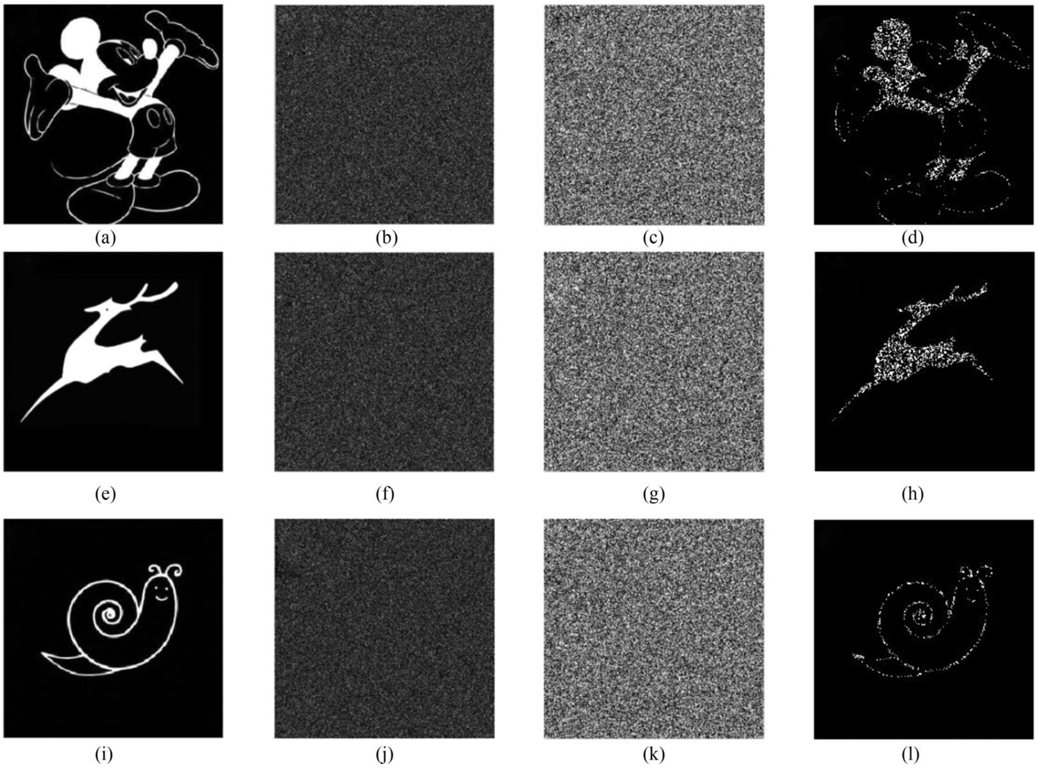


Fig. 2. Attack results in the case that the image are binary image. (a), (e), (i) are three original binary plaintexts (P_1, P_2, and P_3), respectively. C_1, C_2, and C_3 are the corresponding ciphertexts of P_1, P_2, and P_3, respectively. (b), (f) and (j) are the amplitude distribution of C_1, C_2, and C_3, respectively. (c), (g) and (k) are the phase distribution of C_1, C_2, and C_3, respectively. (d), (h) and (l) are the attack results by utilizing the proposed COA.

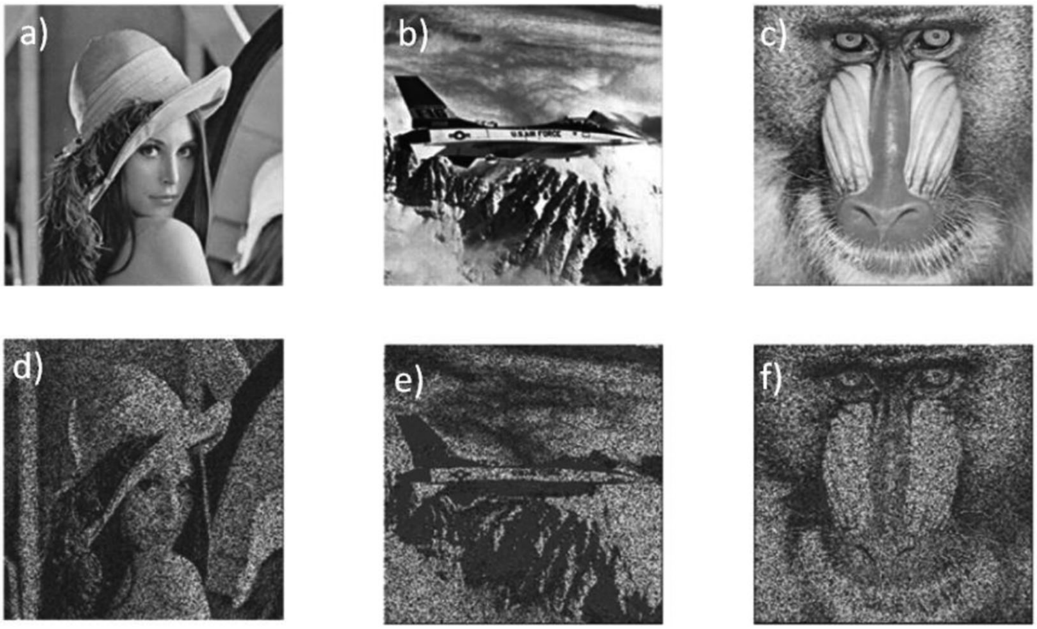


Fig. 3. Attack results in the case that the plaintext are gray-scale image (256 × 256 × 8 bits). (a), (b), and (c) are three original plaintexts P_1, P_2, and P_3, respectively. (d), (e) and (f) are corresponding attack results by applying the proposed COA method.

We can see that, in the above COA, there are two constraints to ensure the successful attack: 1. The coefficients of the matrix A ($a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}$) should meet the condition: $a_{11} + a_{12} + a_{13} = 0$, $a_{21} + a_{22} + a_{23} = 0$, $a_{31} + a_{32} + a_{33} = 0$; 2. The determinant of perturbation matrix δ is not zero and the elements of matrix should satisfy the condition $|\delta_{\mathrm{ij}}| < 0.005|a_{\mathrm{ij}}|$ ($i, j = 1, 2, 3$).

To evaluate the performance of the proposed COA method, the MSE between two images is defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1,j=1}^{M,N} \left[P'(x, y) - P(x, y)\right]^2 \tag{20}$$

where $P(x, y)$ represents the original image and $P'(x, y)$ stands for the attack results.

3. Attack Results and Analysis

We have performed a series of simulations to test the feasibility of the proposed COA. In the encryption procedure, the two random phase keys M_1 and M_2 are $\exp[j\phi_1(x, y)]$ and $\exp[j\phi_2(x, y)]$, respectively. The diffraction distance z_1 (from M_1 to the detector) and z_2 (from M_2 to the detector) are 30mm and 50mm, respectively. In the attack process, the matrix A to construct the linear equations is [1.632 −0.512 −1.120; 2.372 1.347 −3.719; −5.257, 1.785, −3.472]. The matrix δ is [0.0407, 0.0457, 0.0139; 0.0453, 0.0316, 0.0273; 0.063, 0.0049, 0.0479]. Note that the matrix A and δ can be arbitrary chosen by the opponent only if it meets the two constraints shown in the Section 2 (Principle of proposed COA).

3.1 Feasibility of the Proposed COA

First, we test the feasibility of the proposed COA in the simplest case that all the plaintexts are binary image. We prepare three binary plaintexts to verify the feasibility of proposed COA method and each plaintext [Fig. 2(a), (e) and (i)] has a size of 256 × 256 pixels. We utilize the proposed COA to crack the three ciphertexts [Fig. 2(b)–(c), (f)– and (j)–(k)]. Fig. 2(d), (h), and (l) illustrate the attack results by using the proposed COA. Comparing with the original images [Fig. 2(a), (e), and (i)] and attack results [Fig. 2(d), (h), (l)], there are some noise on the attack results. However, the main information in the attack results can be obtained. These results demonstrate the feasibility of the proposed COA.

Second, we testify the feasibility of the proposed COA in the case that all the plaintexts are gray-scale image. We prepare three gray-scale plaintexts to verify the validity of proposed COA method and each plaintext [Fig. 3(a)–(c)] has a size of 256×256 pixels. We utilize the proposed COA to crack the ciphertexts. Fig. 2(d)–(f) show the attack results. Comparing with the original image [Fig. 3(a)–(c)] and attack results [Fig. 3(d)–(f)], there are some noise on the attack result. However, the main information (Lena, Plane, and Monkey) in the attack results can be obtained. These above results further demonstrate the feasibility of the proposed COA. Further, we test a series of the maxtri A and perturbation matrix δ which meets the two required conditions. The corresponding attack results indicate that the COA is stable and can be work once the two constraints are satisfied. For example, we test another matrix A and δ to perform attack: The matrix A to construct the linear equations is [−1.135, 0.612, 0.523; 1.653, −1.799, 0.146; 0.268, 1.864, −2.132]. The matrix δ is [0.0756, 0.0694, 0.0207; 0.0333, 0.0133, 0.0549; 0.0737, 0.0402, 0.0990]. The attack result is similar to Fig. 3, which is not shown here for simplicity. These results demonstrate that the proposed COA has a huge space for the different matrix choice.

3.2 Robustness of the Proposed COA

In this section, the robustness of the proposed COA has been tested. As the ciphertexts (C_1, $C_{2,}$ and C_3) may be contaminated by the noise in practical case, the performances of proposed method are

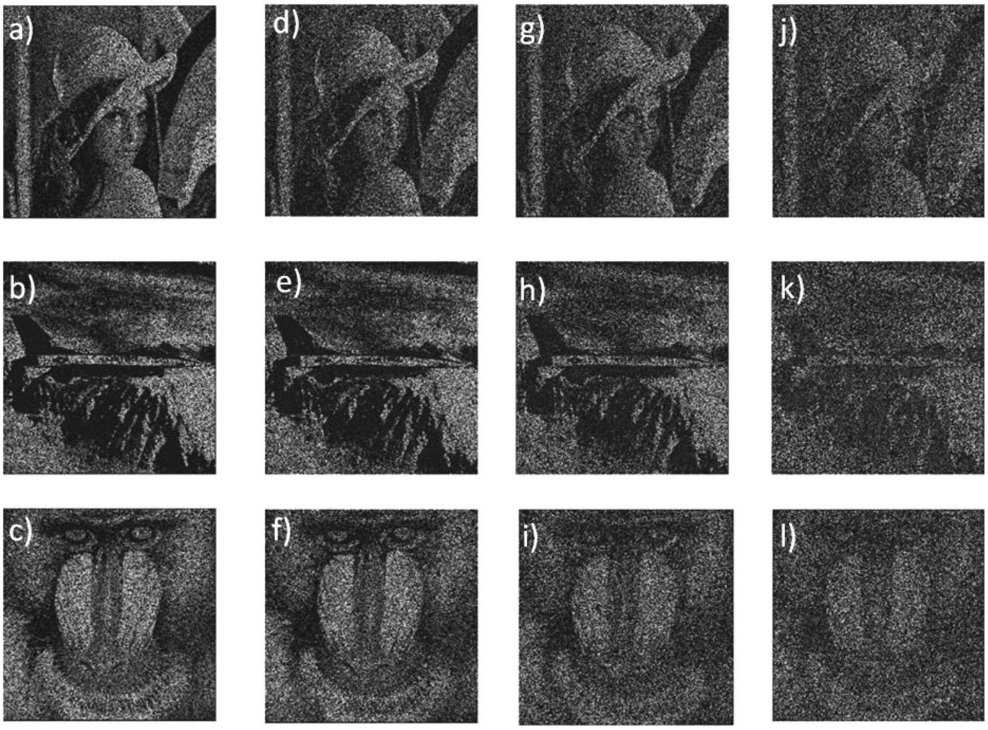


Fig. 4. Robustness of the COA method in the case that the ciphertexts C_1, C_2, and C_3 are all contaminated by noise. (a)–(c), (d)–(f), (g)–(i), and (j)–(l) are attack results by applying the proposed COA method when the ciphertexts were contaminated with random noise of different degree ($SNR = 20$, 10, 5, 2), respectively.

tested in the noise contaminated condition. Firstly, we test the case that the ciphertext C_1, $C_{2,}$ and C_3 are all contaminated by random noise. The random noise is generated by (Mean[$|C_i|$]}$/$SNR)*V, where Mean denotes a mean value of the ciphertext, V is 2D variable randomly distributed in a range of $[-0.5, 0.5]$ and SNR represents the signal-to-noise ratio [36]. Fig. 4(a)–(c), (d)–(f), (g)–(i), and (j)–(l) are the attack results when C_1, C_2 and C_3 are contaminated with different degree noise (SNR value 20, 10, 5, and even 2), respectively. These results demonstrate the robustness of the proposed COA.

4. Conclusion

We proposed a COA method to evaluate the security strength of optical encryption based on the PSI-based scheme. The proposed COA strategy converts the problem of COA into a question of solving linear equations. To the best of our knowledge, this should be the first work to breach the PSI-based optical cryptosystem with a COA method. A set of attack results have demonstrated the feasibility and validity of the proposed method and shown that there is a serious security problem in the PSI-based scheme.

References

[1] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 16, pp. 120–155, 2014.
[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767–769, 1995.
[3] Z. Liu and S. Liu, "Random fractional Fourier transform," *Opt. Lett.*, vol. 32, pp. 2088–2090, 2007.
[4] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, pp. 887–889, 2000.

[5] G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett.*, vol. 29, pp. 1584–1586, 2004.
[6] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” *Opt. Eng.*, vol. 39, pp. 2031–2035, 2000.
[7] E. Rueda, J. Barrera, R. Henao, and R. Torroba, “Optical encryption with a reference wave in a joint transform correlator architecture,” *Opt. Commun.*, vol. 282, pp. 3243–3249, 2009.
[8] R. Henao, E. Rueda, J. Barrera, and R. Torroba, “Noise-free recovery of optodigital encrypted and multiplexed images,” *Opt. Lett.*, vol. 35, pp. 333–335, 2010.
[9] Y. Shi, G. Situ, and J. Zhang, “Multiple-image hiding by information prechoosing,” *Opt. Lett.*, vol. 33, pp. 542–544, 2008.
[10] W. Chen, “Optical multiple-image encryption using three-dimensional space,” *IEEE Photon. J.*, vol. 8, no. 2, Apr. 2016, Art. no. 6900608.
[11] X. Li *et al.*, “Multiple-image encryption based on compressive ghost imaging and coordinate sampling,” *IEEE Photon. J.*, vol. 8, no. 4, Aug. 2016, Art. no. 3900511.
[12] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, “Optoelectronic information encryption with phase-shifting interferometry,” *Appl. Opt.*, vol. 39, pp. 2313–2320, 2000.
[13] X. Wang and D. Zhao, “Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry,” *Opt. Commun.*, vol. 268, pp. 240–244, 2006.
[14] M. He, L. Cai, Q. Liu, and X. Yang, “Phase-only encryption and watermarking based on phase-shifting interferometry,” *Appl. Opt.*, vol. 44, pp. 2600–2606, 2005.
[15] X. Meng, L. Cai, and Y. Wang, “Two-step phase-shifting interferometry and its application in image encryption,” *Opt. Lett.*, vol. 31, pp. 1414–1416, 2006.
[16] P. Liu and C. Poon, “Two-step-only quadrature phase-shifting digital holography,” *Opt. Lett.*, vol. 34, pp. 250–252, 2009.
[17] Y. Zhang and B. Wang, “Optical image encryption based on interference,” *Opt. Lett.*, vol. 33, pp. 2443–2445, 2008.
[18] C. Niu, X. Wang, N. Lv, Z. Zhou, and X. Li, “An encryption method with multiple encrypted keys based on interference principle,” *Opt. Exp.*, vol. 18, pp. 7827–7834, 2010.
[19] X. Wang and D. Zhao, “Fully phase multiple-image encryption based on superposition principle and the digital holographic technique,” *Opt. Commun.*, vol. 285, pp. 4280–4284, 2012.
[20] B. Wang and Y. Zhang, “Double images hiding based on optical interference,” *Opt. Commun.*, vol. 282, pp. 3439–3443, 2009.
[21] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, “Optical image encryption via ptychography,” *Opt. Lett.*, vol. 38, pp. 1425–1427, 2013.
[22] D. Kong, L. Cao, G. Jin, and B. Javidi, “Three-dimensional scene encryption and display based on computer-generated holograms,” *Appl. Opt.*, vol. 55, pp. 8296–8300, 2016.
[23] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys,” *Opt. Lett.*, vol. 30, pp. 1644–1646, 2005.
[24] J. F. Barrera, C. Vargas, M. Tebaldi, and R. Torroba, “Chosen-plaintext attack on a joint transform correlator encrypting system,” *Opt. Commun.*, vol. 283, pp. 3917–3921, 2010.
[25] X. Peng, P. Zhang, H. Wei, and B. Yu, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” *Opt. Lett.*, vol. 31, pp. 3261–3263, 2006.
[26] T. Li and Y. Shi, “Security risk of diffractive-imaging-based optical cryptosystem,” *Opt. Exp.*, vol. 23, pp. 21384–21391, 2015.
[27] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” *Opt. Exp.*, vol. 15, pp. 10253–10265, 2007.
[28] X. Peng, H. Wei, and P. Zhang, “Known-plaintext attack on optical encryption based on double random phase keys,” *Opt. Lett.*, vol. 31, pp. 1044–1046, 2006.
[29] D. Kong, X. Shen, L. Cao, and G. Jin, “Phase retrieval for attacking fractional Fourier transform encryption,” *Appl. Opt.*, vol. 56, pp. 3449–3456, 2017.
[30] X. Wang and D. Zhao, “A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Commun.*, vol. 285, pp. 1078–1081, 2012.
[31] C. Zhang, M. Liao, W. He, and X. Peng, “Ciphertext-only attack on a joint transform correlator encryption system,” *Opt. Exp.*, vol. 21, pp. 28523–28530, 2013.
[32] M. Liao, W. He, D. Lu, and X. Peng, “Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: From the view of imaging through scattering medium,” *Scientific Rep.*, vol. 7, 2017, Art. no. 41789.
[33] G. Li, W. Yang, D. Li, and G. Situ, “Ciphertext-Only attack on the double random-phase encryption: Experimental demonstration,” *Opt. Exp.*, vol. 25, pp. 8690–8697, 2017.
[34] W. Qin, X. Peng, X. Meng, and B. Gao, “Vulnerability to chosen-plaintext attack of optoelectronic information encryption with phase-shifting interferometry,” *Opt. Eng.*, vol. 50, pp. 0656011–0656015, 2011.
[35] T. Li, Y. Wang, J. Zhang, and Y. Shi, “Analytic known-plaintext attack on a phase-shifting interferometry-based cryptosystem,” *Appl. Opt.*, vol. 54, pp. 306–311, 2015.
[36] W. Chen and X. Chen, “Structured-illumination-based diffractive imaging and its application to optical image encryption,” *Opt. Commun.*, vol. 285, pp. 2044–2047, 2012.