Published in final edited form as:

Opt Eng. 2011 June 13; 50(6): . doi:10.1117/1.3590725.

Vulnerability to chosen-plaintext attack of optoelectronic information encryption with phase-shifting interferometry

Wan Qin,

Shenzhen University, College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems, Ministry of Education, Guangdong Province, Shenzhen 518060, China and Clemson University, Department of Bioengineering, Clemson, South Carolina 29634

Xiang Peng,

Shenzhen University, College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems, Ministry of Education, Guangdong Province, Shenzhen 518060, China and Clemson University, Department of Bioengineering, Clemson, South Carolina 29634

Xiangfeng Meng, and

Shandong University, School of Information Science and Engineering, Jinan 250100, China

Bruce Z. Gao

Clemson University, Department of Bioengineering, Clemson, South Carolina 29634

Xiang Peng: xpeng@szu.edu.cn

Abstract

The optical cryptosystem based on phase-shifting interferometry (PSI) is one of the most interesting optical cryptographic schemes in recent years. However, we find that the PSI technique provides an attractive method to record the ciphertext, but contributes little to the security level of the cryptosystem. From the cryptanalysis point of view, in a certain simplified case, an attacker is only required to crack two equivalent decryption keys instead of the original random phase keys and geometric key. Moreover, a chosen-plaintext attack method is proposed, in which an impulse function is chosen as a known plaintext. By using this attack, the attacker can effectively recover any plaintext from the corresponding ciphertext. The validity of the attack is verified by computer simulations.

Subject terms

optical information security; chosen-plaintext attack; phase-shifting interferometry; optical cryptanalysis

1 Introduction

Optical information processing technology has emerged as a very promising means of encryption.¹ With the pioneering work on double random phase encoding (DRPE), Refrégier and Javidi paved the way for many subsequent proposals for optical security and encryption systems.² During the past 15 years, a number of optical techniques have been introduced in the optical cryptology to make it a significant progress.^{3–11} However, from the cryptanalysis point of view, any cryptosystem could be claimed secure only if it is able to endure various attacks. Recently, the classical DRPE-based optical encryption schemes have undergone a series of rigorous cryptanalysis.^{12–18} Frauel and Javidi et al.¹³ demonstrated that an exhaustive search of the phase key is generally intractable in DRPE scheme. At the same time, they also presented some attacks that are able to efficiently recover the keys of the scheme. Moreover, even though extended from the Fourier domain to the fractional Fourier

domain and the Fresnel domain with extra secret keys, the DRPE-based optical encryption schemes are still demonstrated vulnerable to the known-plaintext attack¹⁷ and the chosen-plaintext attack.¹⁵

The optical encryption technique based on the concept of phase-shifting interferometry (PSI) is another category of an interesting optical cryptographic scheme. Much effort has been made on the construction of high-security-level and feasible cryptosystems based on the PSI technique,^{19–22} owing to the following advantages: 1. The complex-value ciphertext is recorded with a group of intensity-only interferograms, which facilitate the storage and transmission; 2. Digital phase-shifting interferometry can make a more efficient use of the limited CCD resolution than off-axis digital holography. However, to the best of our knowledge, the security level of this technique has not been rigorously evaluated from the cryptanalysis point of view yet. In this paper, we present a chosen-plaintext attack on this type of optical encryption scheme. It will be seen that an attacker can successfully retrieve the decryption keys with the pre-knowledge of a special pair of plaintext-ciphertext.

2 Security Analysis of the Encryption and Decryption Procedures

Among the existing PSI-based encryption systems, some employ four-step PSI,¹⁹ and some three-step²⁰ or two-step,²¹ etc. In fact, the basic principles of these schemes are similar. Generally, the system errors decrease with an increase in the number of phase-shift steps used to infer the fully complex information. Taking Tajahuerce's four-step encoding method¹⁹ as an example, we briefly describe the PSI-based optical cryptosystem. The encryption procedure is based on Mach–Zehnder interferometer architecture. A random phase mask is attached to the input image in the object beam and another random phase mask is located at a variable position in the reference arm. There are also two phase retarders, one quarter- and one half-wave plate, inserted in the reference beam. By aligning the different slow and fast axes with the direction of the polarization, shifting phase values of 0, $-\pi/2$, $-\pi$, and $-3\pi/2$ can be produced. In this way, four phase-shifting interferograms are generated on the output plane and captured in turn by a CCD camera. Figures 1(a) and 1(b) show the encryption and decryption procedures, respectively. To facilitate the analysis, we mathematically describe them. Assume that $t(x, y)$ is the amplitude object (a plaintext) to be encrypted and $\phi_1(x, y)$ is the random phase mask attached to the object. The complex amplitude distribution of the Fourier transformation pattern at the output plane, $U_O(x, y)$, is

$$U_O(x, y) = FT\{t(x, y) \cdot \exp[i\phi_1(x, y)]\}, \quad (1)$$

where $FT\{\cdot\}$ denotes the Fourier transform operator. Assume that the reference phase $\phi_2(x, y)$ (another random phase mask) is placed at a distance z from the CCD. Then the complex amplitude distribution of the reference beam at the exit of the interferometer can be expressed by

$$U_R(x, y; \alpha) = \exp(i\alpha) \cdot FRT_{\lambda, z}\{\exp[i\phi_2(x', y')]\}, \quad (2)$$

where $FRT_{\lambda, z}\{\cdot\}$ denotes the Fresnel diffraction with the illumination wavelength of λ and the distance of z . α is the relative phase changes introduced by the retarder plates on the reference beam. Let $U_O(x, y) = A_O \exp[i\phi_O(x, y)]$, $U_R(x, y, \alpha) = A_R \exp\{i[\phi_R(x, y) + \alpha]\}$, then the intensity pattern recorded by the CCD camera is given by

$$I(x, y; \alpha) = |U_O(x, y) + U_R(x, y; \alpha)|^2 = [A_O(x, y)]^2 + [A_R(x, y)]^2 + 2A_O(x, y)A_R(x, y) \times \cos[\phi_O(x, y) - \phi_R(x, y) - \alpha]. \quad (3)$$

In this way, the phase $\phi_E(x, y)$ and the amplitude $A_E(x, y)$ of the ciphertext can be recorded with the interferograms as follows:^{22,23}

$$\phi_E(x, y) = \arctan \left[\frac{I(x, y; -3\pi/2) - I(x, y; -\pi/2)}{I(x, y; 0) - I(x, y; -\pi)} \right], \quad (4)$$

$$A_E(x, y) = \frac{1}{4} \frac{I(x, y; 0) - I(x, y; -\pi)}{\cos[\phi_O(x, y) - \phi_R(x, y)]}. \quad (5)$$

The PSI-related Eqs. (3)–(5) have apparently complex and nonlinear forms, whereas the following simple relations also exist

$$\phi_E(x, y) = \phi_O(x, y) + \phi_R(x, y), \quad (6)$$

$$A_E(x, y) = A_O(x, y) A_R(x, y). \quad (7)$$

Equations (6) and (7) enable an easy approach in decryption, as shown in Fig. 1(b). However, they also reveal the linear property of the decryption system. It is known that linear cryptosystems may be vulnerable to impulse attack,^{13, 15} because linear systems can always be described by their impulse responses. Unfortunately, impulse attack is only helpful to retrieve the phase key but inadequate to recover the geometric key.

Now let us discuss the keys of the cryptosystem. In the encryption procedure, two random phase masks $\{\exp[i\phi_1(x, y)]$ and $\exp[i\phi_2(x', y')]\}$, the phase keys } and a distance parameter of Fresnel diffraction (z , the geometric key) are the encryption keys. In regular secure communications between two persons, from the symmetric cryptography point of view, the encryption keys are always fixed, because changing keys may lead to a burden of safely distributing keys. In other words, if different encryption keys are used in different encryption procedures, in each communication, the sender who sends a cipher message to the receiver has to find another absolute secure channel to transmit the keys. It will greatly degrade the practicability of the cryptosystem. To this point, it is reasonable to assume the encryption keys will not be changed, from the symmetric cryptanalysis point of view. Once $\exp[i\phi_2(x', y')]$ and z are fixed, infer from Eq. (2), $\phi_R(x, y)$ and $A_R(x, y)$ are also invariable. Therefore, in the case of amplitude image encryption, none of the three encryption keys is necessary for decryption. Only $\phi_R(x, y)$ and $A_R(x, y)$ serve as the decryption keys. By deducing the amplitude and the phase of $U_O(x, y)$ from Eqs. (6) and (7), one can recover the amplitude object $t(x, y)$ from the inverse Fourier transform intensity. It indicates that only Eqs. (1)–(7) are enough to exactly describe the relationship between plaintext, ciphertext, and decryption keys.

In Sec. 3, we demonstrate that the decryption keys $\phi_R(x, y)$ and $A_R(x, y)$ can be retrieved through a chosen-plaintext attack, choosing a delta function as a known resource.

3 Chosen-Plaintext Attack

3.1 Retrieve the Decryption Keys $\phi_R(x, y)$ and $A_R(x, y)$

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.²⁴ At first, we choose a Dirac delta function, $t_1(x, y) = \delta(x - x_1, y - y_1)$, as the known plaintext, and also know the corresponding ciphertext. Assume the amplitude and the phase of the ciphertext are $A_{E1}(x, y)$ and $\phi_{E1}(x, y)$, respectively. According to Eq. (1), we have

$$U_{OI}(x, y) = FT\{\delta(x - x_1, y - y_1) \cdot \exp[i\phi_1(x, y)]\} = \exp[i\phi_1(x_1, y_1)]. \quad (8)$$

Therefore, $A_{OI} = 1$ and $\phi_{OI}(x, y) = \phi_1(x_1, y_1)$. Then substituting them into Eqs. (6) and (7), we have

$$\phi_R(x, y) = \phi_{OI}(x, y) + \phi_{EI}(x, y) = \phi_1(x_1, y_1) + \phi_{EI}(x, y), \quad (9)$$

$$A_R(x, y) = A_{OI}(x, y)A_{EI}(x, y) = A_{EI}(x, y). \quad (10)$$

Note that $A_{EI}(x, y)$ and $\phi_{EI}(x, y)$ are known resources. $\phi_1(x_1, y_1)$ is a constant phase angle, corresponding to one pixel value of $\phi_1(x, y)$ at the coordinate $(x = x_1, y = y_1)$. In the discrete condition, $\phi_1(x, y)$ in Eq. (9) represents a matrix with all the elements equal to $\phi_1(x, y)$, which can be ignored or set to be 0. Then the estimates of the cracked decryption keys are obtained as follows:

$$\phi_R^*(x, y) = \phi_{EI}(x, y), \quad (11)$$

$$A_R^*(x, y) = A_{EI}(x, y), \quad (12)$$

where the asterisk denotes the estimate value. Inferred from Eqs. (11) and (12), theoretically the cracked $A_R(x, y)$ is equal to the true one and the cracked $\phi_R(x, y)$ is an estimate that the same phase value is added to the true one in all pixels. Nevertheless, this deviation will not tamper the decryption, demonstrated in the following simulations.

3.2 Computer Simulations

The validity of the cracked keys is verified by computer simulations performed under the environment of MATLAB 7.01. Assume that in the encryption procedure, the two random phase keys of the PSI-based optical cryptosystem are $\exp[i\phi_1(x, y)]$ and $\exp[i\phi_2(x', y')]$, and the geometric key z is equal to 30 mm. A pair of decryption keys, shown in Figs. 2(a) and 2(b), is generated from a Fresnel transform of $\exp[i\phi_2(x', y')]$ with a diffraction distance of z . Here we call them phase key and amplitude key, respectively. Assume that an attacker has obtained a ciphertext [amplitude in Figs. 3(b) and phase in Fig. 3(c)] corresponding to a plaintext of Dirac delta function, $\delta(x - x_1, y - y_1)$ [Fig. 3(a), 256×256 pixels]. The discrete Dirac delta function is displayed as a matrix with only one nonzero pixel located at pixel coordinate (x_1, y_1) . Without loss of generality, we set the value of the middle pixel to be 1 and the others 0 ($x_1 = 129, y_1 = 129$). With the specially chosen plaintext-ciphertext pair, the attacker can retrieve the estimates of the decryption keys by using the proposed chosen-plaintext attack. The retrieved keys are shown in Figs. 4(a) and 4(b).

The correlation coefficient between two images A and B is defined as follows:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left[\sum_m \sum_n (A_{mn} - \bar{A})^2 \right] \left[\sum_m \sum_n (B_{mn} - \bar{B})^2 \right]}}, \quad (13)$$

where $\bar{A}$ and $\bar{B}$ denote the mean values of images A and B . A_{mn} and B_{mn} are the pixel values at the coordinate (m, n) of images A and B , respectively. According to Eq. (13), we calculate the correlation coefficient between the estimates and the real keys to be 1 for

amplitude key and 0.7545 for phase key. It indicates that the amplitude key is completely recovered, but the retrieved phase key has a certain deviation from the true one. As mentioned above, this deviation is only due to the same phase value is added to the true phase key in all pixels and will not degrade the decryption effectiveness. It can be approved by decoding another ciphertext, which is encrypted with the same cryptosystem, with the retrieved decryption keys.

Figures 5(b) and 5(c) depict the amplitude and phase of another ciphertext obtained by the attacker. The corresponding plaintext is the Lena image (256×256 pixels), shown in Fig. 5(a). By using the retrieved decryption keys, one can recover Lena as shown in Fig. 6, from the corresponding ciphertexts. Again, according to Eq. (13), the correlation coefficient between the recovered Lena image and the original one is calculated to be 1. This result demonstrates an accurate decryption by using the proposed CPA method.

4 Conclusion

In conclusion, we have proposed a chosen-plaintext attack against the optoelectronic encryption scheme based on the phase-shifting interferometry. By performing this attack, an illegal user can recover any plaintext from the corresponding ciphertext with a pair of cracked decryption keys. The process of cracking the decryption keys can also be illustrated from the perspective of optical phenomenon, since a Dirac delta function is chosen as the object to be encrypted, which is directly multiplied by a random phase mask in the arm of object beam. The product still represents a plane wave with amplitude of 1 and phase of a constant value. At the output plane, CCD detects the interferograms of the object beam (a plane wave) and the reference beam (consisting of the amplitude key and phase key). Essentially, using the PSI technique to encrypt a Dirac delta function is just a process of recording the decryption keys.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 60775021 and 60777008), Independent Innovation Foundation of Shandong University, Grant No. 2010TB019, NIH (SC COBRE P20RR021949 and Career Award 1k25hl088262-01) and NSF (MRI CBET-0923311 and SC EPSCoR RII EPS-0903795 through SC GEAR program). Xiang Peng and Bruce Gao would also like to acknowledge the support from the grant established by the State Key Laboratory of Precision Measuring Technology and Instruments (Tianjin University).

References

1. Javidi B. Securing information with optical technologies. *Physics Today*. 1997; 50:27–32.
2. Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* 1995; 20:767–169.
3. Han JW, Park CS, Ryu DH, Kim ES. Optical image encryption based on XOR operations. *Opt. Eng.* 1999; 38:47–54.
4. Wang PK, Watson LA, Chatwin C. Random phase encoding for optical security. *Opt. Eng.* (Bellingham). 1996; 35:2464.
5. Li Y, Kreske K, Rosen J. Security and encryption optical systems based on a correlator with significant output images. *Appl. Opt.* 2000; 39:5295–5301. [PubMed: 18354525]
6. Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture. *Opt. Eng.* 2000; 39:2031–2035.
7. Situ G, Zhang J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* 2004; 29:1584–1586. [PubMed: 15309826]

8. Meng XF, Cai LZ, Yang XL, Shen XX, Dong GY. Information security system by iterative multiple-phase retrieval and pixel random permutation. *Appl. Opt.* 2005; 45:3289–3297. [PubMed: 16676034]
9. Meng XF, Cai LZ, Wang YR, Yang XL, Xu XF, Dong GY, Shen XX, Zhang H, Cheng XC. Hierarchical image encryption based on cascaded iterative phase retrieval algorithm in the Fresnel domain. *J. Opt. A: Pure Appl. Opt.* 2007; 9:1070–1075.
10. Chang HT, Lu WC, Kuo CJ. Multiple-phase retrieval for optical security systems by use of random phase encoding. *Appl. Opt.* 2002; 41:4825–4834. [PubMed: 12197649]
11. Qin W, Peng X. Asymmetric cryptosystem based on phase-truncated Fourier transform. *Opt. Lett.* 2010; 35:118–120. [PubMed: 20081940]
12. Carnicer A, Montes-Usategui M, Arcos S, Juvells I. Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* 2005; 30:1644–1646. [PubMed: 16075524]
13. Frauel Y, Castro A, Naughton TJ, Javidi B. Resistance of the double random phase encryption against various attacks. *Opt. Express.* 2007; 15:10253–10265. [PubMed: 19547374]
14. Peng X, Wei H, Zhang P. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* 2006; 31:1044–1046. [PubMed: 16625897]
15. Peng X, Tang HQ, Tian JD. Ciphertext-only attack on double random phase encoding optical encryption system. *Acta Physica Sinica.* 2007; 56:2629–2636. (In Chinese).
16. Peng X, Zhang P, Wei H, Yu B. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* 2006; 31:3261–3263. [PubMed: 17072390]
17. Qin W, Peng X. Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys. *J. Opt. A: Pure Appl. Opt.* 2009; 11:075402.
18. Qin W, Peng X, Meng X. Cryptanalysis of optical encryption schemes based on joint transform correlator architecture. *Opt. Eng.* 2011; 50:028201.
19. Tajahuerce E, Matoba O, Verrall SC, Javidi B. Optoelectronic information encryption with phase-shifting interferometry. *Appl. Opt.* 2000; 39:2313–2320. [PubMed: 18345139]
20. Wang X, Zhao D. Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry. *Opt. Commun.* 2006; 268:240–244.
21. Meng XF, Cai LZ, Wang YR. Two-step phase-shifting interferometry and its application in image encryption. *Opt. Lett.* 2006; 31:1414–1416. [PubMed: 16642123]
22. La Mela C, Iemmi C. Optical encryption using phase-shifting interferometry in a joint transform correlator. *Opt. Lett.* 2006; 31:2562–2564. [PubMed: 16902619]
23. Yamaguchi I, Zhang T. Phase-shifting digital holography. *Opt. Lett.* 1997; 22:1268–1270. [PubMed: 18185816]
24. Stallings, W. *Cryptography and Network Security: Principles and Practice*. 2nd ed. New Jersey: Prentice Hall; 1999. p. 25–26.

Biographies

Wan Qin received his BS degree in applied physics and his MS degree in physical electronics from Taiyuan University of Technology, Taiyuan, China, in 2004 and 2007, respectively, and his PhD degree in optical engineering from Shenzhen University, Shenzhen, China, in June 2010. His research interests are solid-state laser, optical information security, and biophotonics.

Xiang Peng received his BS and MS degrees in optical engineering, and his PhD degree in instrumentation and metrology from the Tianjin University. He completed his post-doc at the Institute of Applied Optics at the University of Stuttgart as an Alexander von Humboldt Research Fellow. He had visiting positions at the University of Houston and the University of Calgary. He is currently a professor at the College of Optoelectronic Engineering, Shenzhen University. Before joining Shenzhen University, he was a professor at Tianjin University. His main interests are three dimensional imaging and modeling, optical metrology, and optical information processing.

Xiangfeng Meng obtained his PhD in 2008 with a specialty in optics engineering. He is currently an associate professor in Shandong University (Jinan, China). His research interests include optical nondestructive testing, phase-shifting interferometry, and optical information security. He has co-authored more than 40 professional papers in international publications.

Bruce Z. Gao received his BS degree in physical electronics and optoelectronics in 1985 and his MS degree in applied laser physics in 1988, both from Tianjin University, China. He received his PhD degree in biomedical engineering at the University of Miami in 1999, following a three-year post-doctoral training in cell and tissue engineering at the University of Minnesota. He is currently an associate professor in the Department of Bioengineering at Clemson University. His long-term research goal is to understand the mechanisms used by various cell types to form a functional tissue. To achieve this goal, he has been focusing his research on microfabrication, laser cell micromanipulation, coherent light and nonlinear optics-based 3D imaging and multiscale modeling to explore cell-cell interactions in an engineered microenvironment, such as a biochip.

Fig. 1. Diagrams of (a) encryption and (b) decryption procedures with phase-shifting interferometry architecture (Ref. 19).

(a)

(b)

Fig. 2.
Decryption keys (a) $\phi_R(x, y)$ and (b) $A_R(x, y)$ of the PSI-based optical cryptosystem.

Fig. 3.

(a) Specially chosen plaintext [Dirac delta function, the nonzero pixel located at (129, 129)], (b) amplitude, and (c) phase of complex ciphertext.

(a)

(b)

Fig. 4.

(a) Retrieved phase key

$$\phi_R^*(x, y)$$

and (b) amplitude key

$$A_R^*(x, y)$$

by using CPA.

Fig. 5.

(a) Plaintext ("Lena", $256 \times 256 \times 8$ bits), (b) amplitude and (c) phase of complex.

Fig. 6.
Decryption result with the retrieved decryption keys.