Applied Physics B (2023) 129:130
https://doi.org/10.1007/s00340-023-08077-w

Applied Physics B
Lasers and Optics

RESEARCH

Optical double-image cryptosystem based on phase truncation in the Fresnel domain

Guangyu Luan[1,2] · Chenggen Quan[2]

Received: 23 May 2023 / Accepted: 14 July 2023 / Published online: 20 July 2023

Abstract

In this study, we propose an optical double-image information-leakage-free cryptosystem using phase truncation in the Fresnel domain. During the encryption process, two plaintexts by three public keys are encoded as one ciphertext mask and three private key masks. In the proposed method, the leakage of the information on two plaintexts as well as their silhouettes are no longer appear despite the use of one, two or even three masks for decryption. Moreover, the illuminating wavelength, the two diffraction distances and the three parameters of chaotic pixel scrambling also function as six additional keys to enhance security significantly. This scheme also avoids the crosstalk problem and dismisses the vulnerability against the special attack. Numerical simulations are conducted to demonstrate the effectiveness and validity of the proposed method.

1 Introduction

Optical encryption techniques [1–11] have attracted increasing attention recently for image security due to the excellent characteristics in terms of parallel processing and multiple parameters. The most attractive technique of double-random phase encoding (DRPE) was firstly realized in the Fourier transform domain [12]. Afterwards, many techniques have been attempted to develop DRPE to other different transform domains [13–17], involving the gyrator transform domain, Fresnel transform domain, fractional Fourier transform domain, and so on. In the meantime, other optical encryption techniques [18–30], which make use of digital holography, compressive sensing, iterative phase retrieval, photon counting, polarized light, and optical interference, have also been devised to strengthen the information security.

The phase-truncated Fourier transform (PTFT) technique initiated by Qin and Peng [31] has opened a new encryption way. Subsequently, other encryption techniques based on phase truncation were also emerged in the Fresnel transform domain or the fractional Fourier transform domain [32–35]. Wang et al. [36] studied the risk of information disclosure in the PTFT-based cryptosystem. This study revealed that most original information could be divulged when one of two private keys is released. It is highly probable that a risk of unintended information leakage exists in the above-mentioned cryptosystems [32–35]. To prevent the information leakage, new encryption techniques based on phase truncation were reported. For instance, Wang et al. [37] employed a cascading manner to realize color image encryption. Wu et al. [38] constructed a scalable asymmetric image encryption method based on phase-truncation in cylindrical diffraction domain. In addition, the traditional PTFT technique is an asymmetric cryptosystem and destroys the linearity characteristics of DRPE. However, it can be cracked by using a specific attack [39], which is founded on an amplitude-phase retrieval method. Recently, other new techniques are developed for the increased security of optical image cryptosystems. For instance, Cai et al. [40] utilized coherent superposition and equal modulus decomposition (EMD) to eliminate the silhouette problem. However, the disadvantage of EMD concentrates on the same modulus of two masks. Random modulus decomposition (RMD) [41] can be regarded as unequal modulus decomposition [42], which means two masks with random moduli. Chaotic pixel scrambling (CPS) [9] stems from a pixel exchange mechanism. An asymmetric encryption and authentication technique [11] via EMD and sparse sampling was reported in the Fresnel domain. However, its output masks were complex valued causing inconvenient

✉ Guangyu Luan
luanguangyu@126.com

[1] College of Electrical and Information, Heilongjiang Bayi Agricultural University, Daqing 163319, Heilongjiang, China

[2] Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

for display, storage, and transmission. Therefore, despite the significant progress, attaining high security continues to be a major challenge for optical image encryption using phase truncation.

To simultaneously eliminate the issues of linearity system, complex-valued output, and information leakage, we propose a novel crosstalk-free method in the Fresnel domain via phase truncation into optical double-image cryptosystem. The proposed method has one ciphertext and three private keys and can dismiss the vulnerability against the special attack. In addition, the illuminating wavelength, the two diffraction distances, and the three parameters of CPS provide additional keys to realize security enhancement. The numerical simulation results demonstrate the reliability and validity of the proposed method.

2 Principle of the method

In the proposed cryptosystem, assume the two original images $I_1(x, y)$ and $I_2(x, y)$ to be encrypted, the following steps are implemented for double-image encryption:

(1) A complex value function $f(x, y)$ is constructed by $I_1(x, y)$ and $I_2(x, y)$ given by Eq. (1):

$$f(x, y)=I_1(x, y)+iI_2(x, y) \tag{1}$$

(2) An operation of chaotic pixel scrambling (CPS) is utilized to the function $f(x, y)$ for enhancing the security of the system:

$$fSC(x, y) = CPS_{\{a_0,k,p\}}\left[f(x, y)\right] \tag{2}$$

where a_0 denotes the initial value in the interval [0, 1], k represents the map coefficient in the interval [3.57,4], p is the truncated position. The CPS parameters a_0, k, and p are regarded as the additional keys (Fig. 1).

(3) The function $fSC(x, y)$ is separated into two complex-valued masks $P_1(x, y)$ and $P_2(x, y)$ with unequal moduli, as shown in. With the geometrical relationship and the random distributions of $\theta(x, y)$ and $\beta(x, y)$, $P_1(x, y)$ and $P_2(x, y)$ can be mathematically illustrated as

$$\arg\left[P_1(x, y)\right] = \theta(x, y) = 2\pi R_1(x, y) \tag{3}$$

$$\beta(x, y) = 2\pi R_2(x, y) \tag{4}$$

$$P_1(x, y) = \frac{A(x, y)\sin\beta(x, y)}{\sin\left(\varphi(x, y) - \theta(x, y) + \beta(x, y)\right)}\exp\left[i\theta(x, y)\right] \tag{5}$$

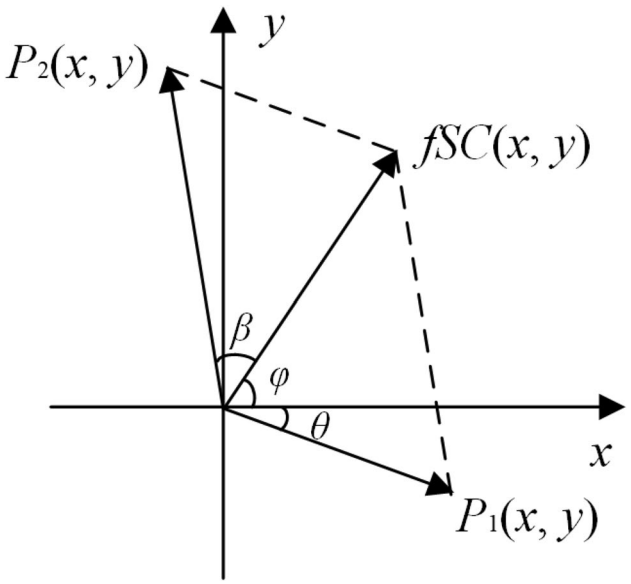

Fig. 1 Principle of RMD

$$P_2(x, y) = \frac{A(x, y)\sin\left(\varphi(x, y) - \theta(x, y)\right)}{\sin\left(\varphi(x, y) - \theta(x, y) + \beta(x, y)\right)}\exp\left[i(\varphi(x, y) + \beta(x, y))\right] \tag{6}$$

where $R_1(x, y)$ and $R_2(x, y)$ are both the random functions with uniform distribution in a range of [0, 1], $A(x, y)$ is the amplitude part of $fSC(x, y)$ and equal to $|fSC(x, y)|$, "$|\cdot|$" is the modulus operator, $\varphi(x, y)$ is the phase part of $fSC(x, y)$ and equal to $\arg\left[fSC(x, y)\right]$, "arg [·]" is the argument operator. $\theta(x, y)$ and $\beta(x, y)$ act as the public keys. $P_2(x, y)$ is regarded as the private key.

(4) The complex-valued mask $P_1(x, y)$ is Fresnel transformed, and then the phase truncation and the phase reservation are performed to generate $g(u_1, v_1)$ and $P_3(u_1, v_1)$, respectively:

$$g(u_1, v_1) = PT\left\{Fr\mathrm{T}_{(-d_1,\lambda)}\left[P_1(x, y)\right]\right\} \tag{7}$$

$$P_3(u_1, v_1) = PR\left\{Fr\mathrm{T}_{(-d_1,\lambda)}\left[P_1(x, y)\right]\right\} \tag{8}$$

where $PT\{\cdot\}$ is the phase truncation operator, $PR\{\cdot\}$ is the phase reservation operator, $FrT_{(-d_1,\lambda)}\{\cdot\}$ is the operator of Fresnel transform with the diffraction distance $-d_1$ and the wavelength λ. $P_3(u_1, v_1)$ is regarded as the private key.

(5) The operation of Fresnel transform with the diffraction distance $-d_2$ and the wavelength λ is carried out for the function $g(u_1, v_1)$ boned with the random distribution $R_3(u_1, v_1)$. Finally the ciphertext $C(u_2, v_2)$ and the private key $P_4(u_2, v_2)$ can be generated by conducting the $PT\{\cdot\}$ and $PR\{\cdot\}$:

$$C(u_2, v_2) = PT\left\{ \mathrm{FrT}_{(-d_2,\lambda)}\left[g(u_1, v_1) \cdot \exp\left[i2\pi R_3(u_1, v_1)\right]\right]\right\} \tag{9}$$

shows the encryption process and Fig. 2b illustrates the decryption process.

In the decryption process, the retrieved complex value function $f\prime(x, y)$ by the legal users is deduced as

$$f\prime(x, y) = ICPS_{\{a_0,k,p\}}\left[FrT_{(d_1,\lambda)}\left[PT\left[FrT_{(d_2,\lambda)}\left[C(u_2, v_2) \cdot \exp\left[iP_4(u_2, v_2)\right]\right]\right] \cdot \exp\left[iP_3(u_1, v_1)\right]\right] + P_2(x, y)\right] \tag{11}$$

$$P_4(u_2, v_2) = PR\left\{ \mathrm{FrT}_{(-d_2,\lambda)}\left[g(u_1, v_1) \cdot \exp\left[i2\pi R_3(u_1, v_1)\right]\right]\right\} \tag{10}$$

where $R_3(u_1, v_1)$ is a random distribution in the range of [0, 1]. A flowchart for illustrating the proposed nonlinear cryptosystem is depicted in Fig. 2. Figure 2a

where $ICPS_{\{a_0,k,p\}}[\cdot]$ is the operator of inverse chaotic pixel scrambling (ICPS). After separating the real and the imaginary components of $f\prime(x, y)$, two original images can be visualized. Obviously, the recovered results of the proposed scheme are free from crosstalk noise. The schematic optical system for the decryption procedure is shown in Fig. 3. Spatial light modulators (SLM_1 and SLM_2) placed at designated

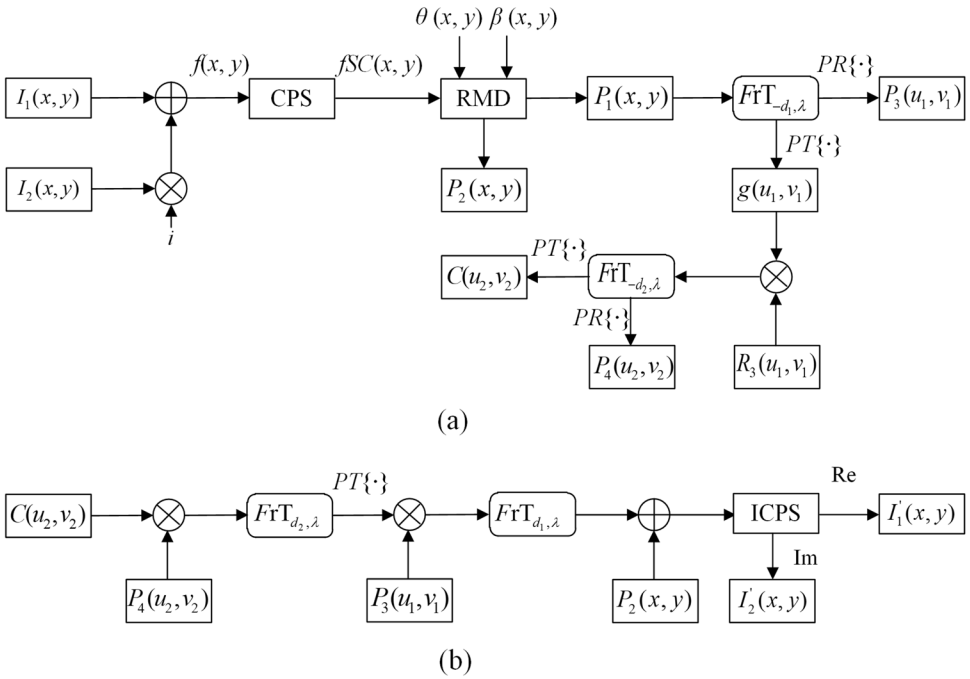

Fig. 2 Schematic diagram of the proposed **a** encryption process, **b** decryption process

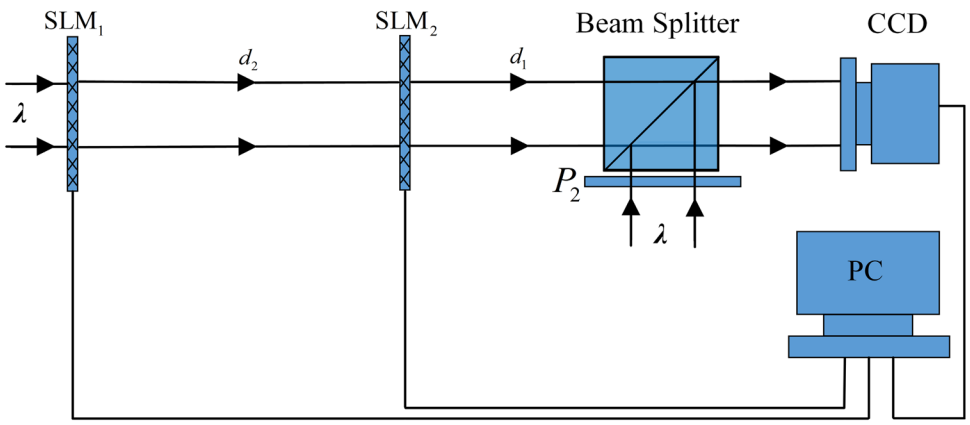

Fig. 3 Schematic optical setup for decryption process

places are employed for modulating phase information. The operation of ICPS can be digitally carried out in the computer. It should be noted that the impact of optical parameters need be considered while doing the optical experimental validation.

3 Numerical results and performance analysis

To verify the feasibility and the advantages of the proposed method, numerical simulations are carried out. In the simulations, the laser wavelength λ is 633 nm, the two axial distances d_1 and d_2 are 50 mm and 90 mm respectively, and the three CPS parameters a_0, k, p are set as $a_0 = 0.241$, $k = 3.97$, and $p = 11096$, respectively. To evaluate the similarity between the original image $I_k(x, y)$ ($k = 1, 2$) and the decrypted image $I_k'(x, y)$, the correlation coefficient (CC) is expressed as

$$CC = \frac{E\left\{\left[I_k(x,y) - E\left[I_k(x,y)\right]\right]\right\}\left\{\left[I_k'(x,y) - E\left[I_k'(x,y)\right]\right]\right\}}{E\sqrt{\left\{\left[I_k(x,y) - E\left[I_k(x,y)\right]\right]^2\right\}}\sqrt{\left\{\left[I_k'(x,y) - E\left[I_k'(x,y)\right]\right]^2\right\}}} \tag{12}$$

Two original images with a size of 256×256 pixels as shown in Fig. 4a,b are utilized as the two plaintexts. After the CPS operation, two public keys $\theta(x, y)$ (Fig. 4c) and $\beta(x, y)$ (Fig. 4d) are utilized in the RMD to generate two complex-valued matrices $P_1(x, y)$ (Fig. 4e) and $P_2(x, y)$ (Fig. 4f). Then $P_1(x, y)$ and $R_3(u_1, v_1)$ (Fig. 4h) are utilized to perform phase truncation in the Fresnel domain for producing the two phase masks $P_3(u_1, v_1)$ (Fig. 4g) and $P_4(u_2, v_2)$ (Fig. 4i), and the amplitude mask $C(u_2, v_2)$ (Fig. 4j). The recovered images as shown in Fig. 4k, l are attained for all the correct security keys and ciphertexts for decryption. The CC values between Fig. 4a, k are 1.0000. The CC values between Fig. 4b, l are 1.0000. These results illustrate that each of the two decrypted images $I_1'(x, y)$ and $I_2'(x, y)$ is exactly equal to its corresponding original image. It is shown that all information of the two original images has been retrieved without crosstalk noise.

To demonstrate the information-leakage-free of the proposed method, Fig. 5a–h illustrate the decrypted images when one of P_2, P_3, P_4, and C is released. The CC values are 0.0066, 0.0011, − 0.0024, − 0.0075, 0.0053, − 0.0012, − 0.0026, − 0.0011, respectively. Figure 6a–l show the decrypted images retrieved by two of these masks. The CC values are 0.0017, − 0.0013, 0.0071, 0.0062, 0.0015, 0.0076, 0.0064, − 0.0022, 0.0039, 0.0025, − 0.0024, 0.0029,

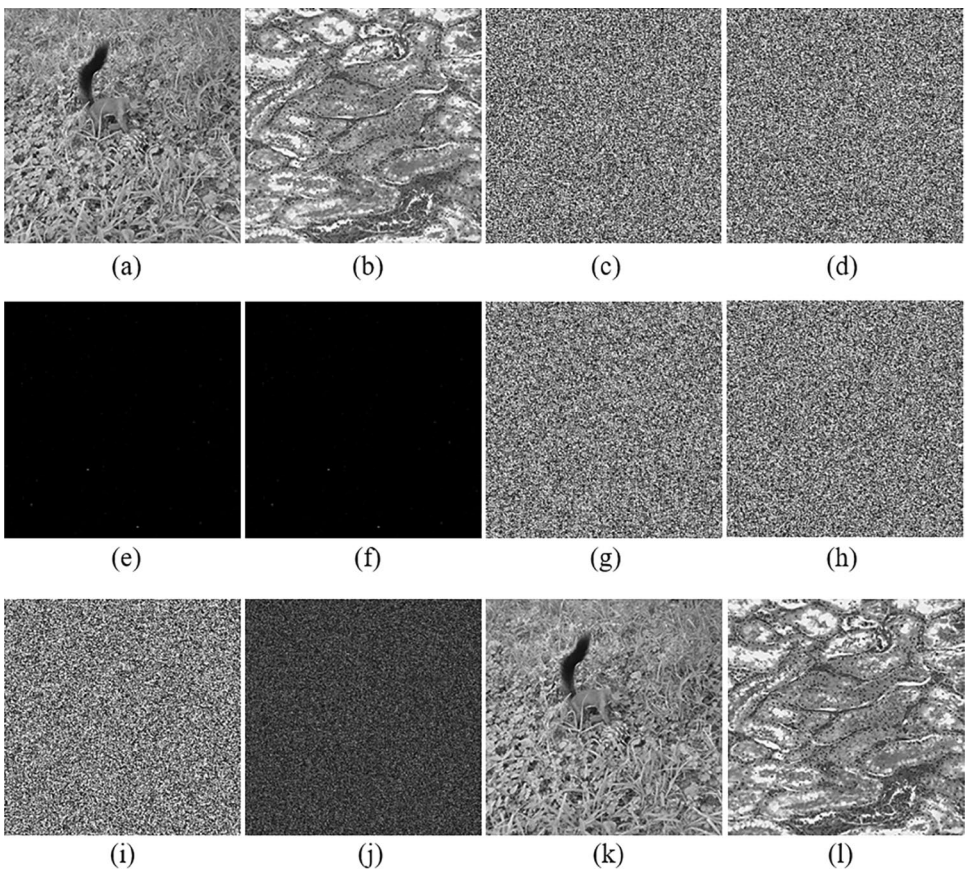

Fig. 4 Encryption and decryption results of the proposed cryptosystem: **a** and **b** two images to be encrypted, **c** the public key $\theta(x, y)$, **d** the public key $\beta(x, y)$, **e** the mask $P_1(x, y)$, **f** the private key $P_2(x, y)$, **g** the private key $P_3(u_1, v_1)$, **h** the public key $R_3(u_1, v_1)$, **i** the private key $P_4(u_2, v_2)$, **j** the ciphertext $C(u_2, v_2)$, **k** and **l** the two decrypted images with all correct private keys

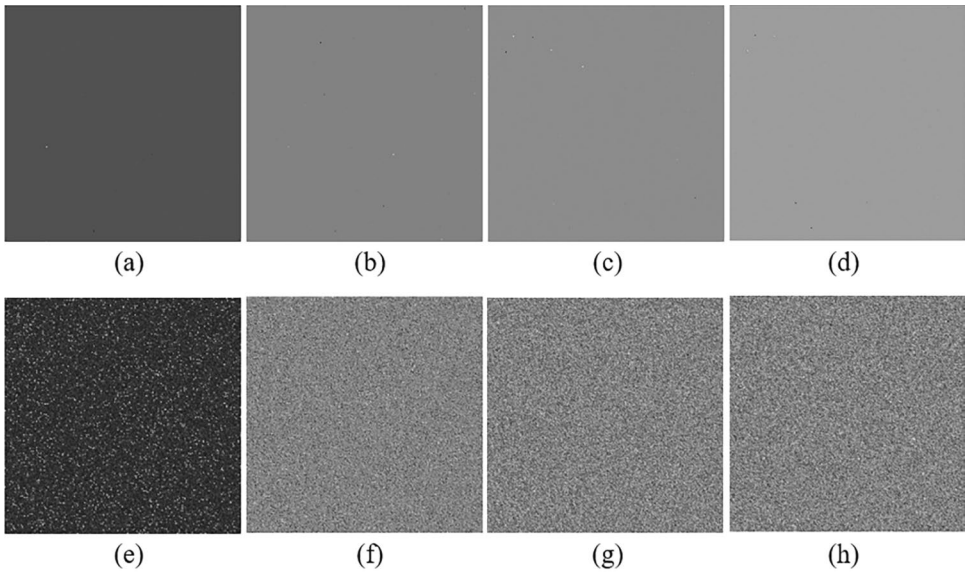

Fig. 5 The decrypted images with **a** and **b** P_2, **c** and **d** P_3, **e** and **f** P_4, **g** and **h** C (the ciphertext)

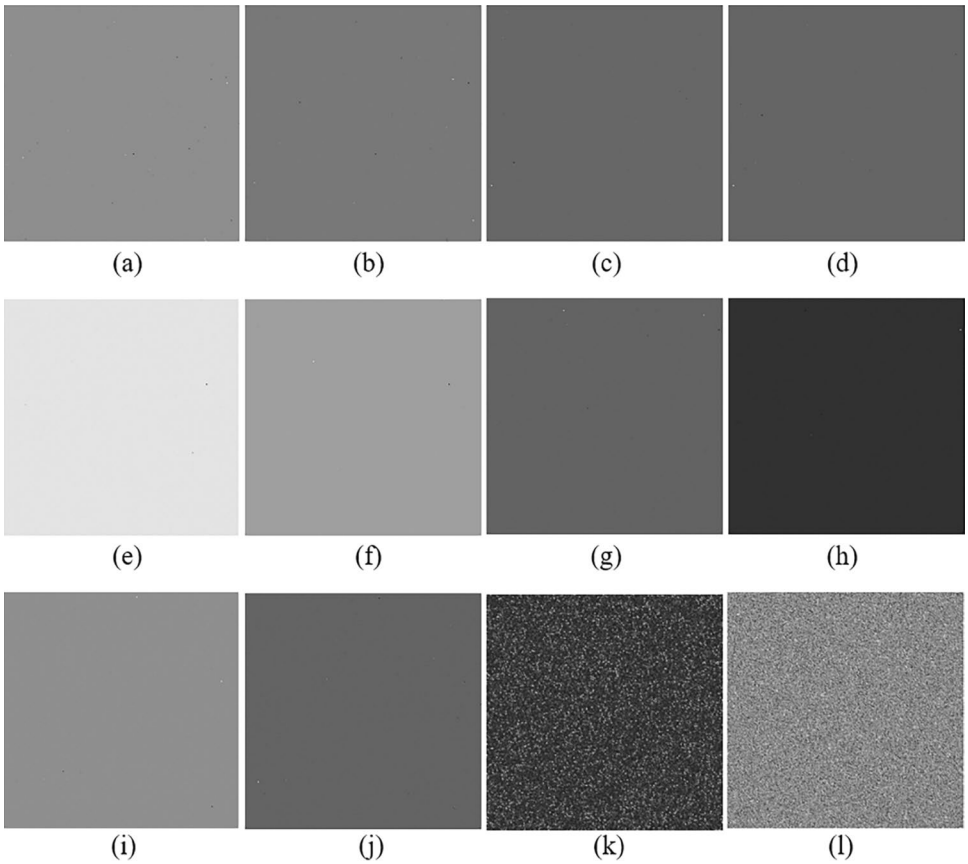

Fig. 6 The decrypted images with **a** and **b** P_2 and P_3, **c** and **d** P_2 and P_4, **e** and **f** P_2 and C (the ciphertext), **g** and **h** P_3 and P_4, **i** and **j** P_3 and C (the ciphertext), **k** and **l** P_4 and C (the ciphertext)

respectively. Figure 7a–h show the decrypted images produced when utilizing three of these masks. The CC values are 0.0048, 0.0061, 0.0042, 0.0068, 0.0042, 0.0029, 0.0076, 0.0021, respectively. It can be seen from Figs. 5, 6, 7 that none of all the decrypted images has information concerning the two plaintexts and their silhouettes. Hence, it is revealed that information leakage issues have been eliminated thoroughly in the proposed method.

We have further evaluated whether the proposed method is sensitive to the additional keys, i.e., the illuminating wavelength λ, the two diffraction distances d_1 and d_2, the three CPS parameters a_0, k, p. Figures 8, 9, 10, 11, 12, 13 show

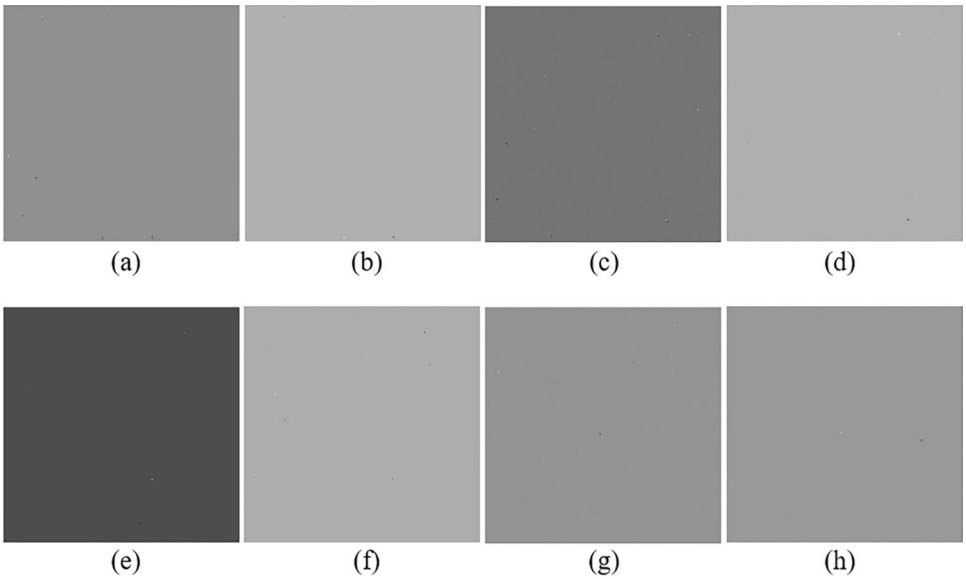

Fig. 7 The decrypted images with **a** and **b** P_2, P_3, and P_4, **c** and **d** P_2, P_3, and C (the ciphertext), **e** and **f** P_3, P_4, and C (the ciphertext), **g** and **h** P_2, P_4 and C (the ciphertext)

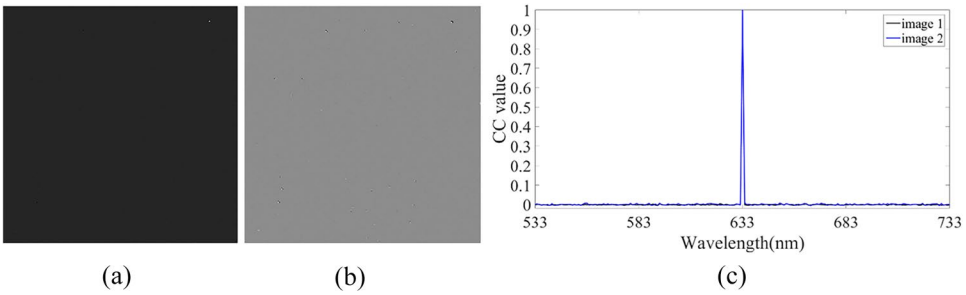

Fig. 8 **a** and **b** The decrypted two images with $\lambda = 632$ nm (i.e. $\Delta\lambda = 1$ nm), **c** relation curves between the CC value and the illuminating wavelength λ

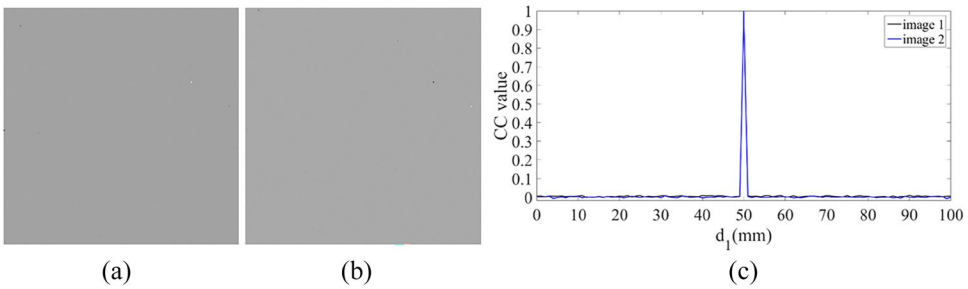

Fig. 9 **a** and **b** The decrypted two images with $d_1 = 49$ mm (i.e. $\Delta d_1 = 1$ mm), **c** relation curves between the CC value and the diffraction distance d_1

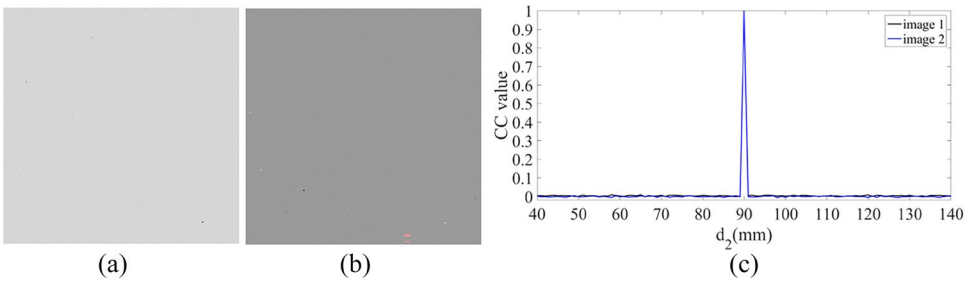

Fig. 10 **a** and **b** The decrypted two images with $d_2 = 89$ mm (i.e. $\Delta d_2 = 1$ mm), **c** relation curves between the CC value and the diffraction distance d_2

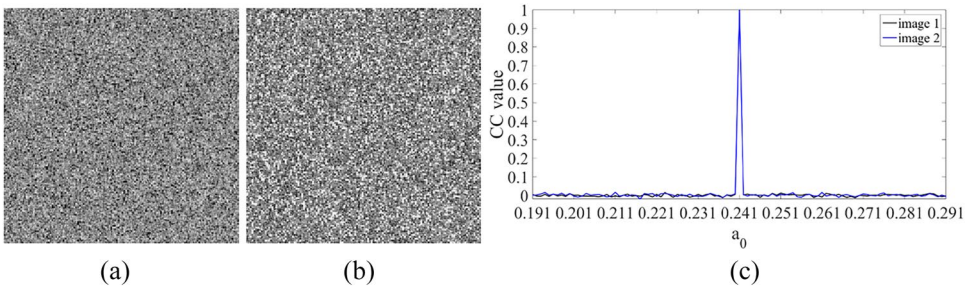

Fig. 11 **a** and **b** The decrypted two images with $a_0 = 0.24$ (i.e. $\Delta a_0 = 0.001$), **c** relation curves between the CC value and the initial value a_0 of CPS

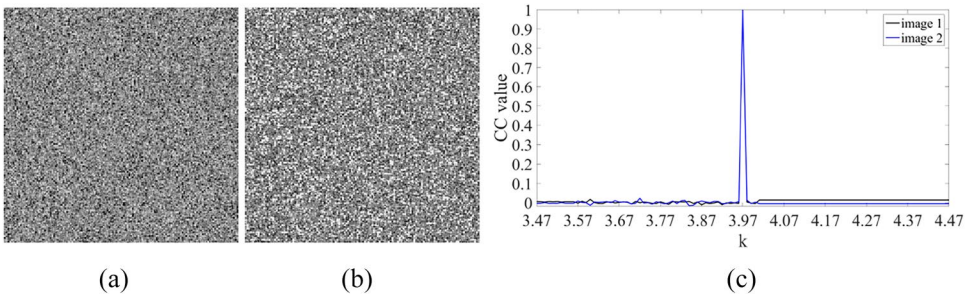

Fig. 12 **a** and **b** The decrypted two images with $k = 3.96$ (i.e. $\Delta k = 0.01$), **c** relation curves between the CC value and the map coefficient k of CPS

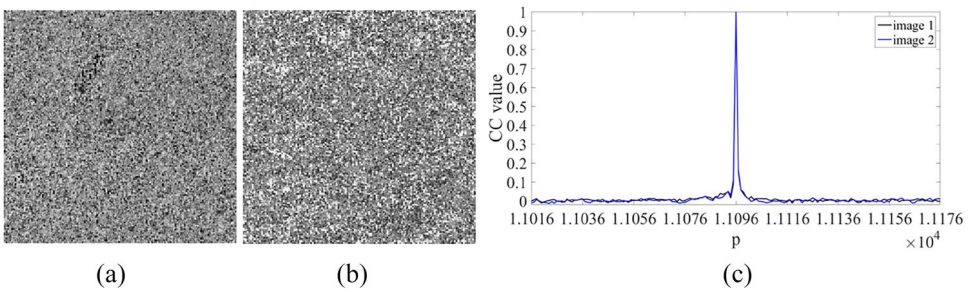

Fig. 13 **a** and **b** The decrypted two images with $p = 11{,}095$ (i.e. $\Delta p = 1$), **c** relation curves between the CC value and the truncated position p of CPS

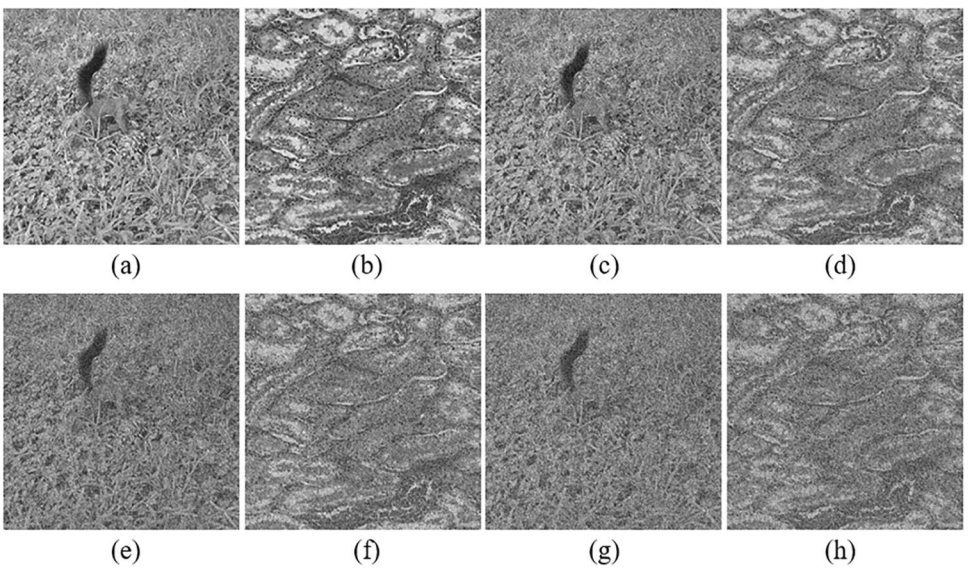

Fig. 14 Decrypted images with zero-mean white additive Gaussian noise with **a** and **b** $\sigma = 0.1$, **c** and **d** $\sigma = 0.2$, **e** and **f** $\sigma = 0.3$, **g** and **h** $\sigma = 0.4$

the sensitive results of those keys. These results invariably reveal that information discrimination for the two plaintexts is prohibited in the case that any one of the above-mentioned keys has a minor error. Therefore, the proposed method has six sensitive additional keys, which can strengthen the security of the proposed method.

To further assess the robustness of the proposed method against noise attacks, Fig. 14 demonstrates the decrypted images with white additive Gaussian noise, which has a mean of 0 and $\sigma = 0.1$ (Fig. 14a, b), $\sigma = 0.2$ (Fig. 14c, d), $\sigma = 0.3$ (Fig. 14e, f), $\sigma = 0.4$ (Fig. 14g, h). In addition, the CC values are 0.9532, 0.9659, 0.8453, 0.8819, 0.7235, 0.7767, 0.6210, 0.6835, respectively. From these results, it is shown that the proposed method has the resistance capability for noise attacks.

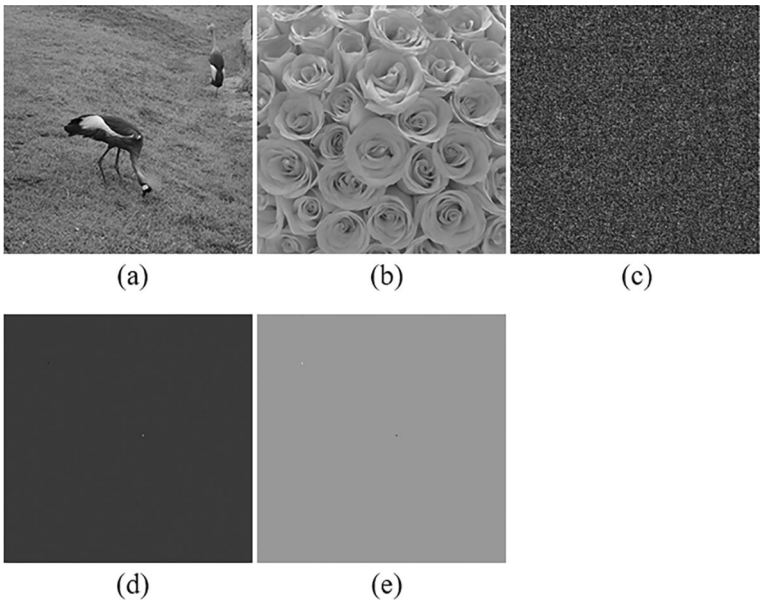

Fig. 15 KPA on the proposed scheme: **a** and **b** the two original images to be retrieved, **c** the ciphertext of **a** and **b**, **d** and **e** the two retrieved images using private keys in Fig. 4f, g, i and all correct parameters

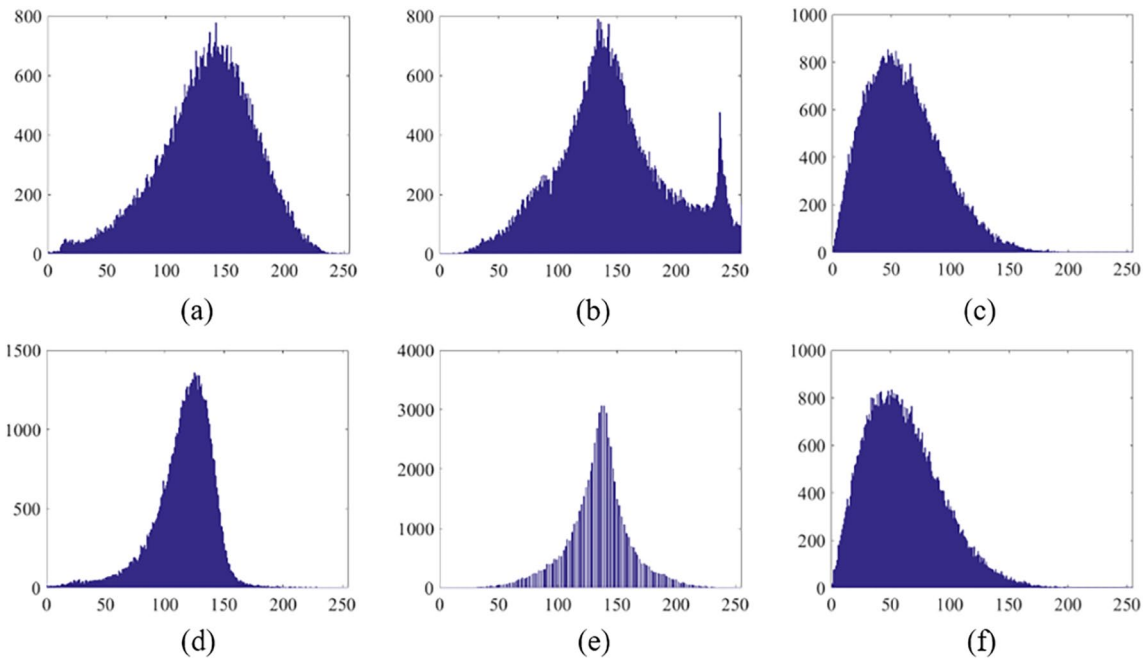

Fig. 16 Histogram comparison results: (a) and (b) the histograms of Fig. 4a and b, c the histogram of Fig. 4j, d and e the histograms of Fig. 15a and b, f the histogram of Fig. 15c

In addition, we have also evaluated the validity of the proposed method against known-plaintext attack (KPA). In KPA, assume that the attackers can access the known plaintext-ciphertext pairs as well as the encryption scheme. In the simulation, Fig. 4a, b and Fig. 4j are utilized as a pair of the two known plaintexts and their corresponding ciphertext. The proposed method is employed to encrypt two images in Fig. 4a, b, private keys in Fig. 4f, g and i are generated. Two images with size 256×256 retrieved are shown in Fig. 15a, b. The corresponding ciphertext produced by the proposed method is shown in Fig. 15c. Using the private keys (Fig. 4f, g and i) and all correct parameters, the two retrieved images are shown in Fig. 15d, e. From these results (Fig. 15), it is shown that no information of the two original images can be visible. Thus, the proposed method is free from the KPA.

We have also validated the statistical property of the proposed method; histogram comparison results are illustrated in Fig. 16. It is noteworthy that there is a significant difference among Fig. 16a–c, as well as among Fig. 16d–f. Besides, the histograms (Fig. 16c, f) have similar distributions. As a result, any useful information cannot be accessed by the attackers in accordance with the statistical property.

Finally, to demonstrate the effectiveness of the proposed method against a potential specific attack (PSA), a simulation is carried out. In a ciphertext-only attack, assume that the attackers can access the given ciphertext as well as the encryption scheme. In the simulation, Fig. 17 illustrates a flowchart of the PSA. The three public keys $\theta(x, y)$, $\beta(x, y)$, $R_3(u_1, v_1)$ and the ciphertext $C(u_2, v_2)$ are employed as four constraints. Figure 15c is utilized as the given ciphertext in the PSA. Figure 18a–c show the results using the PSA. Figures 18d–f show the results using the specific attack [39]. From Fig. 18a, it is shown that the two curves are non-convergent and unstable. From Fig. 18b, c, we cannot see any information of the two original images (Fig. 15a, b). Thus, it is revealed that the proposed method can effectively resist the PSA.

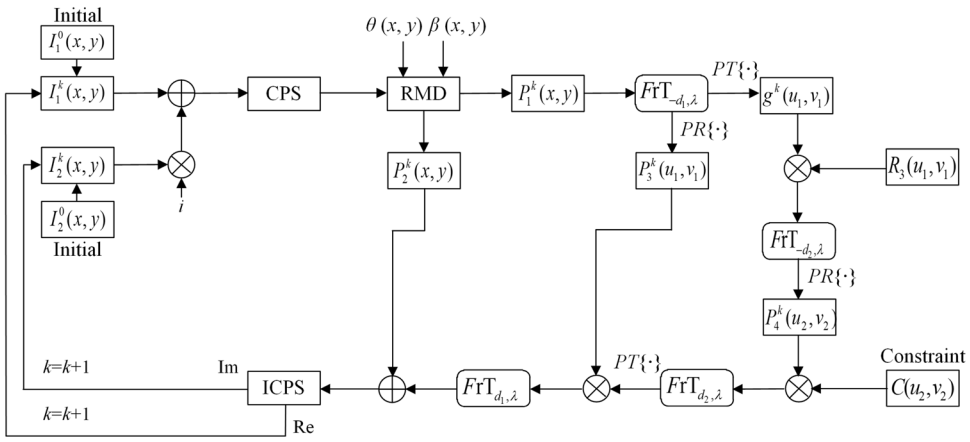

Fig. 17 A flowchart of a PSA

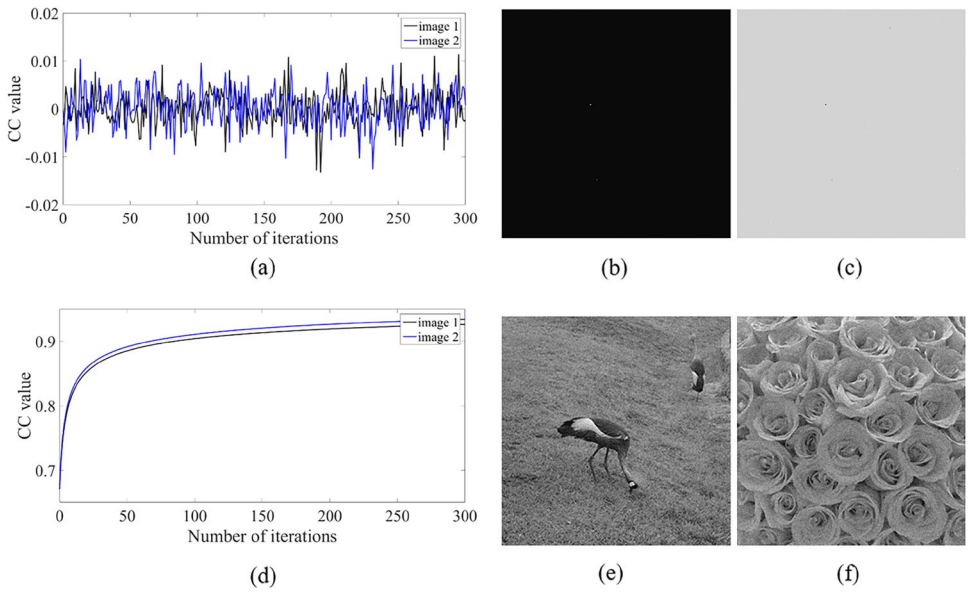

Fig. 18 Attack comparison results: CC value versus number of iterations using **a** the PSA, and **d** the specific attack [39], respectviely; the recovered images after 300 iterations using **b** and **c** the PSA, and **e** and **f** the specific attack [39], respectviely

4 Concluding remarks

In summary, an optical double-image cryptosystem using phase truncation in the Fresnel domain is developed. The proposed method utilizes three public keys to generate one ciphertext and three private keys. The method is novel and attains the decrypted images free from the crosstalk noise. Comparing to the existing schemes via phase truncation, the proposed method can completely alleviate the information leakage, and efficiently resist the specific attack. Meanwhile, six parameters (λ, d_1, d_2, a_0, k, p) act as additional keys for strengthening security significantly. Numerical simulations are carried out to validate the performance of the proposed method which provides a new solution for optical image cryptosystem by using phase truncation.

Author contributions GL: idea, programming and numerical analysis, writing manuscript. CQ: writing-reviewing and editing. The authors declared that they have no conflicts to interest to this work.

Funding This study is supported by China Scholarship Council [202208230113], Education Department Foundation of Heilongjiang Province of China [12541584], and Natural Science Foundation of Heilongjiang Province of China [C2018049, C2018050].

Data availability The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. A. Alfalou, C. Brosseau, Optical image compression and encryption methods. Adv. Opt. Photon. **1**, 589–636 (2009)
2. W. Chen, B. Javidi, X.D. Chen, Advances in optical security systems. Adv. Opt. Photon. **6**, 120–155 (2014)
3. L.S. Sui, X. Zhang, C.T. Huang et al., Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. Opt. Lasers Eng. **113**, 29–37 (2019)
4. V.C. Mandapati, H. Vardhan, S. Prabhakar et al., Multi-user nonlinear optical cryptosystem based on polar decomposition and fractional vortex speckle patterns. Photonics **10**, 561 (2023)
5. Y. Xiong, J. Gu, R. Kumar, Collision in a phase-only asymmetric cryptosystem based on interference and phase-truncated Fourier transforms. Opt. Quant. Electron. **55**, 667 (2023)
6. Y.L. Zhou, M. Yang, B. Zhou et al., An optical image watermarking method based on computational ghost imaging and multiple logistic maps. Appl. Phys. B **128**, 134 (2022)
7. H.Y. Wei, X.G. Wang, Optical multiple-image authentication and encryption based on phase retrieval and interference with sparsity constraints. Opt. Laser Technol. **142**, 107257 (2021)
8. L.S. Sui, X.Y. Zhao, C.T. Huang et al., An optical multiple-image authentication based on transport of intensity equation. Opt. Lasers Eng. **116**, 116–124 (2019)
9. Z. Zhong, H.T. Qin, L. Liu et al., Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain. Opt. Exp. **25**, 6974–6982 (2017)
10. L. Liu, M.G. Shan, Z. Zhong et al., Compressive interference-based image encryption via sparsity constraints. Opt. Lasers Eng. **134**, 106297 (2020)
11. G.Y. Luan, A.C. Li, D.M. Zhang et al., Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain. IEEE Photonics J. **11**, 6900207 (2019)
12. P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**, 767–769 (1995)
13. L.S. Sui, M.T. Xin, A.L. Tian, Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain. Opt. Lett. **38**, 1996–1998 (2013)
14. J.X. Chen, Z.L. Zhu, Z.J. Liu et al., A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains. Opt. Exp. **22**, 7349–7361 (2014)
15. X.G. Wang, W. Chen, X.D. Chen, Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. Opt. Exp. **22**, 22981–22995 (2014)
16. L.S. Sui, K.K. Duan, J.L. Liang et al., Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. Opt. Exp. **22**, 10605–10621 (2014)
17. H.F. Xu, W.H. Xu, S.H. Wang et al., Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain. Opt. Commun. **402**, 302–310 (2017)
18. D. Maluenda, A. Carnicer, R. Martinez-Herrero et al., Optical encryption using photon-counting polarimetric imaging. Opt. Exp. **23**, 655–666 (2015)
19. X.W. Li, D. Xiao, Q.H. Wang, Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. Opt. Lasers Eng. **100**, 200–207 (2018)
20. L.F. Chen, G.J. Chang, B.Y. He et al., Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition. Opt. Lasers Eng. **88**, 221–232 (2017)
21. A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona et al., Security authentication using phase-encoded nanoparticle structures and polarized light. Opt. Lett. **40**, 135–138 (2015)
22. E. Perez-Cabre, M.J. Cho, B. Javidi, Information authentication using photon-counting double-random-phase encrypted images. Opt. Lett. **36**, 22–24 (2011)
23. Y. Zhang, B. Wang, Optical image encryption based on interference. Opt. Lett. **33**, 2443–2445 (2008)
24. A. Fatima, N.K. Nishchal, Optical image security using Stokes polarimetry of spatially variant polarized beam. Opt. Commun. **417**, 30–36 (2018)
25. N. Rawat, I.C. Hwang, Y. Shi et al., Optical image encryption via photon-counting imaging and compressive sensing based ptychography. J. Opt. **17**, 065704 (2015)
26. Y. Wang, C. Quan, C.J. Tay, Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm. Opt. Lasers Eng. **78**, 8–16 (2016)
27. Y.G. Su, C. Tang, X. Chen et al., Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. Opt. Lasers Eng. **88**, 20–27 (2017)
28. I. Moon, F. Yi, M. Han et al., Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms. Appl. Opt. **55**, 4328–4335 (2016)
29. Y. Chen, Q. Liu, J. Wang et al., Single-channel optical encryption of color image using chessboard grating and diffraction imaging scheme. Opt. Eng. **56**, 123106 (2017)
30. Y. Qin, Z.P. Wang, H.J. Wang et al., Robust information encryption diffractive-imaging-based scheme with special phase retrieval

algorithm for a customized data container. Opt. Lasers Eng. **105**, 118–124 (2018)
31. W. Qin, X. Peng, Asymmetric cryptosystem based on phase-truncated fourier transforms. Opt. Lett. **35**, 118–120 (2010)
32. S.K. Rajput, N.K. Nishchal, Image encryption based on interference that uses fractional Fourier domain asymmetric keys. Appl. Opt. **51**, 1446–1452 (2012)
33. W. Chen, X.D. Chen, Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. Opt. Commun. **284**, 3913–3917 (2011)
34. S.K. Rajput, N.K. Nishchal, Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask. Appl. Opt. **51**, 5377–5386 (2012)
35. I. Mehra, S.K. Rajput, N.K. Nishchal, Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification. Opt. Eng. **52**, 028202 (2013)
36. X.G. Wang, D.M. Zhao, Y.X. Chen, Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask. Appl. Opt. **53**, 5100–5108 (2014)
37. Y. Wang, C. Quan, C. Tay, Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask. Opt. Commun. **344**, 147–155 (2015)
38. C. Wu, K.Y. Hu, Y. Wang et al., Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain. Opt. Commun. **448**, 26–32 (2019)
39. X.G. Wang, Y.X. Chen, C.Q. Dai et al., Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform. Appl. Opt. **53**, 208–213 (2014)
40. J.J. Cai, X.J. Shen, M. Lei et al., Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition. Opt. Lett. **40**, 475–478 (2015)
41. H.F. Xu, W.H. Xu, S.H. Wang et al., Phase-only asymmetric optical cryptosystem based on random modulus decomposition. J. Mod. Optic. **65**, 1245–1252 (2018)
42. S. Sachin, R. Kumar, P. Singh, Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain. Opt. Quant. Electron. **53**, 254 (2021)