scientific reports

Check for updates

OPEN

Optical phase-truncation-based double-image encryption using equal modulus decomposition and random masks

Guangyu Luan[1]✉ & Chenggen Quan[2]

This work reports an optical double-image crosstalk free encryption scheme that employs equal modulus decomposition and random masks. For the encryption, two plaintexts by a random amplitude mask and a random phase mask have been encrypted into a single ciphertext mask and two private key masks. Owing to the two random masks introduced, the functional relation between the plaintext pair and the ciphertext indirectly cause the paucity of constraints employed for the specific attack. Unlike the traditional phase-truncation-based techniques, this scheme is immune to the information leakage and different types of attacks. Furthermore, the three different diffraction distances and the illuminating wavelength also function as four additional keys to significantly reinforce the security. Simulation results demonstrate the feasibility and validity of the proposal.

Recently, optical techniques[1–11] in image encryption have been intensely studied, owing to their inherent superiority with respect to multiple parameters and parallel processing. The pioneering work of optical image encryption is on double-random phase encoding (DRPE)[12], which is done on the Fourier transform domain. Several works that followed have reported the expansion of initial DRPE work into different transform domains[13–17], comprising the domains such as fractional Fourier transform (FrFT), Fresnel transform (FrT), and fractional random transform. During the period, other optical encryption works[18–30] that employ compressive sensing, optical interference, iterative phase retrieval, digital holography, photon counting, and polarized light, have also emerged to improve the image security in succession.

However, owing to intrinsic linearity, DRPE-based structures cannot withstand several types of attacks[31–34]. Various nonlinear encryption methods have been proposed to overcome these weaknesses, and the best illustrative work is on phase-truncated Fourier transform by Qin and Peng[35]. Subsequently, there are several works based on phase truncation (PT) in FrT and FrFT domains[36–39]. Wang et al.[40] showed that there is an information leakage in the work[35] if one of two private keys are utilized, and hence, proposed a solution. They also pointed out the works[36–39] being susceptible to information-leakage issue. Chen et al.[41] developed a multi-image encryption scheme through feature fusion, compressed sensing, and PT. Yi and Tan[42] presented a binary-tree multiple image encryption scheme. Su et al.[43] proposed an optical encryption strategy for multiple color images through a complete trinary tree structure. Besides, the specific attack (SA)[44], which employs an amplitude-phase-retrieval method, indicates that it can break the traditional PT-based technique[35]. Unfortunately, these techniques[41–43] cannot be also an alternative to SA[44]. Additionally, the work[45] has utilized the coherent superposition and equal modulus decomposition (EMD) to fully address the silhouette problem. However, there is the same modulus (i.e. same amplitude information) of two masks in EMD. The complex-valued masks cannot directly display in optical system. Chen et al.[46] presented an optical image cryptosystem via two-beam coherent superposition and unequal amplitude decomposition for security improvement. However, unequal amplitude decomposition requires an additional random phase distribution than EMD. Thus, constantly improving the security of encryption scheme based on PT, despite the progress in the field, is still inevitable.

This study presents a double-image crosstalk free encryption scheme. The scheme, which works by utilizing the equal modulus decomposition and random masks, generates a single ciphertext mask and two private key masks. The random masks have been introduced to bring the indirect mathematical relation between the plaintext pair and the ciphertext, where an illegal user has insufficient constraints utilized for SA. Compared with

[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. ✉email: luanguangyu@126.com

certain PT-based works[35–39], the proposal eliminates information leakage. When compared with other existing PT-based work[41–43], the proposal is still effective against SA. The additional keys, which comprise the three different diffraction distances and the illuminating wavelength, can strengthen the security. Simulation results and performance analysis demonstrate the reliability and validity of the proposal.

Principle of the method

The diagram of the proposed double-image cryptosystem is depicted as Fig. 1. The random amplitude mask (RAM) and a random phase mask (RPM) have been described with respect to the encryption (Fig. 1a) and decryption (Fig. 1b). The encryption keys have been generated from the random masks RAM and RPM by applying EMD in the Fresnel domain. Figure 2 shows the optical relationship between RAM, S_1, and S_2. In this setup, a collimated plane wave with the wavelength λ, perpendicularly illuminates RAM and the image which is

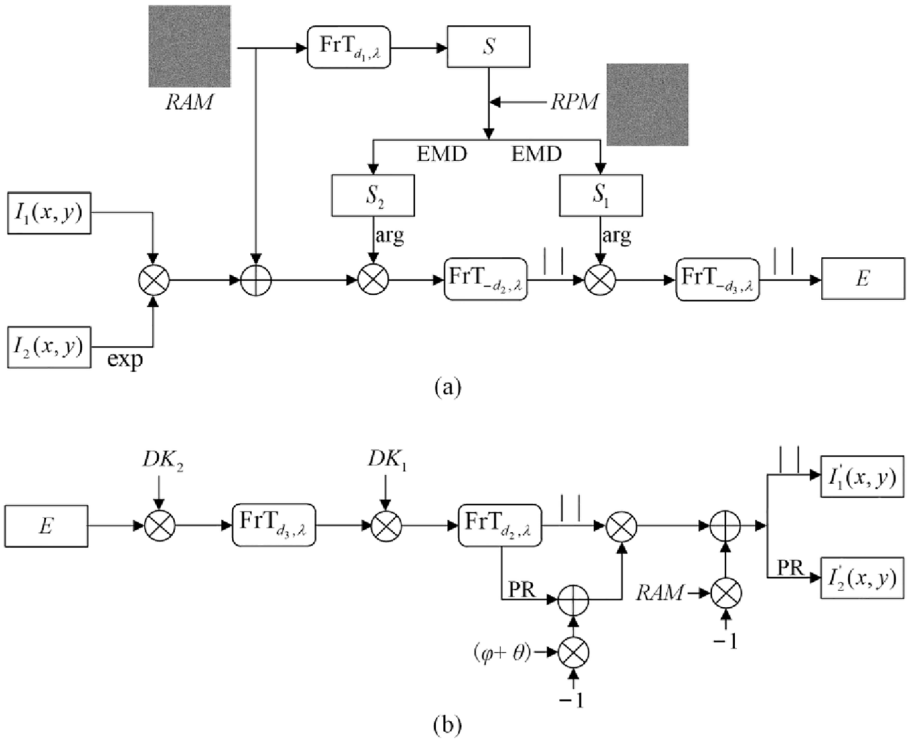

Figure 1. Schematic diagram for the proposed (**a**) encryption and (**b**) decryption.

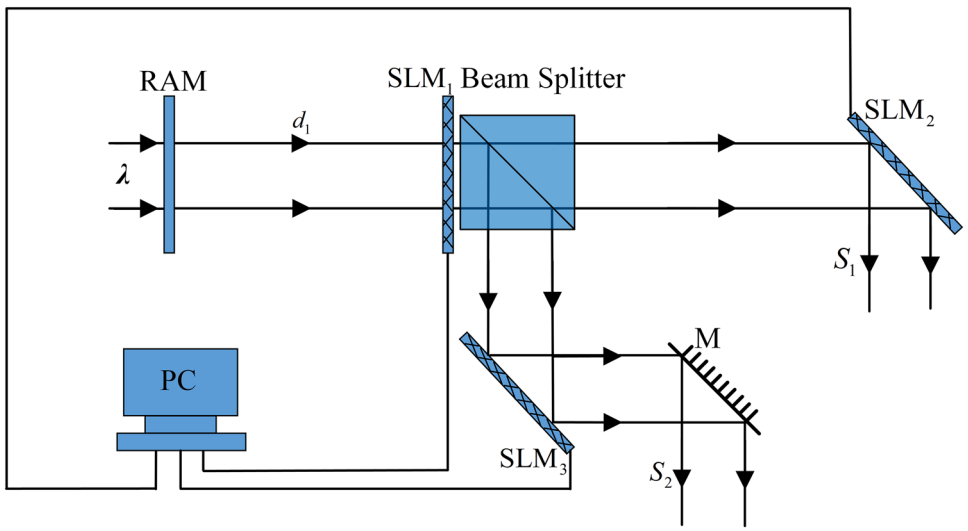

Figure 2. Optical relationship between RAM and S_1, S_2. M reflective mirrors.

subsequently Fresnel transformed with the diffraction distance d_1. The first spatial light modulator (SLM_1) were employed for amplitude modulation. SLM_2 and SLM_3 were utilized for phase modulation.

In the proposed double-image encryption process, $R_1(x, y)$ and $R_2(u, v)$ are the random functions, whose values fall in the interval [0, 1]. The following encryption steps have been depicted.

First, the RAM denoted as $R_1(x, y)$ was Fresnel transformed given by Eq. (1).

$$S{=}FrT_{(d_1,\lambda)}[RAM] = FrT_{(d_1,\lambda)}\left[R_1(x,y)\right] \tag{1}$$

where $FrT_{(d_1,\lambda)}[\cdot]$ is the FrT operator, and d_1 and λ are the diffraction distance and the wavelength, respectively. The amplitude part and the phase part of S are represented as $A{=}|S|$ and $\varphi = \arg[S]$, respectively, and "$|\cdot|$" and "arg $[\cdot]$" are the modulus and argument operators, respectively.

Subsequently, the complex-valued function S was separated into two masks, viz, S_1 and S_2, with equal moduli, as illustrated in Fig. 3. Owing to the random phase distribution RPM (denoted as, $\theta(u, v)$) introduced, and the geometrical relationship, S_1 and S_2 can be deduced as

$$\theta{=}RPM = 2\pi R_2(u, v) \tag{2}$$

$$S_1{=}\frac{A/2}{\cos(\theta)}\exp[i(\varphi-\theta)] \tag{3}$$

$$S_2{=}\frac{A/2}{\cos(\theta)}\exp[i(\varphi+\theta)] \tag{4}$$

The phase parts of S_1 and S_2 serve as the encryption keys.

Next, a new complex-value function $f(x, y)$ was constructed by the two original images, viz., ($I_1(x, y)$ and $I_2(x, y)$), and RAM, as follows

$$f(x,y){=}k_1 I_1(x,y)\exp[ik_2 I_2(x,y)] + k_3 RAM(x,y) \tag{5}$$

where $k_i (i = 1, 2, 3)$ are the constants.

Then, by employing the encryption keys obtained in the above-mentioned step, the function $f(x, y)$ was encrypted based on PT in the Fresnel domain. Thus, the ciphertext E can be expressed as

$$E{=}\left|\mathrm{FrT}_{(-d_3,\lambda)}\left[\left|\mathrm{FrT}_{(-d_2,\lambda)}\left[f(x,y)\exp[i(\varphi+\theta)]\right]\right|\exp[i(\varphi-\theta)]\right]\right| \tag{6}$$

where d_2 and d_3 are the diffraction distances. Meanwhile, two decryption keys, viz., DK_1 and DK_2, generated are given by

$$DK_1 = \mathrm{conj}\left\{\exp[i(\varphi-\theta)]\right\}PR\left[\mathrm{FrT}_{(-d_2,\lambda)}\left[f(x,y)\exp[i(\varphi+\theta)]\right]\right] \tag{7}$$

$$DK_2{=}PR\left[\mathrm{FrT}_{(-d_3,\lambda)}\left[\left|\mathrm{FrT}_{(-d_2,\lambda)}\left[f(x,y)\exp[i(\varphi+\theta)]\right]\right|\exp[i(\varphi-\theta)]\right]\right] \tag{8}$$

where "conj{·}" is the complex conjugate operator, $PR[\cdot]$ the phase reservation operator.

For the decryption, the retrieved function $f\prime(x, y)$ by the authorized users can be derived as,

$$f\prime(x,y){=}\left|\mathrm{FrT}_{(d_2,\lambda)}\left[\mathrm{FrT}_{(d_3,\lambda)}[DK_2E]DK_1\right]\right|\exp\left[i\left[PR\left[\mathrm{FrT}_{(d_2,\lambda)}\left[\mathrm{FrT}_{(d_3,\lambda)}[DK_2E]DK_1\right]\right]-(\varphi+\theta)\right]\right] \tag{9}$$

After obtaining the $f\prime(x, y)$, two retrieved images, $I_1\prime(x, y)$ and $I_2\prime(x, y)$, are mathematically represented as,

$$I_1\prime(x,y){=}\frac{1}{k_1}\left|f\prime(x,y) - k_3 RAM(x,y)\right| \tag{10}$$

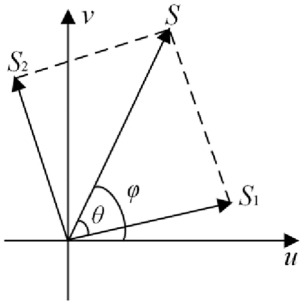

Figure 3. Principle of EMD.

$$I_2{}'(x,y)=\frac{1}{k_2}PR\left[f'(x,y)-k_3RAM(x,y)\right] \tag{11}$$

Figure 4 illustrates the optical schematic apparatus for decryption. A light beam carrying the information of ciphertext E was modulated by SLM_1. SLM_1 and SLM_2 are being employed for phase modulation. CCD captures the intensity part of $f'(x,y)$. The phase part of $f'(x,y)$ is digitally acquired. Then two decrypted images, viz.,$I_1{}'(x,y)$ and $I_2{}'(x,y)$, are digitally acquired with the function $f'(x,y)$.

Numerical results and performance analysis

To demonstrate the validity and the advantages of the proposal, numerical simulations have been implemented. In those simulations, the illumination wavelength λ is 633 nm, and the three axial distances, viz., d_1, d_2, and d_3, are 60, 50, and 70 mm, respectively, and the parameters k_1, k_2, and k_3 are set as 0.6, 0.5, and 1.5, respectively. Furthermore, the correlation coefficient (CC) was utilized to objectively assess the similarity between the plaintext $I_k(x,y)$ $(k=1, 2)$ and its corresponding decrypted image $I_k{}'(x,y)$ as

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

For convenience of the analysis, the CC values were directly labelled in the recovered images.

Figure 5a, b show two original images having 512×512 pixels, which are employed as the two plaintexts. The two random masks, RAM and RPM, are shown in Fig. 5c, d. By employing RAM, RPM, and EMD, the encryption keys (Fig. 5e, f) are acquired. The ciphertext and decrypted keys, after conducting the proposed encryption process, are displayed in Fig. 5g–i, respectively. Finally, the decrypted images acquired by using all the correct keys are shown in Fig. 5j, k. These results signify that each decrypted image and its corresponding plaintext are completely equal, or the influence of crosstalk noise is non-existent. Thus, the proposal is feasible and effective, and can retrieve the high-quality images without the crosstalk noise.

To evaluate the information-leakage-free of the proposal, Fig. 6a–f show the decrypted images with releasing of E, DK_1, and DK_2. Figure 7a–f illustrate the decrypted images when two of these masks are utilized. According to Figs. 6 and 7, each of all the decrypted images has the noise-like distribution, where no useful information of the two plaintexts appears. We illustrated that the information-leakage issue has been thoroughly settled in the proposal.

We have further validated the sensitivity of the proposal for the additional keys, i.e., the three diffraction distances d_1, d_2, and d_3, and the illuminating wavelength λ. Figures 8, 9, 10 and 11 illustrate the sensitive results of those keys, where the deviation ranges of those keys are [− 50 50]. These results invariably reveal that the CC values are one, only when the deviation is equal to zero. And for other values of the deviation, the CC values are below or equal to 0.0863. Moreover, when the deviations are − 1 and 1, all the decrypted images have no useful content of the two plaintexts. Therefore, the proposal has four sensitive additional keys, which can further reinforce the security of the proposal.

To further demonstrate the robustness of the proposal against noise and occlusion attacks, Fig. 12 illustrates the decrypted results when the ciphertext is contaminated by the zero-mean white additive Gaussian noise with $\sigma = 0.2$ and $\sigma = 0.3$. Figure 13 represents the decrypted results acquired from the ciphertexts with 3% and 5% occlusion. According to Figs. 12 and 13, the quality of the decrypted images steadily worsens with the increase of the noise or occlusion strength. Although the content of those images becomes blurred for $\sigma = 0.3$ noise or 5% occlusion, the main-structure information can be still distinguished. Hence, it is verified for these results that the proposal has the resistance to noise and occlusion attacks.

Furthermore, we have proved the validity of the proposal against known-plaintext attack (KPA). The decryption keys of our scheme varies with the different plaintext pair. In the KPA simulation, Fig. 5a, b, g serve as a known plaintext pair and their corresponding ciphertext. Using the proposal, RAM (Fig. 5c) and RPM (Fig. 5d) encrypt the plaintext pair in Fig. 5a, b, and the private keys in Fig. 5h, i are generated. Figure 14a, b demonstrate the other plaintext pair. Figure 14c illustrates the ciphertext of Fig. 14a, b, which were produced by the proposal,

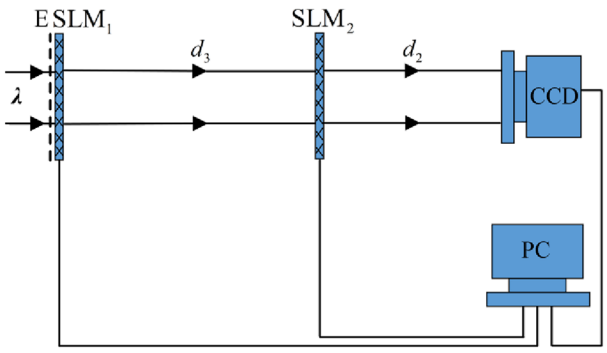

Figure 4. Optical schematic system for decryption.

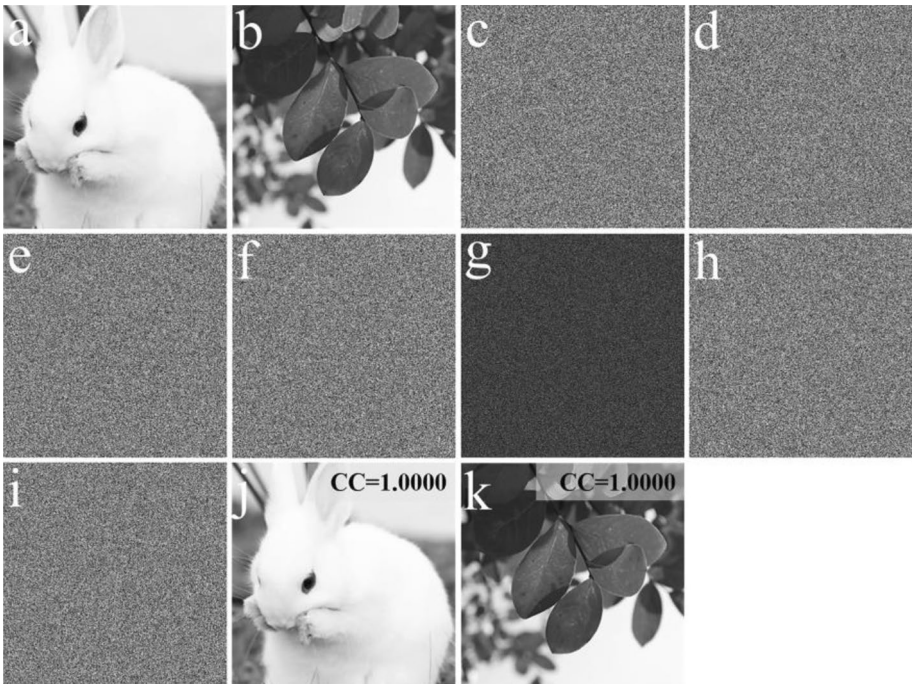

Figure 5. (**a**, **b**) The two plaintexts, (**c**) RAM, (**d**) RPM, (**e**, **f**) the two encryption keys, (**g**) the ciphertext *E*, (**h**) DK_1, (**i**) DK_2, (**j**, **k**) the two decrypted images.

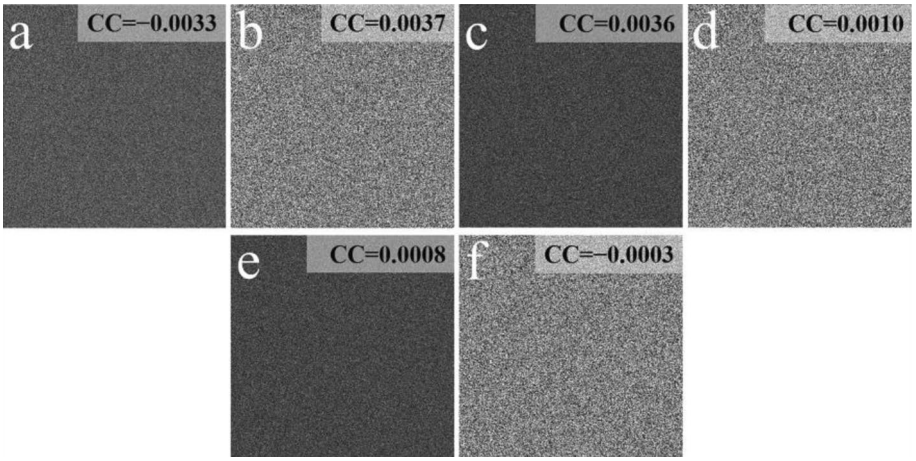

Figure 6. Decrypted images with (**a**, **b**) *E*, (**c**, **d**) DK_1, and (**e**, **f**) DK_2.

RAM′ and RPM′. RAM and RPM are different from RAM′ and RPM′, respectively. When all the correct parameters, viz., RAM (Fig. 5c), RPM (Fig. 5d), and the private keys (Fig. 5h, i) are used, the two retrieved results of Fig. 14c are shown in Fig. 14d, e. For better explaining the security of this scheme, we have retrieved Fig. 14c in the other two cases in which we suppose that the attacker has known one out of RAM′ and RPM′. Figure 14f, g demonstrate the results of Fig. 14c with RPM′, $DK_1^{\mathrm{RPM}'}$, $DK_2^{\mathrm{RPM}'}$, and for the other abovementioned conditions. Figure 14h, i illustrate the results of Fig. 14c using RAM′, $DK_1^{\mathrm{RAM}'}$, $DK_2^{\mathrm{RAM}'}$, and the other conditions mentioned above. The information of Fig. 14a, b cannot be deciphered from Fig. 14d–i. Hence, the proposal is immune to KPA.

Finally, we have also demonstrated that the proposal can resist SA[44]. SA is a single iteration process, which stem from the modified amplitude-phase retrieval algorithm. The results of SA with two unknown masks, viz., RAM and RPM, are illustrated in Fig. 15a–c. Moreover, the results of SA, when the knowledge of one of RAM and RPM is lacking, are illustrated in Fig. 15d–i. Figure 16 shows the results of SA using Qin and Peng's scheme[35]. It is shown in Fig. 15a, d, g, that the six curves are unstable and non-convergent. According to Fig. 15b, c, e, f, h, i, no information can be deciphered of the two plaintexts (Fig. 15a, b). Therefore, we have shown that the proposal can effectively resist SA.

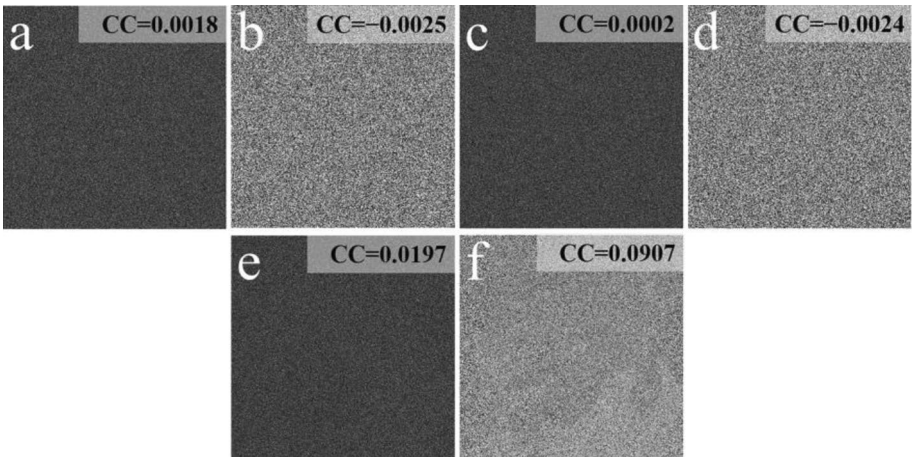

Figure 7. Decrypted images with (**a**, **b**) E and DK_1, (**c**, **d**) E and DK_2, and (**e**, **f**) DK_1 and DK_2.

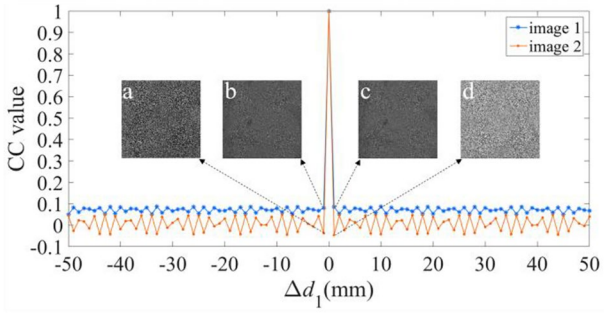

Figure 8. Relation curves of the CC value versus Δd_1, where the decrypted images using Δd_1 of (**a**, **b**) − 1, and (**c**, **d**) 1.

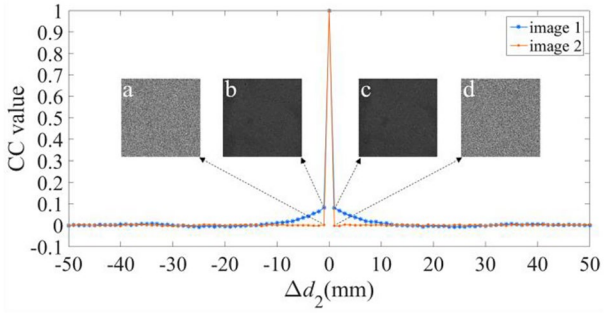

Figure 9. Relation curves of the CC value versus Δd_2, where the decrypted images using Δd_2 of (**a**, **b**) − 1, and (**c**, **d**) 1.

Concluding remarks

An optical phase-truncation-based double-image encryption was developed using the equal modulus decomposition and random masks. The proposal utilizes RAM and RPM to generate a single ciphertext and two private keys. This scheme is novel, and acquires the decrypted images immune to the crosstalk noise. Particularly, the random masks cause insufficient constraints to be utilized for SA. Our proposal, when compared with the reported techniques via PT, has no problem of information leakage, and can efficiently resist different types of attacks. Furthermore, the four parameters serve as additional keys for enhancing the security. Numerical simulation results validate the advantages of the proposal.

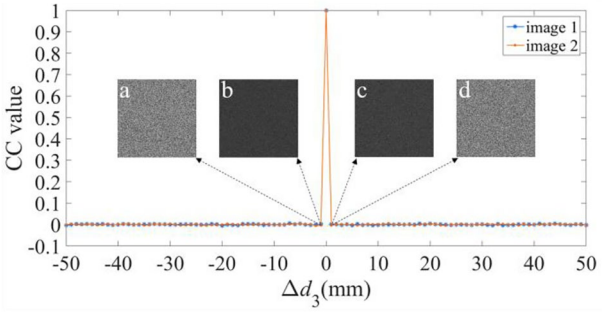

Figure 10. Relation curves of the CC value versus Δd_3, in which decrypted images using Δd_3 of (**a**, **b**) − 1, and (**c**, **d**) 1.

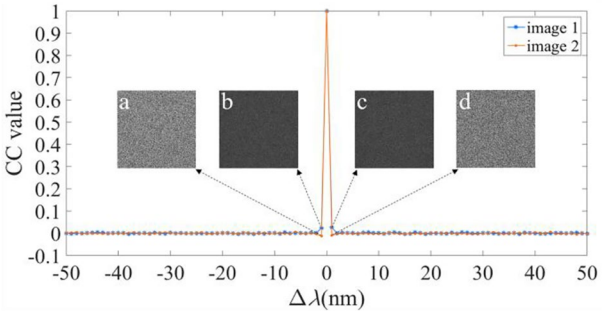

Figure 11. Relation curves of the CC value versus $\Delta\lambda$, in which decrypted images using $\Delta\lambda$ of (**a**, **b**) − 1, and (**c**, **d**) 1.

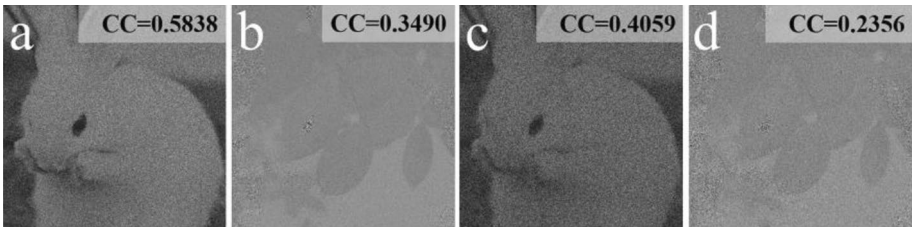

Figure 12. Decrypted images with Gaussian noise with (**a**, **b**) $\sigma = 0.2$, (**c**, **d**) $\sigma = 0.3$.

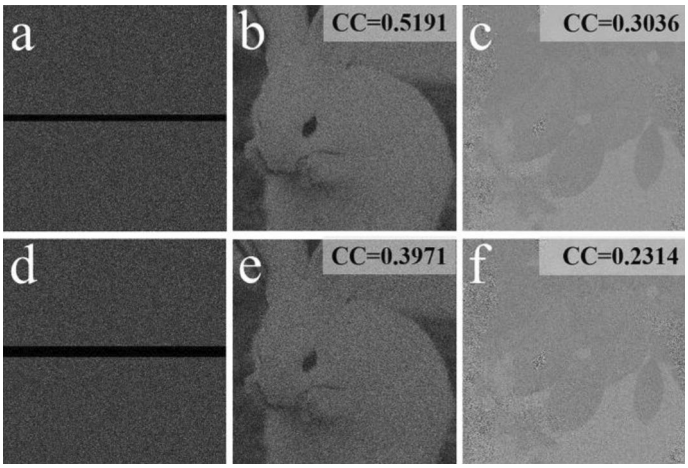

Figure 13. (**a**) Ciphertext with 3% occlusion, (**b**, **c**) decrypted images of (**a**, **d**) ciphertext with 5% occlusion, (**e**, **f**) decrypted images of (**d**).

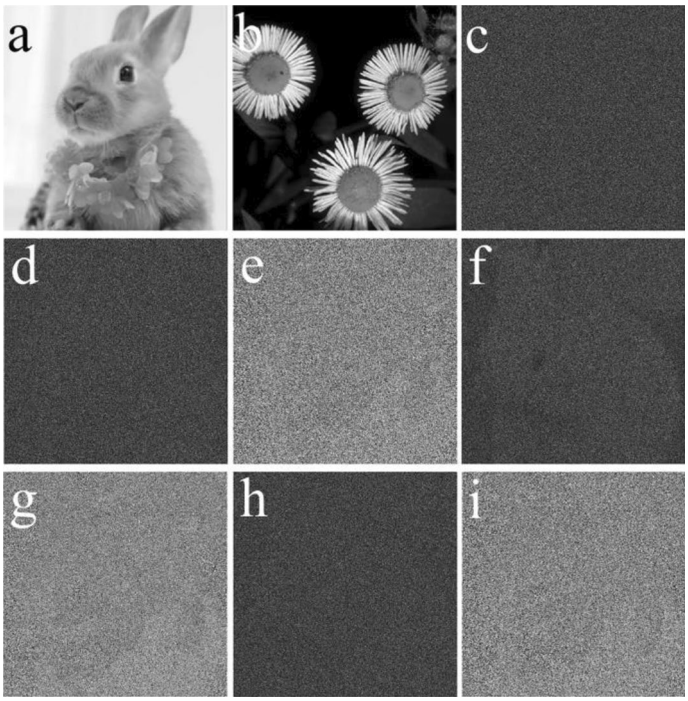

Figure 14. (**a**, **b**) the other plaintext pair, (**c**) ciphertext of (**a**, **b**) with RPM' and RAM', retrieved images of (**c**) using (**d**, **e**) RAM, RPM, DK_1, DK_2, (**f**, **g**) RAM, RPM', $DK_1^{RPM'}$, $DK_2^{RPM'}$, and (**h**, **i**) RAM', RPM, $DK_1^{RAM'}$, $DK_2^{RAM'}$.

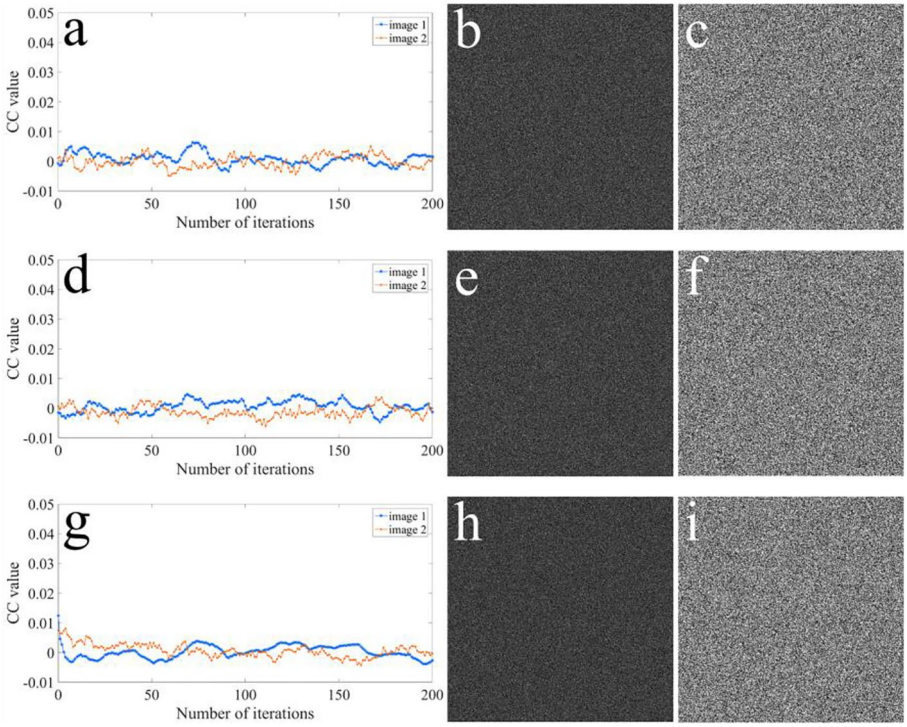

Figure 15. Results of SA using our proposal: the CC value versus number of iterations with (**a**) two unknown masks (RAM and RPM), (**d**) unknown RPM, and (**g**) unknown RAM, respectively; the recovered images after 200 iterations with (**b**, **c**) two unknown masks (RAM and RPM), (**e**, **f**) unknown RPM, and (**h**, **i**) unknown RAM, respectviely.

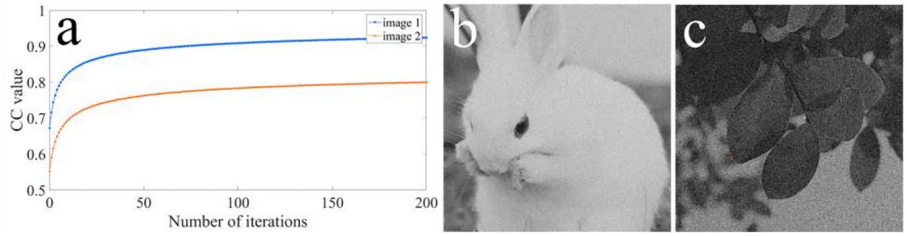

Figure 16. Results of SA using Qin and Peng's scheme: (**a**) the CC value versus number of iterations, and (**b**, **c**) recovered images after 200 iterations.

Data availability

Data are available from the corresponding author upon reasonable request.

Received: 23 January 2024; Accepted: 21 March 2024
Published online: 26 March 2024

References

1. Alfalou, A. & Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photonics* **1**(3), 589–636 (2009).
2. Chen, W., Javidi, B. & Chen, X. D. Advances in optical security systems. *Adv. Opt. Photonics* **6**(2), 120–155 (2014).
3. Javidi, B. *et al.* Roadmap on optical security. *J. Opt.* **18**(8), 083001 (2016).
4. Shikder, A. & Nishchal, N. K. Image encryption using binary polarization states of light beam. *Sci. Rep.* **13**, 14028 (2023).
5. Abuturab, M. R. Multiple color image cryptosystem based on coupled-logistic-map-biometric keys, QR decomposition with column pivoting and optical Fresnel transform. *Opt. Laser Technol.* **161**, 109109 (2023).
6. Wang, X. G., Chen, W. & Chen, X. D. Optical encryption and authentication based on phase retrieval and sparsity constraints. *IEEE Photonics J.* **7**(2), 7800310 (2015).
7. Sui, L. S., Zhang, L. W., Wang, Q., Tian, A. L. & Anand, A. Multiple-image authentication based on the single-pixel correlated imaging and multiple-level wavelet transform. *Opt. Lasers Eng.* **130**, 106102 (2020).
8. Wei, H. Y. & Wang, X. G. Optical multiple-image authentication and encryption based on phase retrieval and interference with sparsity constraints. *Opt. Laser Technol.* **142**, 107257 (2021).

9. Sui, L. S., Zhao, X. Y., Huang, C. T., Tian, A. L. & Anand, A. An optical multiple-image authentication based on transport of intensity equation. *Opt. Lasers Eng.* **116**, 116–124 (2019).
10. Qin, Y., Jiang, H. L. & Gong, Q. Interference-based multiple-image encryption by phase-only mask multiplexing with high quality retrieved images. *Opt. Lasers Eng.* **62**, 95–102 (2014).
11. Luan, G. Y., Li, A. C., Zhang, D. M. & Wang, D. X. Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain. *IEEE Photonics J.* **11**(1), 6900207 (2019).
12. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995).
13. Li, Y. B., Zhang, F., Li, Y. C. & Tao, R. Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. *Opt. Lasers Eng.* **72**, 18–25 (2015).
14. Sui, L. S., Duan, K. K., Liang, J. L. & Hei, X. H. Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. *Opt. Express* **22**(9), 10605–10621 (2014).
15. Chen, J. X. *et al.* A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains. *Opt. Express* **22**(6), 7349–7361 (2014).
16. Wang, X. G., Chen, W. & Chen, X. D. Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. *Opt. Express* **22**(19), 22981–22995 (2014).
17. Xu, H. F., Xu, W. H., Wang, S. H. & Wu, S. F. Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain. *Opt. Commun.* **402**, 302–310 (2017).
18. Zhang, Y. & Wang, B. Optical image encryption based on interference. *Opt. Lett.* **33**(21), 2443–2445 (2008).
19. Perez-Cabre, E., Cho, M. J. & Javidi, B. Information authentication using photon-counting double-random-phase encrypted images. *Opt. Lett.* **36**(1), 22–24 (2011).
20. Maluenda, D., Carnicer, A., Martinez-Herrero, R., Juvells, I. & Javidi, B. Optical encryption using photon-counting polarimetric imaging. *Opt. Express* **23**(2), 655–666 (2015).
21. Chen, L. F., Chang, G. J., He, B. Y., Mao, H. D. & Zhao, D. M. Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition. *Opt. Lasers Eng.* **88**, 221–232 (2017).
22. Li, X. W., Xiao, D. & Wang, Q. H. Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. *Opt. Lasers Eng.* **100**, 200–207 (2018).
23. Carnicer, A., Hassanfiroozi, A., Latorre-Carmona, P., Huang, Y. P. & Javidi, B. Security authentication using phase-encoded nanoparticle structures and polarized light. *Opt. Lett.* **40**(2), 135–138 (2015).
24. Rawat, N., Hwang, I. C., Shi, Y. & Lee, B. G. Optical image encryption via photon-counting imaging and compressive sensing based ptychography. *J. Opt.* **17**(6), 065704 (2015).
25. Fatima, A. & Nishchal, N. K. Optical image security using Stokes polarimetry of spatially variant polarized beam. *Opt. Commun.* **417**, 30–36 (2018).
26. Wang, Y., Quan, C. & Tay, C. J. Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm. *Opt. Lasers Eng.* **78**, 8–16 (2016).
27. Moon, I., Yi, F., Han, M. & Lee, J. Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms. *Appl. Opt.* **55**(16), 4328–4335 (2016).
28. Chen, Y., Liu, Q., Wang, J. & Wang, Q. H. Single-channel optical encryption of color image using chessboard grating and diffraction imaging scheme. *Opt. Eng.* **56**(12), 123106 (2017).
29. Su, Y. G. *et al.* Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. *Opt. Lasers Eng.* **88**, 20–27 (2017).
30. Qin, Y., Wang, Z. P., Wang, H. J., Gong, Q. & Zhou, N. R. 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. Gopinathan, U., Monaghan, D. S., Naughton, T. J. & Sheridan, J. T. A known-plaintext heuristic attack on the Fourier plane encryption algorithm. *Opt. Express* **14**(8), 3181–3186 (2006).
32. Peng, X., Zhang, P., Wei, H. Z. & Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **31**(8), 1044–1046 (2006).
33. Tashima, H. *et al.* Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack. *Opt. Express* **18**(13), 13772–13781 (2010).
34. Zhang, Y. S., Xiao, D., Wen, W. Y. & Liu, H. Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding. *Opt. Lett.* **38**(21), 4506–4509 (2013).
35. Qin, W. & Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **35**(2), 118–120 (2010).
36. Chen, W. & Chen, X. D. Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. *Opt. Commun.* **284**(16–17), 3913–3917 (2011).
37. Rajput, S. K. & Nishchal, N. K. Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask. *Appl. Opt.* **51**(22), 5377–5386 (2012).
38. Rajput, S. K. & Nishchal, N. K. Image encryption based on interference that uses fractional Fourier domain asymmetric keys. *Appl. Opt.* **51**(10), 1446–1452 (2012).
39. Mehra, I., Rajput, S. K. & Nishchal, N. K. Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification. *Opt. Eng.* **52**(2), 028202 (2013).
40. Wang, X. G., Zhao, D. M. & Chen, Y. X. Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask. *Appl. Opt.* **53**(23), 5100–5108 (2014).
41. Chen, X. D., Liu, Q., Wang, J. & Wang, Q. H. Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction. *Opt. Laser Technol.* **107**, 302–312 (2018).
42. Yi, J. W. & Tan, G. Z. Binary-tree encryption strategy for optical multiple-image encryption. *Appl. Opt.* **55**(20), 5280–5291 (2016).
43. Su, Y. G. *et al.* Optical encryption scheme for multiple color images using complete trinary tree structure. *Opt. Lasers Eng.* **98**, 46–55 (2017).
44. Wang, X. G., Chen, Y. X., Dai, C. Q. & Zhao, D. M. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform. *Appl. Opt.* **53**(2), 208–213 (2014).
45. Cai, J., Shen, X., Lei, M., Lin, C. & Dou, S. Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition. *Opt. Lett.* **40**(4), 475–478 (2015).
46. Chen, L. F. *et al.* A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition. *Opt. Laser Technol.* **78**, 167–174 (2016).

Acknowledgements

This study is supported by Science and Technology Planning Project of Daqing City of China (zd-2023-60), China Scholarship Council (202208230113), Basic Cultivation Project of Heilongjiang Bayi Agricultural University (ZRCPY202315), and Education Department Foundation of Heilongjiang Province of China (12541584).

Author contributions

G.L. conceived idea, performed programming and numerical analysis, and wrote manuscript. C.Q. reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to G.L.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.