Optical Review (2020) 27:1–8
https://doi.org/10.1007/s10043-019-00552-0

REGULAR PAPER

Asymmetric multiple-image interference cryptosystem using discrete cosine transform and conditional decomposition

Guanghui Ren[1] · Jianan Han[1] · Jiahui Fu[1] · Mingguang Shan[2]

Received: 13 August 2018 / Accepted: 27 September 2019 / Published online: 11 November 2019

Abstract
In this study, we propose an asymmetric multiple-image encryption technique based on optical interference that utilizes the discrete cosine transform (DCT) and conditional decomposition. First, the DCT spectrum of each original image is cropped by a low-pass filter and spatially multiplexed into a synthetized spectral signal with the same size as the original image. The synthetized spectral signal is then transformed by the DCT to the spatial domain. After undergoing pixel-scrambling, the synthetized signal is encrypted into three phase-only masks (POMs) based on the interference in the discrete multiple-parameter fractional Fourier transform domain and conditional decomposition. One of the POMs is a plaintext-independent cyphertext and the other two are plaintext-dependent private keys. The silhouette of the original image cannot be identified using only one or two of the POMs, all POMs are required. Finally, we demonstrate the performance of our technique through simulations.

Keywords Optical interference · Multiple-image encryption · Conditional decomposition

1 Introduction

Owing to the high speed of 2D processing, parallelism, and high degree of freedom across multiple parameters, optical information processing techniques have been widely employed in image encryption. Since double-random phase encoding (DRPE) in the Fourier domain using two random-phase masks (RPMs) was first proposed by Refregier and Javidi [1], it has been extended to the fractional Fourier domain [2], Fresnel domain [3], multiple-parameter fractional Fourier (MPFrF) domain [4], gyrator domain [5] and others [6–8]. However, these DRPE-based cryptosystems are linear and symmetric, resulting in a low endurance to some attacks. Phase-truncated Fourier transforms (PTFTs) [9] were suggested to remove the linearity and symmetry of DRPE. However, the initial PTFTs have no resistance to a specific attack. Various attack-free PTFTs [9–13] were proposed to enhance the security, but these resulted in complexity in the cryptosystems. A simple asymmetric cryptosystem that utilizes the interference to encrypt a plain image into two phase-only masks (POMs) was first suggested by Zhang et al. [14], but this approach suffered from the silhouette problem. Various improved schemes have been suggested to eliminate the silhouette problem. For example, Zhong et al. [15] suggested encryption that utilizes three POMs in the MPFrF domain, and Lin et al. [16] suggested generating private keys using conditional decomposition. However, these schemes could only encrypt one image. To improve the efficiency and capacity, interference has also been studied with various schemes to simultaneously encrypt multiple images. Niu et al. [17] introduced wavelength multiplexing, but to encrypt only two images. Chen et al. [18] employed multiplane phase retrieval using iteration, and Qin et al. [19] applied position multiplexing and utilized POM multiplexing [20]. However, these schemes suffered from either heavy computational complexity or crosstalk. Recently, Zhang et al. [21] adopted a vector stochastic decomposition algorithm based on a cascaded interference structure. This scheme eliminated time-consuming iteration, but required a complex structure with multiple cascaded POMs, resulting in transmission and storage burdens.

✉ Guanghui Ren
rgh@hit.edu.cn

[1] School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, People's Republic of China

[2] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, People's Republic of China

To realize simple multiple-image encryption free from the silhouette problem, we propose an asymmetric cryptosystem based on optical interference that incorporates the discrete cosine transform (DCT) and the conditional decomposition. During the encryption process, the DCT is employed to multiplex multiple original images into one synthetized signal, and subsequently, interference combined with the conditional decomposition is used to encode the synthetized signal into three POMs. In contrast to Refs. [18–21], our approach can be directly employed in image encryption without crosstalk between the decrypted images and without requiring iteratively generated or cascaded POMs. As a result, our approach eliminates the silhouette problem without increasing the computational complexity, time-consumption, or storage and transmission burdens. Numerical simulation results demonstrate the efficiency and capacity of our approach.

2 Theoretical analysis of the encryption algorithm

As is well-known, the upper-left corner of the DCT spectral plane contains most of the information of the general images. Therefore, by retaining just the upper-left part, the original images can be compressed without reducing the visibility, to a certain extent [22, 23]. In addition, the retained spectral parts can be shifted in space and multiplexed into a new synthetized spectrum, which can be employed to realize multiple-image encryption.

The scheme of our encryption process is illustrated in Fig. 1. Suppose that $O_i(x, y)$ $(i=1, 2,\ldots, m)$ denotes the ith original image with $N\times N$ pixels, where m is the total number of original images. During encryption, the DCT is applied to O_i, and the upper-left part of each image with $N/c\times N/c$ pixels after cropping its spectrum with a retaining coefficient c, is retained. The result is

$$\mathrm{CF}_i(u,v)=\mathrm{SC}_c\left\{\mathrm{DCT}\left[O_i(x,y)\right]\right\} \tag{1}$$

where (x, y) denotes a 2D-matrix in the spatial domain and (u, v) denotes a 2D matrix in the spectral domain; SC_c [·] denotes the cropping process through low-pass (LP) filter, and $m=c^2$.

Each retained spectrum is then shifted in space and multiplexed into one synthetized signal [22] with $N\times N$ pixels, which can be written as

$$\mathrm{SF}(u,v)=\sum_{i=1}^{m}\mathrm{SM}\left[\mathrm{CF}_i(u,v)\right] \tag{2}$$

where SM [·] denotes the process of shifting and multiplexing.

The synthetized signal is transformed by the inverse discrete cosine transform (IDCT) to the image domain and then it undergoes pixel-scrambling (PS) by PS [·]. The result is

$$\mathrm{OM}\ (x,\ y)=\sqrt{\mathrm{PS}\{\mathrm{IDCT}[\mathrm{SF}\ (u,\ v)]\}} \tag{3}$$

It can be deduced that the multiplexed signal OM (x, y) is real-valued; however, it contains most of the information of the original images.

Optical interference and conditional decomposition are then employed to encode OM (x, y). During this process, OM (x, y) is bonded with an RPM of exp $[ip_1\ (x, y)]$ and regarded as the object function

$$I_1\ (x,\ y)=\mathrm{OM}\ (x,\ y)\exp\left[\mathrm{ip}_1\ (x,\ y)\right] \tag{4}$$

where $p_1\ (x, y)$ is uniformly distributed in $[0, 2\pi]$.

For the conditional decomposition, another RPM of exp $[ip_2\ (x, y)]$ is directly served as the cyphertext $C\ (u, v)$, and another new object function can be expressed as

$$\mathrm{FD}\ (u,\ v)=F_{(M_L,M_R)}^{(-\alpha_L,-\alpha_R)}\left(\mathbf{n}'_L,\mathbf{n}'_R\right)\left[I_1\ (x,\ y)\right]-C\ (u,\ v) \tag{5}$$

where $F_{(M_L,M_R)}^{(\alpha_L,\alpha_R)}[]$ represents the operation of discrete multiple-parameter fractional Fourier transform (DMPFrFT) [8, 15] with parameters of $(M_\mathrm{L}, M_\mathrm{R}; \alpha_\mathrm{L}, \alpha_\mathrm{R}; \mathbf{m}_\mathrm{L}, \mathbf{n}_{\mathrm{L};}\ \mathbf{m}_\mathrm{R}, \mathbf{n}_\mathrm{R})$, while $(\alpha_\mathrm{L}, \alpha_\mathrm{R})$ is the fractional order for any value not equal

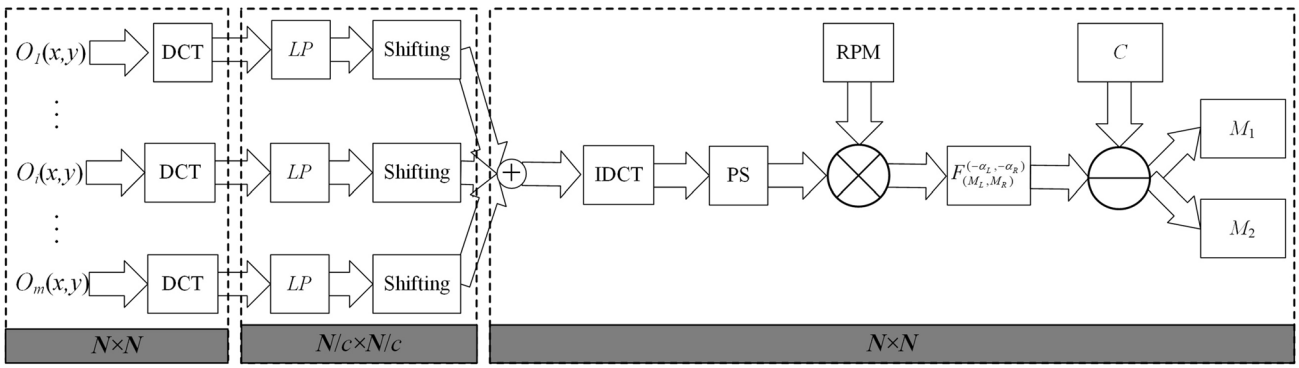

Fig. 1 Scheme of the encryption process

to 0 or ± 2; (M_L, M_R) is the periodicity; ($\mathbf{n}_L'$, $\mathbf{n}_R'$) is the vector parameter; and n' is defined as

$$\mathbf{n}' = \left(km_k + Mm_k n_k + n_k\right) \quad k = 0, 1, 2, \ldots, (M-1) \tag{6}$$

where $\mathbf{m} = (m_0,\ m_1,\ldots,\ m_{(M\text{-}1)}) \in \mathbb{Z}^M$; $\mathbf{n} = (n_0,\ n_1,\ldots,\ n_{(M\text{-}1)}) \in \mathbb{Z}^M$; and M is an arbitrary integer of > 2.

Following the principal of interference, two plaintext-dependent private keys can be obtained as

$$M_1\ (u,\ v) = \arg\left[\mathrm{FD}\ (u,\ v)\right] - \arccos\left\{\mathrm{abs}[\mathrm{FD}\ (u,\ v)]/2\right\} \tag{7}$$

$$M_2\ (u,\ v) = \arg\left\{\mathrm{FD}\ (u,\ v) - \exp\left[iM_1\ (u,\ v)\right]\right\} \tag{8}$$

where M_1 and M_2 are POMs generated analytically in [0, 2π]; arg[·] and abs[·] return the phase angle and modulus of the complex signal, respectively.

Our approach yields three POMs consisting of one plaintext-independent cyphertext and two plaintext-dependent private keys. No information from the original images is encoded into the cyphertext. Because the existing approaches for extracting keys or plaintext through cyphertext look for the mathematical relationship between the cyphertext and the plaintext or keys [16, 24], we believe that our approach can resist the current chosen-cyphertext, known-plaintext, and cyphertext-only attacks.

The scheme of our decryption process is illustrated in Fig. 2, which contains the steps for decrypting and demultiplexing. As shown in Fig. 2a, the decrypting step is straightforward and can be carried out through the superposition of diffraction fields from the three POMs. In this step, the first spatial light modulator (SLM1) is used to produce the summation of the three POMs. A second spatial light modulator (SLM2) and a lens are used to perform the DMPFrFT, in which the optical system is a typical fractional Fourier transformer (FRFT) of the order of 4/M [8, 15]. A parallel laser beam is modulated by SLM1 and then transformed by SLM2 and a lens. After being acquired by a charge-coupled device (CCD) camera, the result can be expressed as

$$|\mathrm{OM}\ (x,\ y)|^2 = \left| \begin{array}{l} F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(\mathbf{n}_L',\ \mathbf{n}_R')[C\ (u,\ v)] + F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(\mathbf{n}_L',\ \mathbf{n}_R')\left\{\exp\left[iM_1\ (u,\ v)\right]\right\} \\ + F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(\mathbf{n}_L',\ \mathbf{n}_R')\left\{\exp\left[iM_2(u,\ v)\right]\right\} \end{array} \right|^2 \tag{9}$$

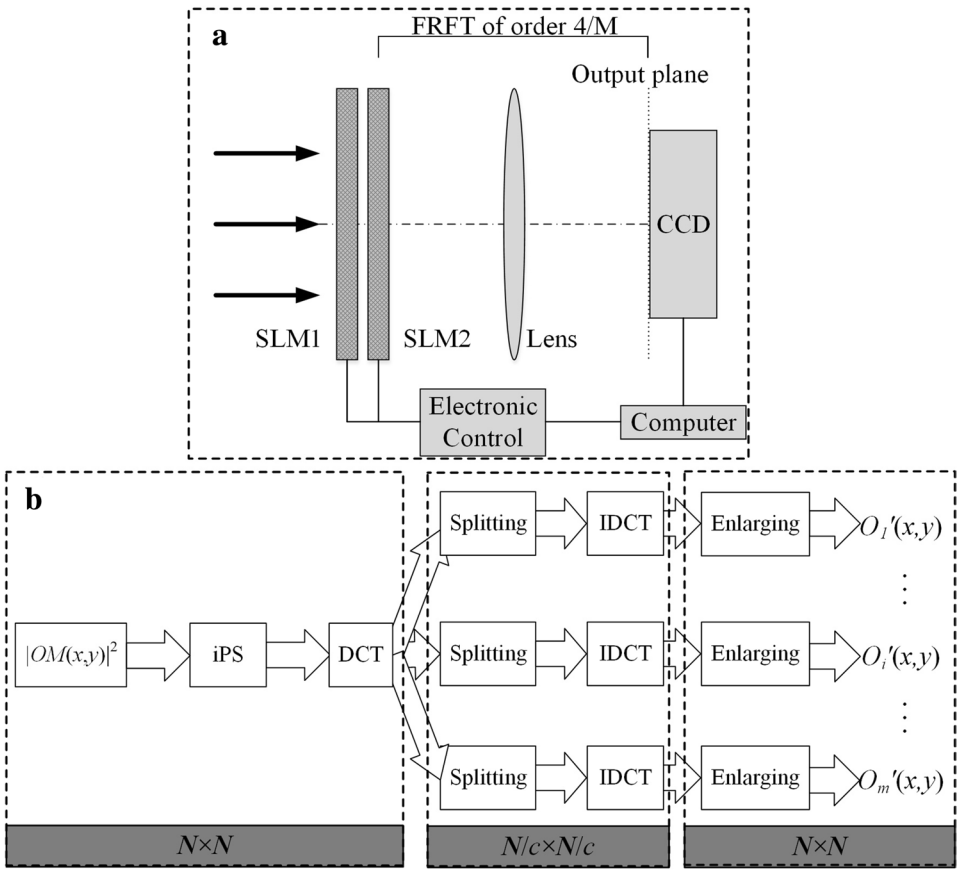

Fig. 2 Scheme of the decryption process. **a** Decrypting, and **b** demultiplexing

As shown in Fig. 2b, the demultiplexing step can be digitally executed on a computer. During this step, the synthetized spectrum SF (u, v) can be achieved in the spectral domain by applying the inverse pixel scrambling (IPS) and the DCT in sequence to OM (x, y). Each reduced image can be retrieved by taking the IDCT after correctly splitting and choosing its corresponding spectrum, and then enlarging it to yield the final decrypted image.

To quantify the performance of our approach, as many others did [16, 18-20, 25], the correlation coefficient (CC) is employed to evaluate the similarity between the original image and the decrypted image, which is defined as

$$CC = \frac{\sum\sum[O - E(O)]\left[O' - E\left(O'\right)\right]}{\sqrt{\left\{\sum\sum[O - E(O)]^2\right\}\left\{\sum\sum[O' - E(O')]^2\right\}}}, \tag{10}$$

where E is used to obtain the mean value of the input.

3 Results and analysis

To demonstrate the validity of the proposed asymmetric cryptosystem, various numerical experiments were conducted. First, we chose four original images with 256×256 pixels as shown in Fig. 3a–d. Their DCT spectra, as illustrated in Fig. 3e–h, were cropped but with the upper-left part retained as depicted by the white squares. The retained spectra were then multiplexed into a synthetized spectrum with the same size as the original image, as shown in Fig. 3i. The synthetized spectrum was transformed by the IDCT back to the spatial domain to yield a synthetized image as shown in Fig. 3j. The PS operation was then applied to the synthetized image, breaking it up into 65,536 subsections of 2×2 pixels, in which the gray value of the pixel of point (x, y) was interchanged with that of point (x', y') [26]. The PS application is shown in Fig. 3k. The synthetized image was then bonded with an RPM using Eq. 4.

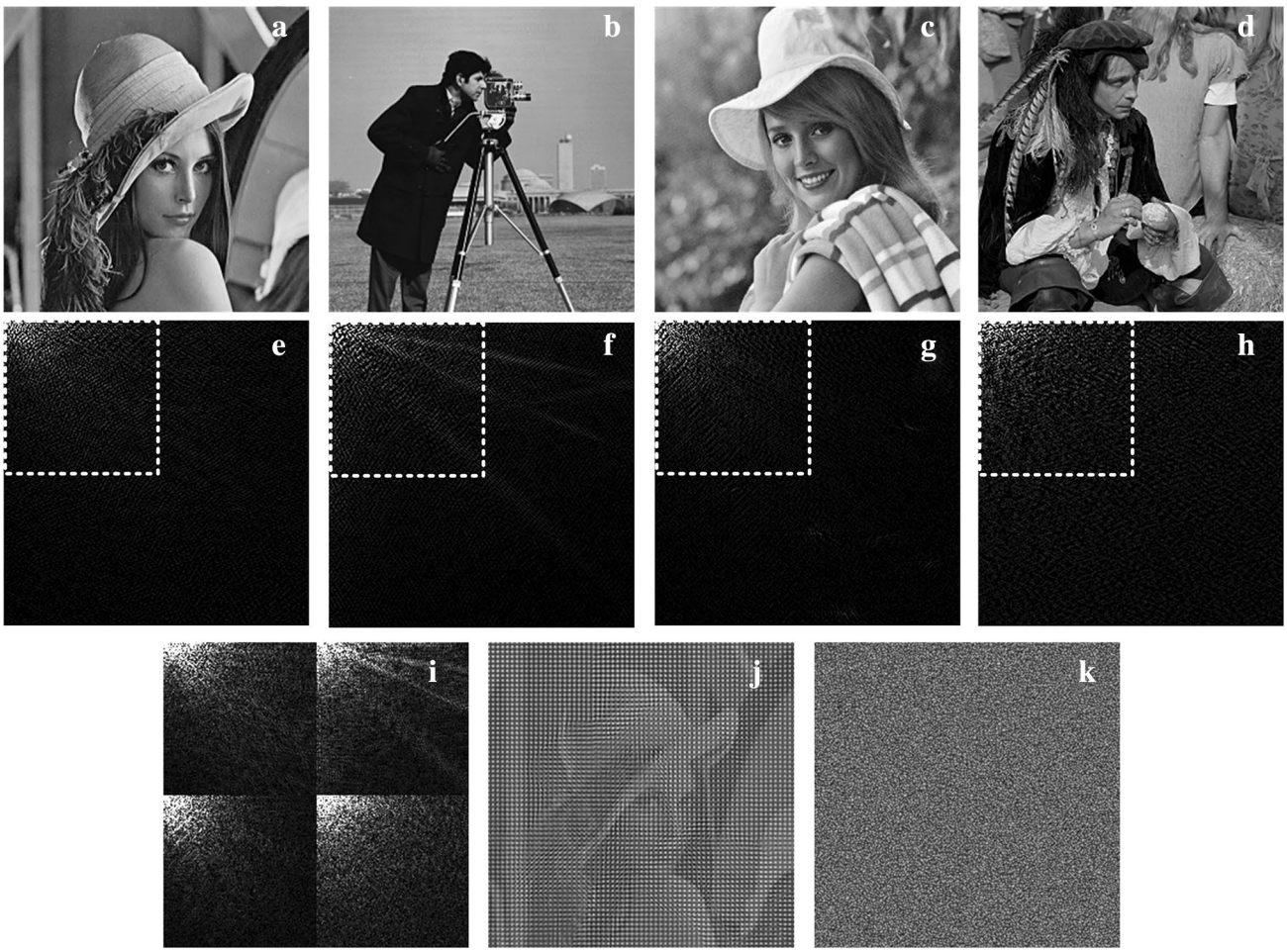

Fig. 3 **a–d** Four original images; **e–h** DCT spectra corresponding to (**a–d**); **i** synthetized spectrum; **j** synthetized image by IDCT on (**i**); and **k** PS-synthetized image

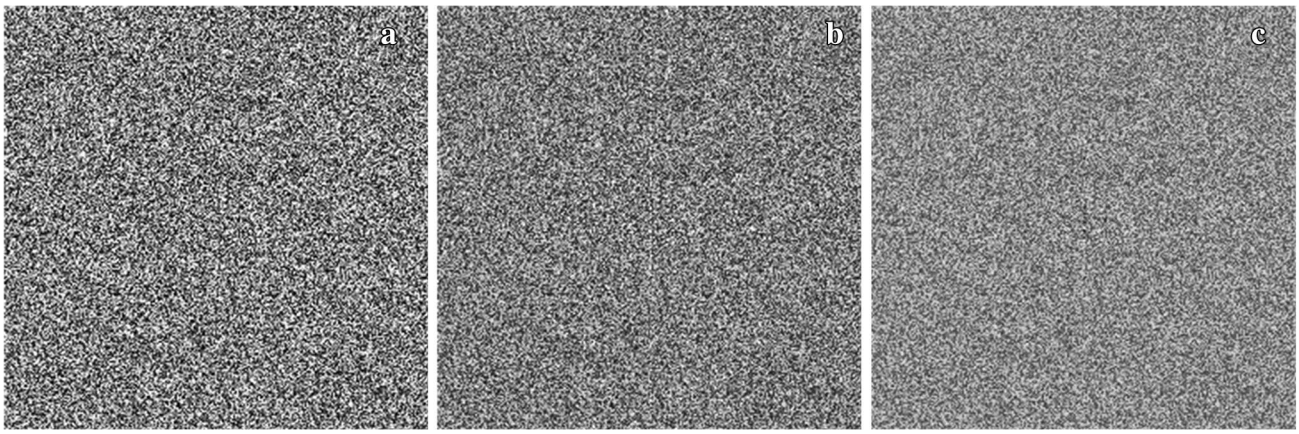

Fig. 4 **a** Cyphertext; private keys of **b** M_1 and **c** M_2

Fig. 5 **a–d** Decrypted images using the correct keys

For the encryption process, the parameters of the DMP-FrFT were set as (α_L, α_R; M_L, M_R) = (0.34, 0.73; 15, 20). The vector parameters (m_L, n_L) and (m_R, n_R) were 1×15 and 1×20 random vectors, respectively, that contained independent integer values. Figure 4a shows the RPM chosen to act as the cyphertext C (u, v), and Fig. 4b, c shows the corresponding generated private keys M_1 and M_2, respectively. During the showing process, the operation of angle was applied to each POM. Clearly, no information from the original images could be identified.

After completing the decryption process with the correct keys, the images could be reproduced as shown in Fig. 5a–d and can be recognized easily. However, owing to the cropping operation on the DCT spectrum, lossy-compression was produced on the four decrypted images. The corresponding CC values were calculated as 0.9826, 0.9847, 0.9920 and 0.9717, respectively.

We further illustrate the importance of the encryption keys in our proposed method. For the sake of the brevity, we show only the first decrypted image. Figure 6 shows the influence of the deviation in the fractional order in the DMP-FrFT on the decrypted image, and Figs. 7 and 8 show the decrypted image extracted using the incorrect periodicity of (M_L, M_R) and vector parameters (m_L, n_L; m_R, n_R). These

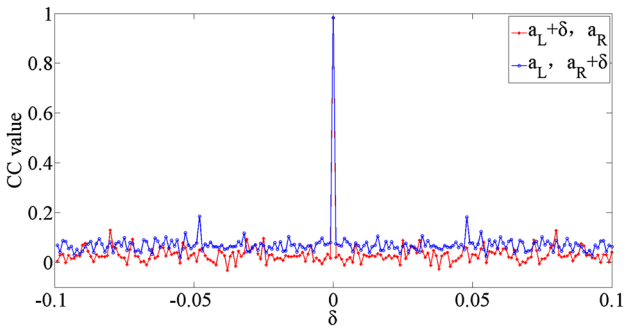

Fig. 6 Influence of the deviation in the fractional order in the DMP-FrFT on the decrypted image

results indicate that any deviation in the DMPFrFT parameters can result in poor image identification.

For interference-based cryptosystem, the silhouette problem is a key issue. As other researchers have stated [15, 25–28], some silhouette information can be recognized using only one POM owing to the equipollence of the three POMs. However, by benefitting from the conditional decomposition algorithm, this drawback is easily overcome. We evaluate this by using only one or two of the three POMs in Eq. 9 to reconstruct the images, and the results are shown in Fig. 9.

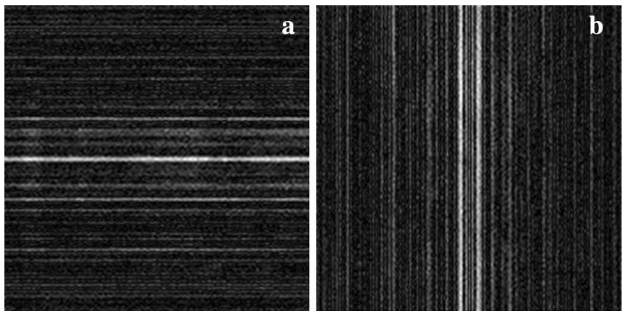

Fig. 7 Decrypted image with **a** $M_L = 14$ and **b** $M_R = 21$

Clearly, none of the visible information associated with the original images could be seen in any of the decrypted images. This is because the cyphertext was generated randomly by the computer while the other two POMs of M_1 and M_2 were obtained in an analytical way [15]; however, the relation between the original images and M_1 (and/or M_2) was disturbed by the conditional decomposition.

Our approach can be utilized to encode greater number of images by cropping smaller parts of the DCT spectrum. Figure 10 shows the decrypted images with overall numbers of 4, 9, and 16. As the number of original images increases, the quality of the decrypted images decreases, but the images can still be visually recognized.

Finally, to further verify the effectiveness of our proposed method, two different binary images and two random patterns were also taken as the original images. As shown in Fig. 11, the decrypted images were identical to the corresponding original images without any noises or distortions.

4 Conclusion

In summary, we presented an asymmetric cryptosystem based on optical interference using the DCT and conditional decomposition. In our approach, one plaintext-independent cyphertext is generated through conditional decomposition,

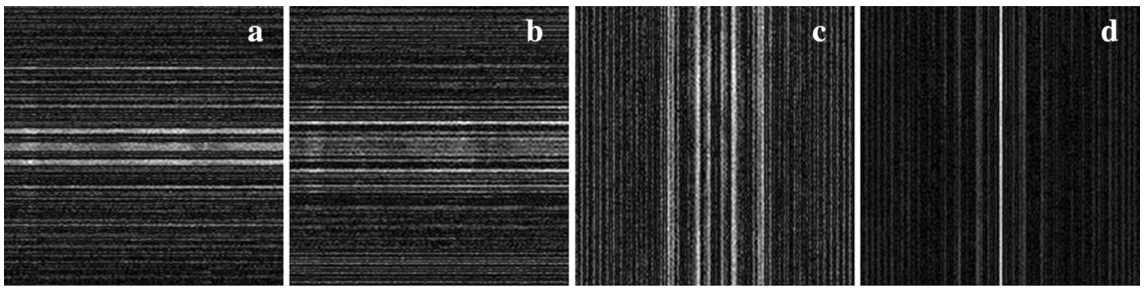

Fig. 8 Decrypted image with **a** $\mathbf{m}_L + 1$, **b** $\mathbf{n}_L + 1$, **c** $\mathbf{m}_R + 1$ and **d** $\mathbf{n}_R + 1$

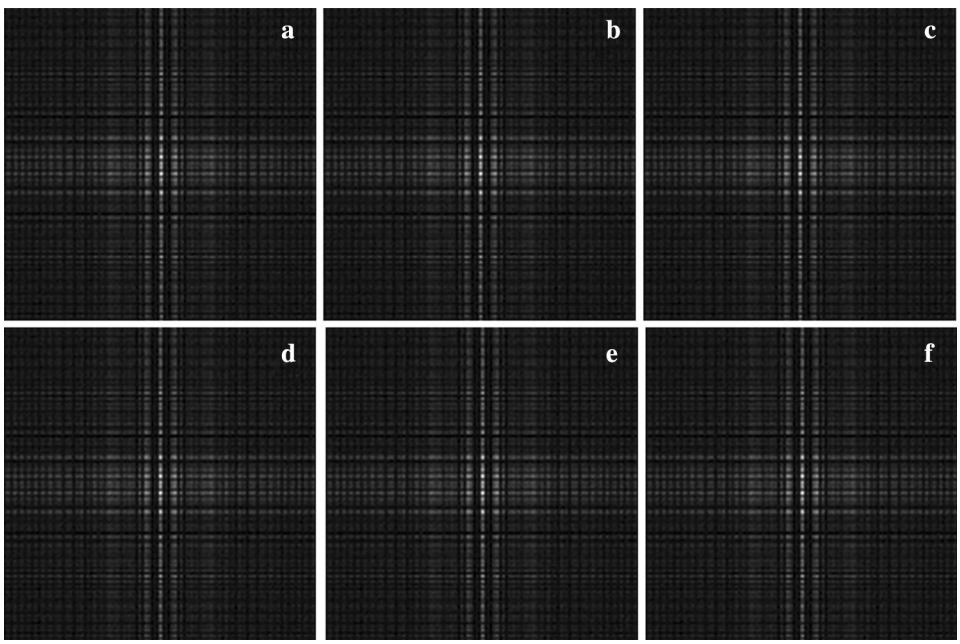

Fig. 9 Decrypted images using **a** only cyphertext; **b** cyphertext together with M_1; **c** cyphertext together with M_2; **d** only M_1; **e** only M_2; and **f** M_1 and M_2

Fig. 10 Decrypted images with encoded numbers of **a** 4, **b** 9 and **c** 16

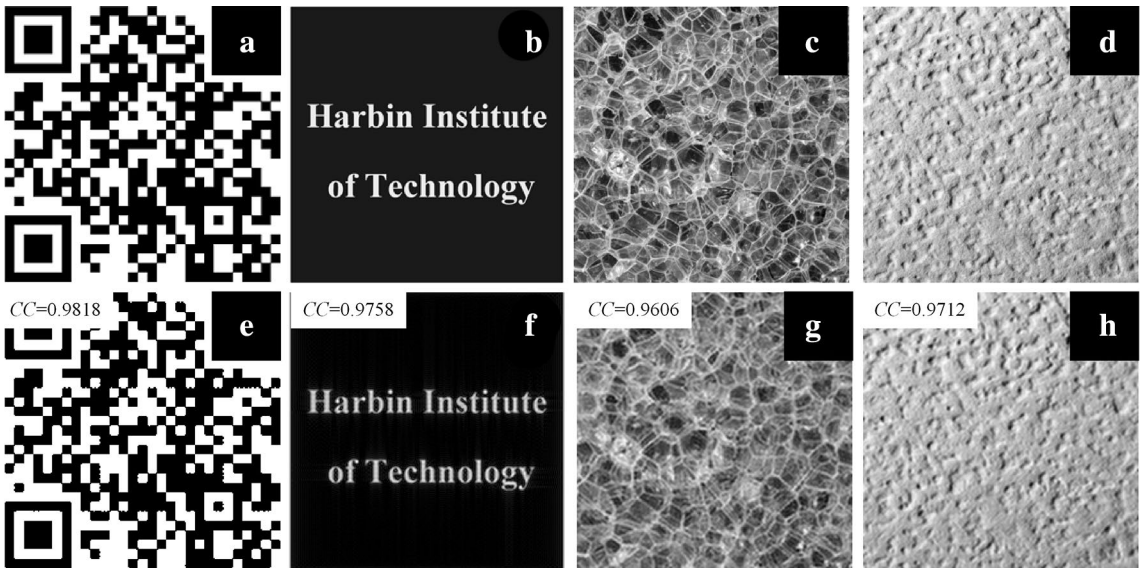

Fig. 11 Original **a**, **b** binary images and **c**, **d** random patterns; **e**–**h** decrypted images corresponding to (**a**–**d**)

and two plaintext-dependent POMs are yielded by interference to act as private keys. Therefore, the security strength is improved owing to the inherent non-linearity and asymmetry. Our numerical simulations demonstrate the validity and feasibility of our approach.

References

1. Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**, 767–769 (1995)
2. Tao, R., Xin, Y., Wang, Y.: Double image encryption based on random phase encoding in the fractional Fourier domain. Opt. Express **15**, 16067–16079 (2007)
3. Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett. **29**, 1584–1586 (2004)
4. Shan, M., Chang, J., Zhong, Z., Hao, B.: Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps. Opt. Commun. **285**, 4227–4234 (2012)
5. Liu, Z., Guo, Q., Xu, L., Ahmad, M.A., Liu, S.: Double image encryption by using iterative random binary encoding in gyrator domains. Opt. Express **18**, 12033–12043 (2010)
6. Zhou, N., Wang, Y., Gong, L., Chen, X., Yang, Y.: Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Opt. Laser Technol. **44**, 2270–2281 (2012)
7. Sui, L., Duan, K., Liang, J., Hei, X.: Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. Opt Express **22**, 10605–10621 (2014)
8. Tao, R., Lang, J., Wang, Y.: Optical image encryption based on the multiple-parameter fractional Fourier transform. Opt. Lett. **33**, 581–583 (2008)
9. Qin, W., Peng, X.: Asymmetric cryptosystem based on phase-truncated Fourier transforms. Opt. Lett. **35**, 118–120 (2010)
10. Wang, X., Zhao, D.: Security enhancement of a phase-truncation based image encryption algorithm. Appl. Opt. **50**, 6645–6651 (2011)
11. Liansheng, S., Bei, Z., Zhanmin, W., Qindong, S.: Amplitude-phase retrieval attack free image encryption based on two random masks and interference. Opt. Laser Eng. **86**, 1–10 (2016)
12. Sinha, A.: Nonlinear optical cryptosystem resistant to standard and hybrid attacks. Opt. Laser Eng. **81**, 79–86 (2016)

13. Wang, X., Zhao, D.: Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask. Opt. Lett. **38**, 3684–3686 (2013)
14. Zhang, Y., Wang, B.: Optical image encryption based on interference. Opt. Lett. **33**, 2443–2445 (2008)
15. Zhong, Z., Qin, H., Liu, L., Zhang, Y., Shan, M.: Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain. Opt. Express **25**, 6974 (2017)
16. Lin, C., Shen, X., Lei, M.: Generation of plaintext-independent private key based on conditional decomposition strategy. Opt. Laser Eng. **86**, 303–308 (2016)
17. Niu, C., Wang, X., Lv, N., Zhou, Z., Li, X.: An encryption method with multiple encrypted keys based on interference principle. Opt. Express **18**, 7827–7834 (2010)
18. Chen, W., Chen, X.: Optical multiple-image encryption based on multiplane phase retrieval and interference. J. Opt. **13**, 115401 (2011)
19. Qin, Y., Gong, Q.: Interference-based multiple-image encryption with silhouette removal by position multiplexing. Appl Opt. **52**, 3987 (2013)
20. Qin, Y., Jiang, H., Gong, Q.: Interference-based multiple-image encryption by phase-only mask multiplexing with high quality retrieved images. Opt. Laser Eng. **62**, 95–102 (2014)
21. Zhang, X., Meng, X., Wang, Y., Yang, X., Yin, Y., Li, X., Peng, X., He, W., Dong, G., Chen, H.: Hierarchical multiple-image encryption based on the cascaded interference structure and vector stochastic decomposition algorithm. Opt. Laser Eng. **107**, 258–264 (2018)
22. Alfalou, A., Brosseau, C., Abdallah, N., Jridi, M.: Simultaneous fusion, compression, and encryption of multiple images. Opt. Express **19**, 24023–24029 (2011)
23. Deng, P., Diao, M., Shan, M., Zhong, Z., Zhang, Y.: Multiple-image encryption using spectral cropping and spatial multiplexing. Opt. Commun. **359**, 234–239 (2016)
24. Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I.: Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. **30**, 1644–1646 (2005)
25. Lu, D., He, W., Liao, M., Peng, X.: Discussion and a new method of optical cryptosystem based on interference. Opt. Laser Eng. **89**, 13–21 (2017)
26. Zhao, J., Lu, H., Song, X., Li, J., Ma, Y.: Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique. Opt. Commun. **249**, 493–499 (2005)
27. Zhang, Y., Wang, B., Dong, Z.: Enhancement of image hiding by exchanging two phase masks. J. Opt. A Pure Appl Opt **11**, 125406 (2009)
28. Wang, X., Zhao, D.: Optical image hiding with silhouette removal based on the optical interference principle. Appl. Opt. **51**, 686–691 (2012)