Optical Review (2018) 25:701–707
https://doi.org/10.1007/s10043-018-0464-x

REGULAR PAPER

Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform

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

Received: 30 March 2018 / Accepted: 12 October 2018 / Published online: 19 October 2018

Abstract

An asymmetric image encryption scheme is proposed using a phase-truncated discrete multiple-parameter fractional Fourier transform (DMPFRFT). After applying a pixel-scrambling operation and random-phase mask, an asymmetric ciphertext with stationary white noise can be obtained using phase truncation in the DMPFRFT domain. Using the phase key, an inverse pixel-scrambling operation, and the parameters of the DMPFRFT, the original image can be successfully retrieved. Numerical simulations were conducted to demonstrate the validity and the security of the proposed method, and electro-optical hybrid setups are suggested for encryption and decryption.

Keywords Asymmetric image encryption · Discrete multiple-parameter fractional Fourier transform · Phase truncation

1 Introduction

Information security using optical technology has been of growing interest over the past decades owing to its particular advantages such as high speed, parallel processing, and multidimensional capabilities [1–3]. Significant work has been conducted in the field of optical encryption. For example, the classical double random-phase encoding (DRPE) technique was proposed by Refregier and Javidi [4] for the encryption of a primary image into a stationary white noise in the Fourier domain. To further enhance the key space and security, the DRPE scheme was extended into the fractional Fourier [5–7], gyrator transform [8, 9], Fresnel transform [10, 11], and spatial domains [12]. However, each of the above-mentioned DRPE schemes can be classified into the category of linear symmetric cryptosystems, in which all encryption keys are used for the decryption keys. Many studies have shown that these schemes are vulnerable to specific attacks such as chosen-cyphertext, chosen-plaintext, and known-plaintext attacks [13–18] owning to the inherently linear property of a mathematical or optical transformation. To resist a potential attack, an optical asymmetric cryptosystem with high security was proposed by Qin and Peng using a phase-truncated Fourier transform (PTFT) [19], in which a nonlinear operation of the phase and amplitude truncations is applied to remove the linearity of the DRPE scheme. In this nonlinear cryptosystem, decryption keys differing from encryption keys are generated during encryption. However, it was found that the cryptosystems are also vulnerable to such specific attacks owning to the use of a two-step iterative amplitude-phase retrieval algorithm [20, 21]. An optical PTFT-based cryptosystem is, therefore, not sufficiently secure when the encryption keys are compromised. Therefore, some variant cryptosystems have been proposed to enhance the security [22–25], such as encryption based on spherical wave illumination [22] and polarized light encoding [23]. The PTFT-based encryption technique has also been extended to the fractional Fourier transform (FRFT) domain for increased safety [26–29]. In this paper, a different asymmetric image encryption method using phase-truncated DMPFRFT (PTDMPFRFT) is adopted to realize the amplitude modulation of the output image. Compared to traditional cryptosystems in the FT [19] and FRFT [26–29] domains, the proposed PTDMPFRFT-based cryptosystem has more parameters characteristic of a larger key space, a signal representation of multiple degrees, and real-time optical processing capability, but without enhancing the complexity of the optical hardware. Compared to linear

✉ Mingguang Shan
smgsir@gmail.com

[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

cryptosystems [30–33], our cryptosystem is asymmetric, in which the decryption keys differ with the encryption keys. To a certain extent, our approach yields high-resistance against various attacks such as a chosen-plaintext attack, and significantly improves the encryption performance and security.

The remaining sections of this paper are organized as follows: Sect. 2 introduces the proposed encryption method, Sect. 3 presents the numerical simulation results showing the performance of the proposed method, and Sect. 4 provides some concluding remarks.

2 Principle of PTDMPFRFT-based cryptosystem

As a generalization of FRFT with multiple parameters, DMPFRFT demonstrates more choices to represent signals with extra degrees of freedom through the vector parameters. For a 2D signal $\boldsymbol{X}=(x_{\mathrm{n,m}})_{N\mathrm{L}\times N\mathrm{R}}$, the DMPFRFT with order (α_{L}, α_{R}), periodicity (M_{L}, M_{R}), and vector parameter ($\mathbf{n}'_{\mathrm{L}}$, $\mathbf{n}'_{\mathrm{R}}$) can be represented using two 1D-DMPFRFTs in the row and column, respectively, as shown below:

$$\begin{aligned}\mathbf{X}^{(\alpha_{\mathrm{L}},\alpha_{\mathrm{R}})}_{(M_{\mathrm{L}},M_{\mathrm{R}})}(\mathbf{m}_{\mathrm{L}},\mathbf{n}_{\mathrm{L}};\mathbf{m}_{\mathrm{R}},\mathbf{n}_{\mathrm{R}}) &= F^{(\alpha_{\mathrm{L}},\alpha_{\mathrm{R}})}_{(M_{\mathrm{L}},M_{\mathrm{R}})}\left(\mathbf{n}'_{\mathrm{L}},\mathbf{n}'_{\mathrm{R}}\right)\mathbf{X} \\ &= F^{(\alpha_{\mathrm{L}})}_{(M_{\mathrm{L}})}\left(\mathbf{n}'_{\mathrm{L}}\right)\cdot\mathbf{X}\cdot F^{(\alpha_{\mathrm{R}})}_{(M_{\mathrm{R}})}\left(\mathbf{n}'_{\mathrm{R}}\right),\end{aligned} \tag{1}$$

where $\mathbf{n}'$ can be defined as

$$n'_{\mathrm{k}} = \left(km_{\mathrm{k}} + Mm_{\mathrm{k}}n_{\mathrm{k}} + n_{\mathrm{k}}\right) \quad k = 0, 1, 2, \cdots, (M-1), \tag{2}$$

and $\mathbf{m} = \left(m_0, m_1, \cdots m_{(M-1)}\right) \in Z^M$, $\mathbf{n} = \left(n_0, n_1, \cdots n_{(M-1)}\right) \in Z^M$, and the eigen-decomposition structure of DMPFRFT is

$$F^{\alpha}_{M}\left(\mathbf{n}'\right) = VD^{\alpha}V^{T} = \begin{cases} \sum\limits_{k=0}^{N-1} \exp\left\{(-2\pi\,\mathrm{i}/M)\left[\alpha\left(\mathrm{mod}(k,M) + n'_{\mathrm{mod}\,(k,M)}M\right)\right]\right\} v_k v_k^T & \text{for } N \text{ odd} \\ \sum\limits_{k=0}^{N-2} \exp\left\{(-2\pi\,\mathrm{i}/M)\left[\alpha\left(\mathrm{mod}(k,M) + n'_{\mathrm{mod}\,(k,M)}M\right)\right]\right\} v_k v_k^T & \\ +\exp\left\{(-2\pi\,\mathrm{i}/M)\left[\alpha\left(\mathrm{mod}(N,M) + n'_{\mathrm{mod}\,(N,M)}M\right)\right]\right\} v_{N-1} v_{N-1}^T & \text{for } N \text{ even} \end{cases}. \tag{3}$$

In addition, *N*L and *N*R are arbitrary integers; *T* denotes the matrix transpose; $\boldsymbol{V}$ denotes a matrix with eigenvectors as the column vectors, i.e., $\boldsymbol{V}=[\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{N-2}|\boldsymbol{v}_{N-1}]$ for odd *N* and $\boldsymbol{V}=[\boldsymbol{v}_0|\boldsymbol{v}_1|\ldots|\boldsymbol{v}_{N-2}|\boldsymbol{v}_N]$ for even *N*; and $\boldsymbol{D}$ denotes a diagonal matrix with its diagonal entries corresponding to the eigenvalues for each column eigenvector $\boldsymbol{v}_{\mathrm{k}}$ in $\boldsymbol{V}$ [30–33].

The proposed encryption and decryption process is shown in Fig. 1. Let $f(x,y)$ represent the original image with $N\times N$ pixels. For encryption, as shown in Fig. 1a, the original image $f(x,y)$ is first scrambled by $\mathbf{J}[\cdot]$, and then multiplied by the RPM function $\exp[ip(x,y)]$. After applying a further DMPFRFT operation with parameters of (M_{L}, M_{R}; α_{L}, α_{R}; $\mathbf{m}_{\mathrm{L}}$, $\mathbf{n}_{\mathrm{L};}$ and $\mathbf{m}_{\mathrm{R}}$, $\mathbf{n}_{\mathrm{R}}$), the final encrypted image $E(x,y)$ can be expressed as

$$E(x,y) = \mathrm{PT}\left\{F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}\left(\mathbf{n}'_L,\mathbf{n}'_{\mathrm{R}}\right)\left\{\mathrm{J}\left[f(x,y)\right]\exp\left[ip(x,y)\right]\right\}\right\}. \tag{4}$$

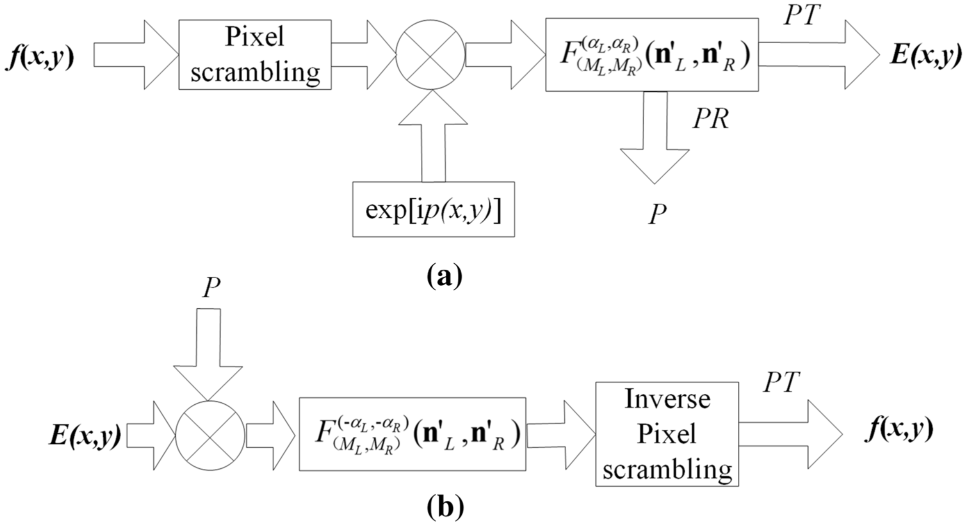
f(x,y)
Pixel scrambling
$F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(\mathbf{n}'_L,\mathbf{n}'_R)$
PT
E(x,y)
PR
P
exp[ip(x,y)]
(a)
P
E(x,y)
$F^{(-\alpha_L,-\alpha_R)}_{(M_L,M_R)}(\mathbf{n}'_L,\mathbf{n}'_R)$
Inverse Pixel scrambling
PT
f(x,y)
(b)

Fig. 1 Schematic of **a** encryption and **b** decryption

In addition, the phase key $P(x,y)$ for decryption generated during the encryption can be expressed as

$$P(x,y) = \mathrm{PR}\left\{ F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)} \left(\mathbf{n}_L^{'}, \mathbf{n}_\mathrm{R}^{'}\right) \left\{ \mathrm{J}\left[f(x,y)\right] \exp\left[ip(x,y)\right] \right\} \right\}, \tag{5}$$

where $p(x,y)$ is a statistically white sequence uniformly distributed in (0, 2π), the operator PT denotes the phase truncation, and PR denotes the amplitude truncation.

For decryption, as shown in Fig. 1b, the decrypted process can be carried out as follows:

$$f(x,y) = PT\left\{ \mathrm{J}^{-1}\left\{ F^{(-\alpha_L,-\alpha_R)}_{(M_L,M_R)} \left(\mathbf{n}_L{'}, \mathbf{n}_R{'}\right) \left[E(x,y) \cdot P\right] \right\} \right\}, \tag{6}$$

where $\mathbf{J}^{-1}[\bullet]$ is the inverse pixel-scrambling operation.

Note that our algorithm extends the PT-based cryptosystem from the FT [19] or FRFT [26–29] domain to the DMPFRFT domain. Obviously, a pixel-scrambling operation, RPM, and the parameters of DMPFRFT including the periodicities (M_L, M_R), transform orders (α_L, α_R), and vector parameters ($\mathbf{m}_\mathrm{L}$, $\mathbf{n}_{\mathrm{L};}$ $\mathbf{m}_\mathrm{R}$, $\mathbf{n}_\mathrm{R}$) serve as the public keys. They take a critical role during the encryption, and particularly increase the public key space fivefold relative to [19] employing two RPMs, and 2.5-fold relative to [26] employing two FRFT orders and two RPMs, which then lead to a superior encryption security standard. As many others have pointed out [19, 26–29], the phase P generated from the phase-truncated encryption process is a private decryption key, but differs from the encryption keys. Compared to [19, 26], the parameters of both a pixel-scrambling operation and DMPFRFT can be regarded as additional decryption keys, which further break the linearity of a cryptosystem [30–33]. Our approach can then efficiently increase the resistance against specific attacks, including known-plaintext and chosen public key attacks.

To quantitatively evaluate the performance of the proposed method, the normalized mean square error (NMSE) between the original image and the decrypted image is defined as

$$\mathrm{NMSE}{=}\sum_{j=1}^{A}\sum_{j=1}^{B}\left[I_\mathrm{D}(i,j) - I_\mathrm{E}(i,j)\right]^2 \Bigg/ \sum_{j=1}^{A}\sum_{j=1}^{B}\left[I_\mathrm{E}(i,j)\right]^2, \tag{7}$$

where $A \times B$ is the size of the image, and $I_\mathrm{D}(i,j)$ and $I_\mathrm{E}(i,j)$ are the values of the decrypted image and the original image at the pixel (i, j), respectively. In a practical sense, when the NMSE is larger than 0.31, the decrypted image can barely be recognized.

In addition to being implemented digitally, the scheme can also be implemented using an electro-optical hybrid setup [20]. For encryption, the original image is set to the input plane, as shown in Fig. 2a. An optical pixel-scrambling device (OPSD) is used to realize the pixel-scrambling operation. First, a spatial light modulator SLM1 is used to generate RPM, and SLM2 and a lens L are used to implement the DMPFRFT. A CCD detector can be applied in a straightforward manner to conduct a phase truncation to record the reservation intensity; however, to record the reservation phase after an amplitude truncation, a reference beam, as shown by the arrow with a dashed line, should be split from the light source to accomplish interferometry [19]. A computer is used to control all SLMs and the CCD. For decryption, as shown in Fig. 2b, the encrypted image $E(x,y)$ is set to the input plane, and the phase key P is displayed on SLM1, whereas the OPSD is tightly located in the input plane of the CCD. As shown in Eq. (6), because the decrypted image results from a phase-truncation operation, a reference beam is again not required, and only the CCD can be used to record the decrypted image during the decryption process. Therefore, it is clear that the decryption process is more convenient and efficient.

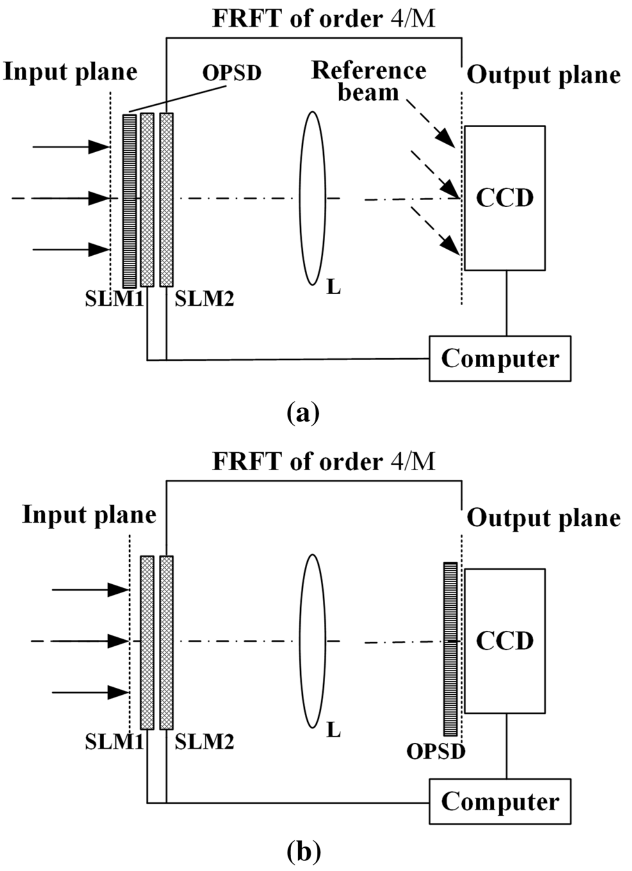

Fig. 2 Optoelectronic hybrid setup of the **a** encryption and **b** decryption system

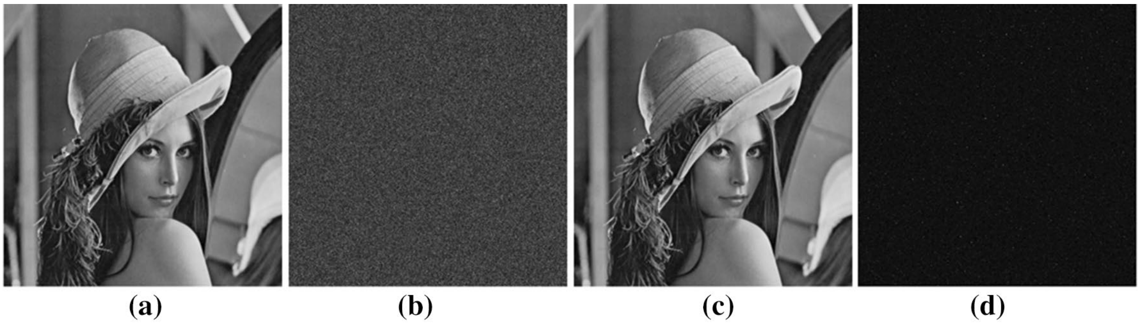

Fig. 3 **a** Original image, **b** encrypted image, and decrypted image with **c** all of the correct keys and **d** only public keys

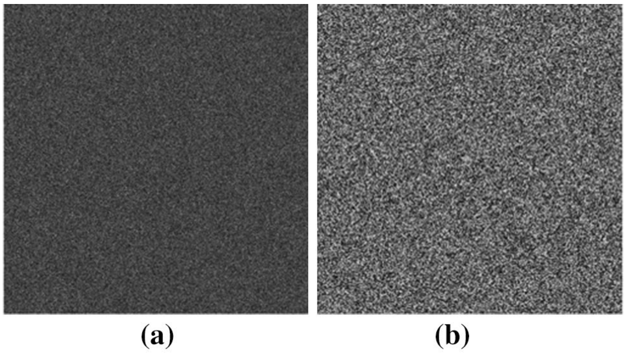

Fig. 4 Decrypted image with incorrect **a** phase key *P*, and **b** inverse pixel-scrambling operation

3 Simulation results and performance analysis

Numerical simulation experiments have been conducted to verify the proposed encryption method. In our experiment, a "Lena" image of 512 pixels × 512 pixels in size and having 256 Gy levels is taken as the original image, as shown in Fig. 3a. The image is broken up into 65,536 subsections of 2 pixels × 2 pixels using a pixel-scrambling operation, as suggested in [34], in which the gray values of the different pixels are interchanged. The DMPFRFT system parameters are (M_L, M_R; α_L, α_R) = (15, 20; 0.34, 0.73). The vector parameters ($\mathbf{m}_L$, $\mathbf{n}_L$) and ($\mathbf{m}_R$, $\mathbf{n}_R$) with independent integer values are 1×15 and 1×20 random vectors. The encrypted image with stationary white noise can then be obtained, as shown Fig. 3b. After applying the correct keys to the encrypted image, the decrypted image can be obtained, as shown in Fig. 3c, which is the same as the original image without any noise or distortion. After applying only the correct public keys without private key *P* to the encrypted image, the decrypted image can barely be recognized, as shown in Fig. 3d. The NMSE value between the decrypted and encrypted images is 4.02×10^{-29} when all of the correct keys are used, but 0.618 when only the correct public keys are used. It can be seen that the proposed method retrieves the original image exactly, and creates an effective trap for the illegal deciphers.

In the following analysis, the effect of the deviation of different keys on the decrypted image is considered. Figure 4a shows the decrypted image obtained using the incorrect phase *P*, and Fig. 4b shows the decrypted image obtained using an incorrect decryption of the inverse pixel-scrambling operation [34]. Figure 5 shows the decrypted image obtained using

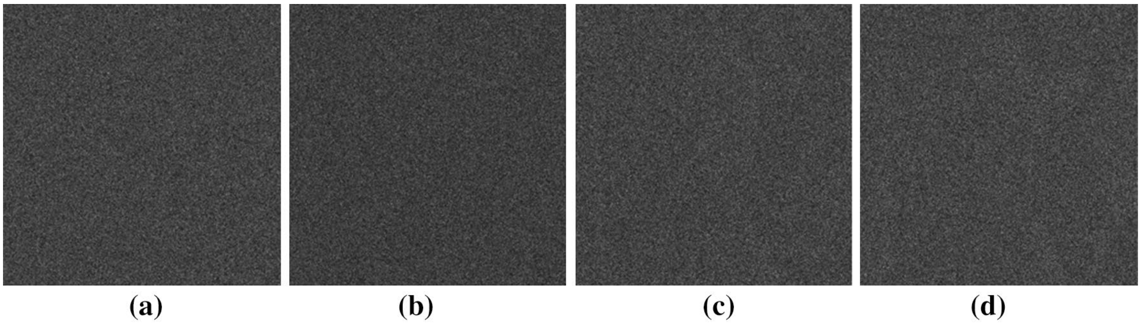

Fig. 5 Decrypted image with different incorrect keys: **a** {(14, 19), (−0.34, −0.73), (mL, nL), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, **b** {(15, 20), ($-0.34+10^{-7}$, $-0.73+10^{-7}$), ($\mathbf{m}_L$, $\mathbf{n}_L$), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, **c** {(15, 20), (−0.34, −0.73), ($\mathbf{m}_L+2$, $\mathbf{n}_L+1$), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, **d** {(15, 20), (−0.34, −0.73), ($\mathbf{m}_L$, $\mathbf{n}_L$), ($\mathbf{m}_R+1$, $\mathbf{n}_R+1$)}

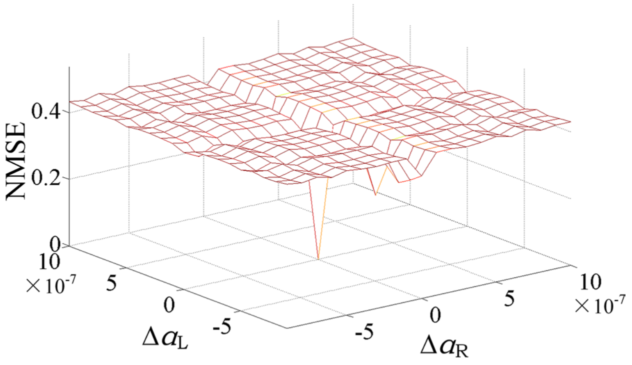

Fig. 6 NMSEs with different deviation of transform order parameters

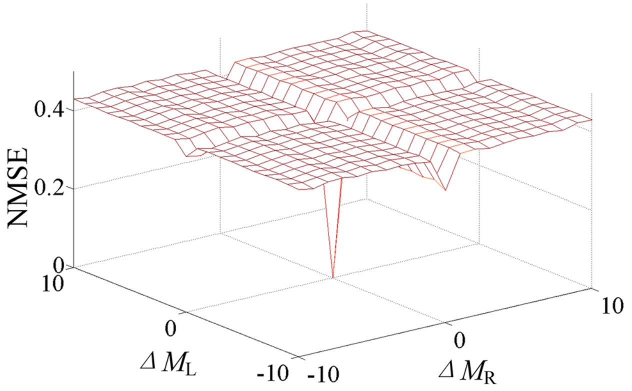

Fig. 7 NMSEs with different deviation of periodicity parameters

the incorrect DMPFRFT keys of {(14,19), (−0.34, −0.73), ($\mathbf{m}_L$, $\mathbf{n}_L$), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, {(15,20), ($-0.34+10^{-7}$, $-0.73+10^{-7}$), ($\mathbf{m}_L$, $\mathbf{n}_L$), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, {(15,20), (−0.34,−0.73), ($\mathbf{m}_L+2$, $\mathbf{n}_L+1$), ($\mathbf{m}_R$, $\mathbf{n}_R$)}, and {(15,20); (−0.34,−0.73); ($\mathbf{m}_L$,$\mathbf{n}_L$); ($\mathbf{m}_R+1$,$\mathbf{n}_R+1$)}. The corresponding NMSEs are 0.5522, 0.4422, 0.4355, 0.4276, 0.4169, and 0.4183. It can be seen that any errors in the phase key, inverse pixel-scrambling operation, and/or DMPFRFT parameters can make the image difficult to retrieve, thereby achieving a high security hierarchy in the applications.

Now, the effects of the derivation of the transform orders on the NMSE are considered when the other parameters are correct. As shown in Fig. 6, the NMSEs approach zero when the transform orders are close to the correct key values. However, high NMSEs of > 0.31 are yielded when a deviation of $\geq 10^{-7}$ is from any of the correct transform orders. Thus, the transform orders result in high sensitivity and security. The effect of the derivation of the periodicities on the NMSE is then considered, whereas the other parameters are correct. As shown in Fig. 7, the NMSEs approach zero when the periodicities are close to the correct key values. However, high NMSEs of > 0.31 are also yielded when

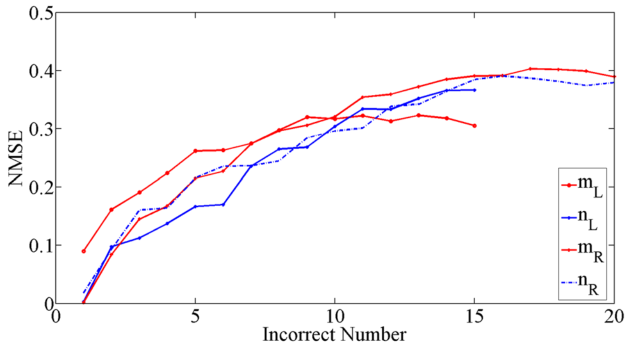

Fig. 8 NMSEs versus deviation of vector parameters

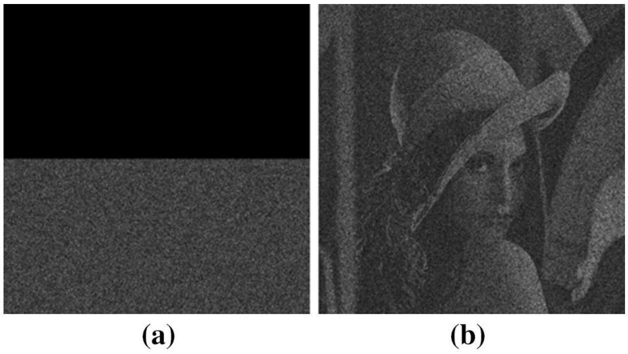

Fig. 9 Robustness against occlusion attack: **a** encrypted image with 50% occlusion, and **b** decrypted image

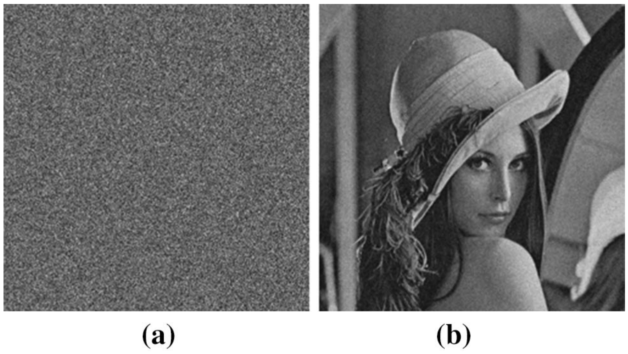

Fig. 10 Robustness against noise attack: **a** encrypted image with Gaussian noise of standard deviation of 0.10 and **b** decrypted image

a deviation of ≥ 1 occurs from any of the correct periodicities. Thus, the periodicities can be employed to improve the security. Finally, the effects of the derivation of the vector parameters on the NMSEs are considered, whereas the other parameters are correct. The results when using incorrect vector parameters are shown in Fig. 8, in which an incorrect number denotes the number of incorrect elements in the matrixes generated for different vector parameters.

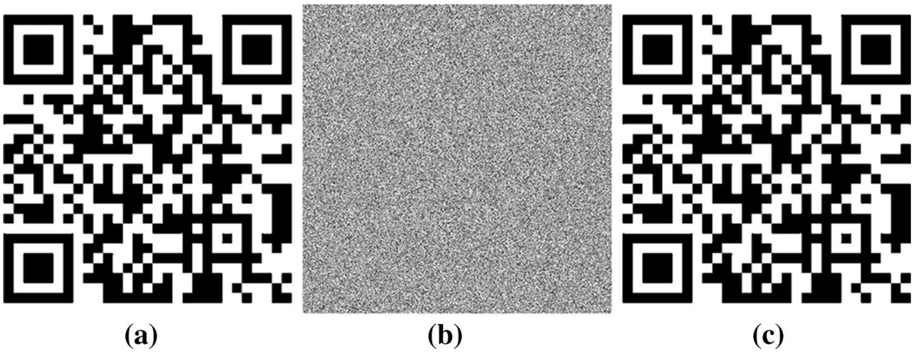

Fig. 11 **a** Original binary image of QR code, **b** encrypted image, and **b** decrypted image

As shown in Fig. 8, although the vector parameters are not as sensitive as the transform orders and periodicities, the NMSEs also increase quickly with a derivation of the vector parameters. When a derivation of a vector parameter makes NMSE higher than 0.31, the decrypted image is also difficult to recognize, as shown in Fig. 5c–d, even with other correct keys. In this case, the vector parameters can also be regarded as additional keys to promote a high level of security.

The robustness against occlusions is usually applied to assess how one encryption method operates with a loss of data in the ciphertext image. An encrypted image reduced by 50% is shown in Fig. 9a, and its decrypted image using all of the correct keys is shown in Fig. 9b. The NMSE is 0.2541. Clearly, the retrieved image can be clearly recognized, which means that our approach has sufficient robustness against an occlusion attack. The robustness of our approach is also tested against a noise attack. The encrypted image is distorted with zero-mean white additive Gaussian noise with a standard deviation of 0.10, which is twice that used in [30]–[33]. A noise-encrypted image is shown in Fig. 10a, and its decrypted image with all of the correct keys is shown in Fig. 10b. The NMSE is 0.0233. The decrypted result can also be easily identified. This is because our approach can transform added noise into a wide stationary white additive noise for a decrypted image [35], which can be suppressed to decrease the effects of the noise degradation. All of the above prove that our approach has certain robustness against various attacks.

Finally, to further confirm the validity of our approach, a binary image of a QR code containing the URL of our university is also utilized as the original image. It can be seen from Fig. 11 that the encrypted image looks like stationary white noise, and the decrypted image is identical to the original image without any noises or distortions.

4 Conclusion

A method using PTDMPFRFT is proposed for asymmetric image encryption. The decryption keys used in the system can be generated during the encryption process, but differ from the encryption keys. The decryption keys include the phase key *P*, pixel-scrambling operation, and a set of DMPFRFT parameters. The security of the asymmetric cryptosystem can be enhanced using DMPFRFT to enlarge the key space. Electro-optical implementation setups for encryption and decryption have also been suggested. Numerical simulations have also been conducted to demonstrate the recovered quality and validity of the proposed method.

References

1. Alfalou, A., Brosseau, C.: Optical image compression and encryption methods. Adv. Opt. Photon. **1**, 589–636 (2009)
2. Chen, W., Javidi, B., Chen, X.: Advances in optical security systems. Adv. Opt. Photon. **6**, 120–155 (2014)
3. Liu, S., Guo, C.L., Sheridan, J.T.: A review of optical image encryption techniques. Opt. Laser. Technol. **57**, 327–342 (2014)
4. Refregier, P., Javidi, B.: Optical image encryption based on input plane encoding and Fourier plane random encoding. Opt. Lett. **20**, 767–769 (1995)
5. Unnikrishnan, G., Joseph, J., Singh, K.: Optical encryption by double random phase encoding in the fractional Fourier domain. Opt. Lett. **25**, 887–889 (2000)
6. Zhong, Z., Chang, J., Shan, M.G., Hao, B.G.: Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption. Opt. Commun. **285**, 18–23 (2012)
7. Liu, Z.J., Li, S., Liu, W., Wang, Y.H., Liu, S.T.: Image encryption algorithm by using fractional fourier transform and pixel scrambling operation based on double random phase encoding. Opt. Lasers Eng. **51**, 8–14 (2013)
8. Liu, Z., Chen, H., Liu, T., Li, P., Dai, J., Sun, X., Liu, S.: Double-image encryption based on the affine transform and the gyrator transform. J. Opt. **12**, 035407 (2010)
9. Wang, Q., Guo, Q., Lei, L.: Double image encryption based on phase–amplitude mixed encoding and multistage phase encoding in gyrator transform domains. Opt. Laser Technol. **48**, 267–279 (2013)
10. Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett. **29**, 1584–1586 (2004)
11. Chen, W., Chen, X., Sheppard, C.J.R.: Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain. Opt. Express **20**, 3853–3865 (2012)
12. Chen, W., Chen, X.: Space-based optical image encryption. Opt. Express **18**, 27095–27104 (2010)
13. 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)

14. Peng, X., Wei, H., Zhang, P.: Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt. Lett. **31**, 3261–3263 (2006)
15. 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**, 3181–3186 (2006)
16. Frauel, Y., Castro, A., Naughton, T.J., Javidi, B.: Resistance of the double random phase encryption against various attacks. Opt. Express **15**, 10253–10265 (2007)
17. Liu, W., Wang, G., Xie, K.: A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption. Opt. Express **17**, 13928–13938 (2009)
18. Barrera, J.F., Vargas, C., Tebaldi, M., Torroba, R., Bolognini, N.: Known-plaintext attack on a joint transform correlator encrypting system. Opt. Lett. **35**, 3553–3555 (2010)
19. Qin, W., Peng, X.: Asymmetric cryptosystem based on phase-truncated Fourier transforms. Opt. Lett. **35**, 118–120 (2010)
20. Wang, X., Zhao, D.: A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms. Opt. Commun. **285**, 1078–1081 (2012)
21. Wang, X., Chen, Y., Dai, C., Zhao, D.: Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform. Appl. Opt. **53**, 208–213 (2014)
22. Ding, X., Deng, X., Song, K., Chen, G.: Security improvement for asymmetric cryptosystem based on spherical wave illumination. Appl. Opt. **52**, 467–473 (2013)
23. Rajput, S.K., Nishchal, N.K.: Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain. Appl. Opt. **52**, 4343–4352 (2013)
24. Wang, X., Zhao, D.: Double images encryption method with resistance against the specific attack based on an asymmetric algorithm. Opt. Express **20**, 11994–12003 (2012)
25. Mehra, I., Nishchal, N.K.: Asymmetric cryptosystem for securing multiple images. Opt. Laser Technol. **60**, 1–7 (2014)
26. Wang, X., Zhao, D.: Security enhancement of a phase truncation based image encryption algorithm. Appl. Opt. **50**, 6645–6651 (2011)
27. Rajput, S.K., Nishchal, N.K.: Image encryption based on interference that uses fractional Fourier domain asymmetric keys. Appl. Opt. **51**, 1446–1452 (2012)
28. 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 (2015)
29. Qu, W., Qing, G., Liang, L.: Asymmetric multiple-image hiding using phase retrieval technique based on amplitude- and phase-truncation in fractional Fourier domain. Optik Int. J. Light Electron Opt. **124**, 3898–3902 (2013)
30. Tao, R., Lang, J., Wang, Y.: Optical image encryption based on the multiple-parameter fractional Fourier transform. Opt. Lett. **33**, 581–583 (2008)
31. Lang, J., Tao, R., Wang, Y.: Image encryption based on the multiple-parameter discrete fractional fourier transform and chaos function. Opt. Commun. **283**, 2092–2096 (2010)
32. Shan, M., Chang, J., Zhong, Z., Hao, B.G.: Double image encryption based on discrete multiple-parameter fractional fourier transform and chaotic maps. Opt. Commun. **285**, 4227–4234 (2012)
33. Zhong, Z., Zhang, Y., Shan, M., Wang, Y., Zhang, Y., Xie, H.: Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform. J. Opt. **16**, 125404 (2014)
34. 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)
35. Javidi, B., Sergent, A., Zhang, G., Guibert, L.: Fault tolerance properties of a double phase encoding encryption technique. Opt. Eng. **36**, 992–998 (1997)