Optica Applicata, Vol. LI, No. 1, 2021
DOI: 10.37190/oa210110

Optical multiple-image encryption in discrete multiple-parameter fractional Fourier transform scheme using complex encoding, theta modulation and spectral fusion

GUANGYU LUAN[1*], ZHI ZHONG[2], MINGGUANG SHAN[2*]

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

[2]College of Information and Communication Engineering, Harbin Engineering University, Harbin, Heilongjiang, 150001, China

[*]Corresponding authors: smgsir@gmail.com (MS), and luanguangyu@126.com (GL)

We present a novel encryption method for multiple images in a discrete multiple-parameter fractional Fourier transform scheme, using complex encoding, theta modulation and spectral fusion. All pairs of original images are encoded separately into a complex signal. The spectrum of each complex signal can then be scattered into various positions in the spectral plane and multiplexed into one spectral image with a combination of theta modulation and spectral fusion. After Fourier transforming back to the spatial domain, the multiplexed signal is encrypted in the discrete multiple -parameter fractional Fourier transform domain. Information about the original images can only be successfully decrypted given the possession of all correct keys. The parameters of chaotic pixel scrambling for the proposed method enlarge the key space. Moreover, the proposed method solves the crosstalk problem of multiple images and improves the multiplexing capacity. Numerical simulations demonstrate the effectiveness of the proposed method.

Keywords: optical security and encryption, multiple images, multiplexing, crosstalk.

1. Introduction

Optical image encryption (OIE) [1–8] has led to significant developments in the field of information security over the past decade, because it uses a fast, parallel, and multidimensional imaging principle. Significant work has been done in OIE since REFREGIER and JAVIDI [1] proposed double random phase encoding (DRPE) for encoding an original image into stationary white noise. Multiple-image encryption [9–13], such as complex

encoding [14], is one of the practical applications of OIE, and is used to transmit image data and protect it from illegal invasion. However, there is crosstalk among the images, as the number of original images increase. Various multiplexing approaches [15–19] have been suggested for multiple-image encryption. One of the most appealing multiplexing approaches was proposed by Mosso *et al*. [20]. Their approach involves encrypting each frame of a movie through DRPE, and then theta modulating the resulting images into a single image. After filtering and applying the correct keys, each image can then be retrieved to rebuild the movie. This approach has been extended from the Fourier to the fractional Fourier [21] and discrete multiple-parameter fractional Fourier domains [22]. Theta modulation [20, 21] can be employed to multiplex multiple images through sinusoidal amplitude grating, with different orientation angles and (or) spatial frequencies. However, crosstalk or even overlap of different images caused by the diffraction orders of the grating can increase concomitantly with the number of images, degrading the quality of the decrypted images. Moreover, the improved theta modulation in [22] still results in crosstalk through the use of space fusion. And the multiplexing capacity in [22] must be improved to facilitate the transmission and storage of multiple images. The aforementioned approaches are implemented in the spatial domain, which increases their complexity and the number of processes needed to encrypt the original images. Thus, spectral fusion has been developed by combining a Fourier transform (FT) [23] or discrete cosine transformation [24, 25] with spatial shifting, where only the low frequencies of the spectra are employed to recover the original images. This is acceptable, because most spectral information in normal images focuses on low frequencies [26]. However, a segmentation criterion [23, 24] or iteration process [25] is required to avoid crosstalk among the overlapping spectra.

Therefore, we propose a new multiple-image encryption approach. Complex encoding, theta modulation and spectral fusion are incorporated into the discrete multiple-parameter fractional Fourier transform (DMPFrFT) scheme for the first time in the literature, to the best knowledge of the authors. The advantage to our method lies in its increased multiplexing capacity, which avoids the crosstalk problem with multiple images. Moreover, the parameters of chaotic pixel scrambling used in the proposed method further strengthen the security. Simulation results are presented to demonstrate the feasibility of the proposed approach to encrypting multiple images.

2. Theoretical analysis

The proposed encryption procedure for multiple images is divided into two parts: multiplexing and encryption. For multiplexing, we consider that the FT can be operated on complex signals, whereas a normal image does not have an imaginary component, such that the FT operation is inefficient. Consequently, it is possible to take advantage of the imaginary component to yield a complex signal from a pair of original images. Each pair of images can be multiplexed as follows:

$$I'_j(x, y) = I_{2j-1}(x, y) + iI_{2j}(x, y), \quad j = 1, ..., J/2 \tag{1}$$

where I' is a complex signal, I denotes an original image, j is the j-th image, and J is the total number of original images.

To rectify the crosstalk caused by theta modulation, the complex signals are multiplexed in the spectral domain. We implement theta modulation g_j, FT, and filtering successively. Owing to the dependency on the orientation and spatial frequency of the grating, the +1st-order positions differ from each other in the spectral plane. Thus, we multiplex the selected spectra in the spectral plane. We denote the spectral fusion operation with filtering by $\mathbf{SF}[\cdot]$, and the final multiplexed result can be expressed as

$$R(x, y) = \mathrm{IFT}\left\{ \sum_{j=1}^{J/2} \mathbf{SF}\left[\mathrm{FT}\left[I'_j(x, y) g_j(x, y) \right] \right] \right\} \tag{2}$$

where

$$g_j(x, y) = \frac{1}{2} + \frac{m}{2} \cos\left[2\pi f_0 (x \cos\theta_j + y \sin\theta_j) \right] \qquad (m \le 1)$$

represents the grating transmittance function, and the parameters f_0 and θ_j express the spatial frequency and orientation angle of the grating, respectively.

For encryption, the multiplexed signal $R(x, y)$ is initially subjected to chaotic pixel scrambling (denoted by $\mathbf{SC}_{\{a_0, \lambda, t\}}[\cdot]$) with the parameters a_0, the coefficient λ, and the truncated position t. It is then bonded with a random phase mask (RPM) of $\exp[iM(x, y)]$, where $M(x, y)$ is uniformly distributed in the interval $[0, 2\pi]$. Through a subsequent DMPFrFT operation with the parameters of order $(\alpha_\mathrm{L}, \alpha_\mathrm{R})$, periodicity $(M_\mathrm{L}, M_\mathrm{R})$, and vector $(\mathbf{m}_\mathrm{L}, \mathbf{n}_\mathrm{L}; \mathbf{m}_\mathrm{R}, \mathbf{n}_\mathrm{R})$, we can obtain the final cipher text $E(x, y)$ in the output plane as

$$\begin{aligned} E(x, y) &= F^{(\alpha_\mathrm{L}, \alpha_\mathrm{R})}_{(M_\mathrm{L}, M_\mathrm{R})}(\mathbf{n}'_\mathrm{L}, \mathbf{n}'_\mathrm{R}) \left\{ \mathbf{SC}_{\{a_0, \lambda, t\}} \left[R(x, y) \right] \exp\left[iM(x, y) \right] \right\} \\ &= F^{(\alpha_\mathrm{L}, \alpha_\mathrm{R})}_{(M_\mathrm{L}, M_\mathrm{R})}(\mathbf{n}'_\mathrm{L}, \mathbf{n}'_\mathrm{R}) \left\{ \mathbf{SC}_{\{a_0, \lambda, t\}} \left[\mathrm{IFT}\left[\sum_{j=1}^{J/2} \mathbf{SF}\left[\mathrm{FT}\left[\left[I_{2j-1}(x, y) + iI_{2j}(x, y) \right] g_j(x, y) \right] \right] \right] \right. \right. \\ &\qquad \left. \left. \times \exp\left[iM(x, y) \right] \right\} \end{aligned} \tag{3}$$

where two 1D-DMPFrFTs along the x and y axes, respectively, can be forthwith expressed as

$$F^{(\alpha_\mathrm{L}, \alpha_\mathrm{R})}_{(M_\mathrm{L}, M_\mathrm{R})}(\mathbf{n}'_\mathrm{L}, \mathbf{n}'_\mathrm{R})\mathbf{X} = F^{(\alpha_\mathrm{L})}_{(M_\mathrm{L})}(\mathbf{n}'_\mathrm{L}) \cdot \mathbf{X} \cdot F^{(\alpha_\mathrm{R})}_{(M_\mathrm{R})}(\mathbf{n}'_\mathrm{R}) \tag{4}$$

where $\mathbf{X} = (x_{n, m})_{N_\mathrm{L} \times N_\mathrm{R}}$ denotes a 2D signal, $\mathbf{n}' = (n'_0, n'_1, \ldots, n'_{(M-1)}) \in Z^M$, and the eigen-decomposition structure of the DMPFrFT is

$$F_M^{\alpha}(\mathbf{n}') = \mathbf{V}\mathbf{D}^{\alpha}\mathbf{V}^{\mathrm{T}}$$

$$= \begin{cases} \sum_{k=0}^{N-1} \exp\left\{\frac{-2\pi i}{M}\left[\alpha(\mathrm{mod}(k, M) + n'_{\mathrm{mod}(k, M)}M)\right]\right\}\mathbf{v}_k\mathbf{v}_k^{\mathrm{T}} & \text{for } N \text{ odd} \\ \sum_{k=0}^{N-2} \exp\left\{\frac{-2\pi i}{M}\left[\alpha(\mathrm{mod}(k, M) + n'_{\mathrm{mod}(k, M)}M)\right]\right\}\mathbf{v}_k\mathbf{v}_k^{\mathrm{T}} & \\ \quad + \exp\left\{\frac{-2\pi i}{M}\left[\alpha(\mathrm{mod}(N, M) + n'_{\mathrm{mod}(N, M)}M)\right]\right\}\mathbf{v}_{N-1}\mathbf{v}_{N-1}^{\mathrm{T}} & \text{for } N \text{ even} \end{cases} \tag{5}$$

where $\mathbf{V}$ denotes a matrix with eigenvectors as column vectors, *i.e.*,

$$\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|...|\mathbf{v}_{N-2}|\mathbf{v}_{N-1}] \quad \text{for } N \text{ odd}$$

$$\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|...|\mathbf{v}_{N-2}|\mathbf{v}_N] \quad \text{for } N \text{ even}$$

and $\mathbf{D}$ denotes a diagonal matrix whose diagonal entries correspond to the eigenvalues for each column of eigenvectors $\mathbf{v}_k$ in $\mathbf{V}$ [27–29], and T denotes the matrix transpose.

In our encryption system, the encryption is performed digitally or optically, while the decryption can be processed digitally in a computer. A schematic for an optoelectronic hybrid implementation of encryption process is shown in Fig. 1. The light path is illuminated with a coherent parallel light beam. The light beam is separately modulated by the first and the second spatial light modulator SLM_1 and SLM_2 for amplitude modulation and phase modulation. In other words, we obtain two original images, respectively. The complex signal is then generated by encoding the two original images. Sinusoidal amplitude grating is generated with SLM_2, the FT is performed via the lens L_1, and filtering is subsequently performed via SLM_3. The multiplexing operation is generated by SLM_4. Next, the final multiplexed result $R(x, y)$ is generated by utilizing the L_2. Then, chaotic pixel scrambling, RPM and DMPFrFT operations are performed in a digital manner.

The proposed decryption procedure contains decryption and demultiplexing parts. The multiplexed signal $R(x, y)$ can be decrypted through the method of inverse

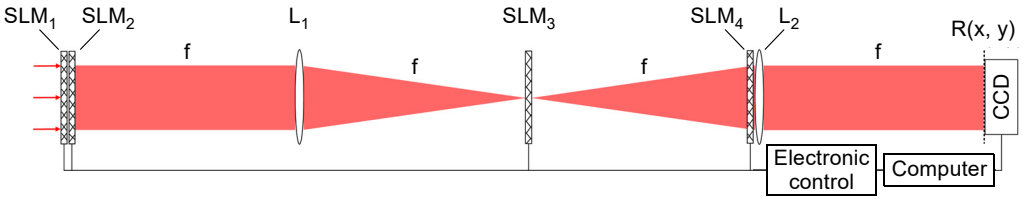

Fig. 1. Optoelectronic hybrid setup of encryption for the proposed method.

DMPFrFT, the conjugate of RPM, and inverse scrambling in sequence. The ensuing result can be expressed as

$$R(x, y) = \mathbf{SC}^{-1}_{\{a_0, \lambda, t\}} \left\{ F^{(-\alpha_L, -\alpha_R)}_{(M_L, M_R)} \left[E(x, y) \right] \exp\left[-iM(x, y) \right] \right\} \tag{6}$$

For demultiplexing, $R(x, y)$ is initially Fourier transformed to yield a spatial power spectrum. Spots containing the information of I'_j can be successively achieved from the spectrum, and then Fourier transformed back to the spatial domain to obtain I'_j. After dividing the real component and the imaginary component, each original image can again be visualized.

3. Numerical simulation and analysis

3.1. Correctness of the proposed method

To demonstrate the feasibility of the proposed method, numerical simulations were performed on 12 original images, each with 1024 × 1024 pixels and 256 gray levels, as shown in Fig. 2**a**. In the simulations, a sinusoidal amplitude grating with a spatial fre-

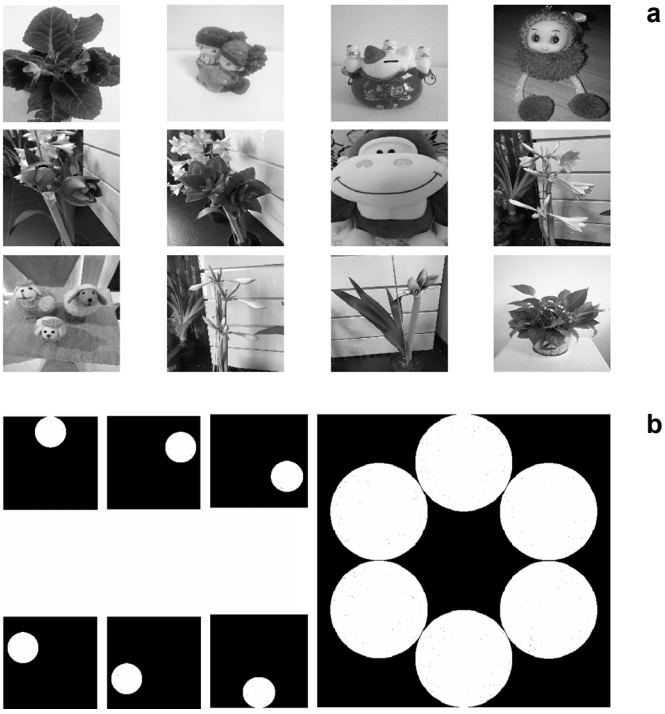

Fig. 2. Encryption and decryption results of the proposed method: (**a**) 12 original images, (**b**) results after applying complex encoding, theta modulation, and spectral fusion, (**c**) final multiplexed result, (**d**) encrypted image, (**e**) decrypted images.

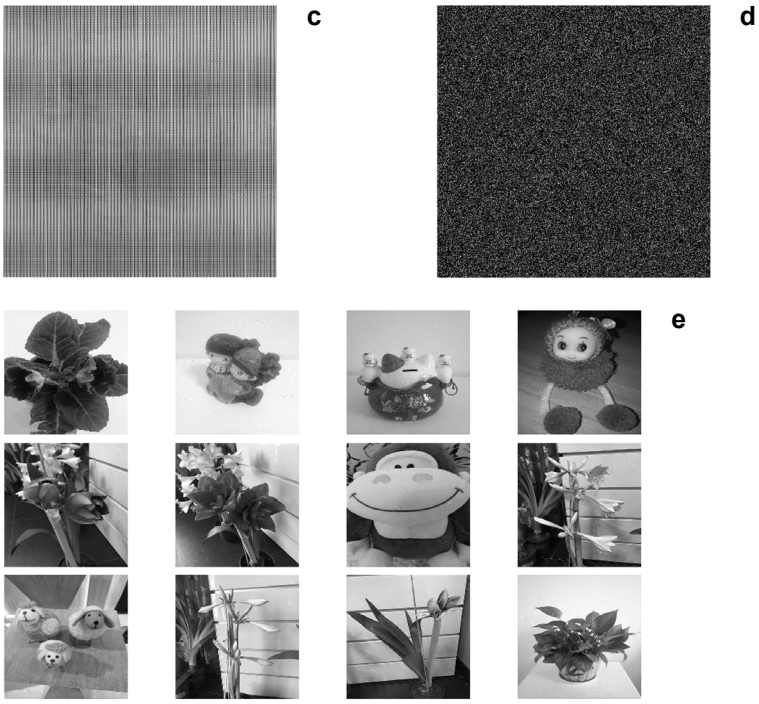

Fig. 2. Continued.

quency of 7.6×10^4 and orientation angle step of 60° was employed to modulate each image. A logistic map with an initial value of $a_0 = 0.241$, a coefficient of $\lambda = 3.95$, and a truncated position of $t = 4000$ was used to perform the scrambling operation, splitting the image into 262 144 subsections of 2 × 2 pixels. The parameters of the DMPFrFT were set as follows: periodicity $(M_L, M_R) = (15, 20)$, order $(\alpha_L, \alpha_R) = (0.34, 0.73)$, and vectors $(\mathbf{m}_L, \mathbf{n}_L)$ and $(\mathbf{m}_R, \mathbf{n}_R)$ (1 × 15 and 1 × 20 random vectors, respectively). After applying complex encoding, theta modulation, and spectral fusion, we obtained the results shown in Fig. 2**b**. Owing to complex encoding, we obtained the spectra of six complex images. By round filtering in spectral fusion, we retained the +1st-order term, namely one spot. Along with the increase in the number of original images, the radius of the round filter needed be adjusted. Subsequently, after Fourier transforming back to the spatial domain, the final multiplexed result was obtained, as shown in Fig. 2**c**. Through the operations of chaotic pixel scrambling, RPM, and DMPFrFT, we obtained an encrypted image with stationary white noise, as shown in Fig. 2**d**. It is obvious that no information from the original images could be visualized. When all the correct keys and FT were executed on the encrypted image in series, the power spectrum of the decrypted complex signal could be yielded. Then, each image could be recovered through the operation of the demultiplexing, as shown in Fig. 2**e**, and all of them could be identified.

3.2. Evaluation of the decrypted image quality

To further corroborate the proposed method, we employed the peak-signal-to-noise ratio (PSNR) [30–32] for an objective evaluation. The PSNR between the original image I and the decrypted image I_E is computed as

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left|I_E(x,y)-I(x,y)\right|^2}\right) \tag{7}$$

where M and N are the values of the corresponding frame size.

We recorded the PNSR values of different images generated by the proposed method and by the method in [22], and the results are shown in Fig. 3. Compared to [22], the proposed method doubled the number of images to be encrypted, enabling a high

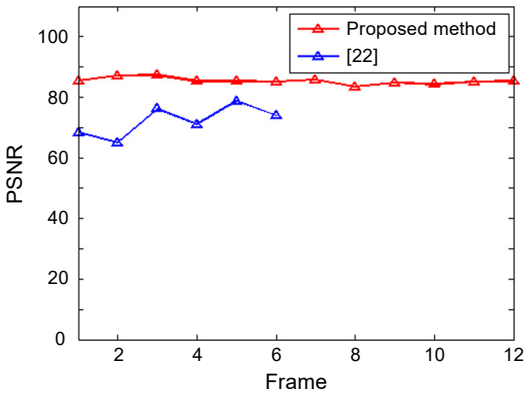

Fig. 3. PSNR for each image from the proposed method and [22].

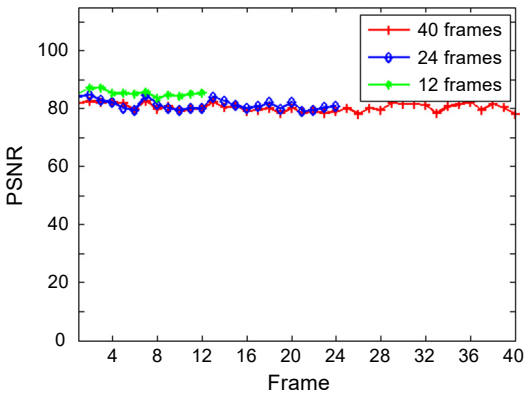

Fig. 4. PSNR for different numbers of images.

PSNR value. We also implemented a runtime comparison in MATLAB, in which the time required for both encryption and decryption was calculated. The results show that the proposed method required 15.2 s, whereas the method in [22] required 14.7 s. It is clear that with double encryption capability and good decrypted image quality, the proposed method was just a little slower than [22]. Stated differently, with the same number of images, the proposed method is faster than [22].

Along with an increase in the number of images, the reconstructed quality may decrease to certain extent. Thus, we also demonstrated our method with PSNR curves with total numbers of 12, 24, and 40, and the results are shown in Fig. 4. It can be seen that the PSNR is inversely proportional to the number of images to be encrypted, and the PSNR values of all the three curves are above 77 dB.

3.3. Sensitivity of the keys

Further, we analyzed the influence of the deviation of the different keys on the reconstructed images when other keys were correct. Figures 5**a**–5**c** show images reconstructed with an incorrect inverse scrambling operation (initial value $a_0 = 0.24$, coefficient $\lambda = 3.94$, truncated position $t = 4001$). Figure 5**d** shows images reconstructed with an incorrect conjugate RPM. Figures 5**e**–5**h** show images reconstructed with incorrect

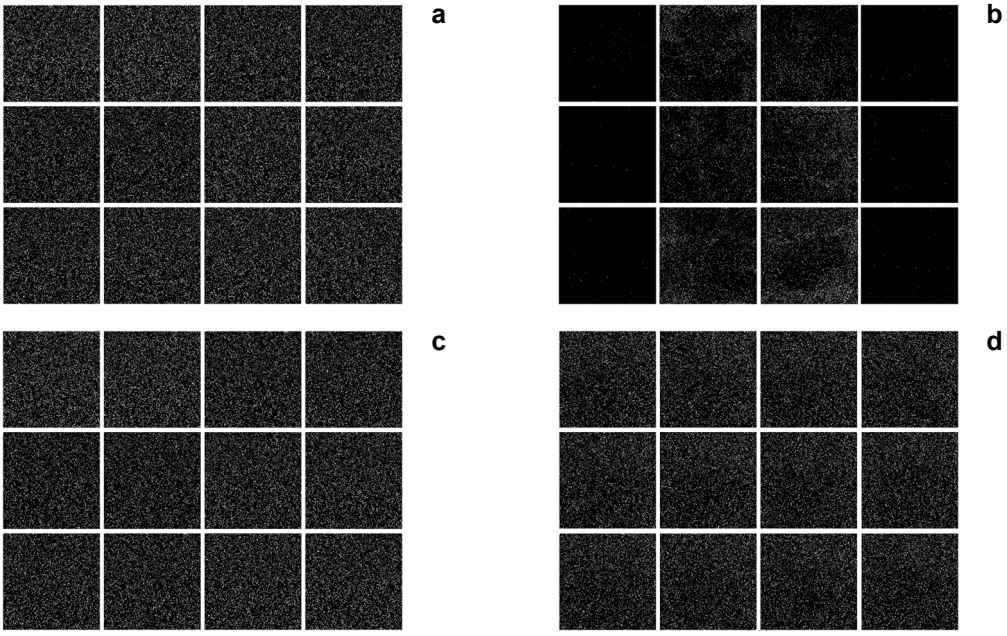

Fig. 5. Reconstructed images with incorrect values: (**a**) initial value of inverse scrambling operation $a_0 = 0.24$, (**b**) coefficient of inverse scrambling operation $\lambda = 3.94$, (**c**) truncated position of inverse scrambling operation $t = 4001$, (**d**) RPM, (**e**) periodicity of DMPFrFT $(M_L, M_R) = (16, 21)$, (**f**) order of DMPFrFT $(\alpha_L, \alpha_R) = (-0.34 + 10^{-8}, -0.73 + 10^{-7})$, vectors of DMPFrFT (**g**) $(\mathbf{m}_L - 1, \mathbf{n}_L - 1)$, (**h**) $(\mathbf{m}_R + 1, \mathbf{n}_R + 1)$.

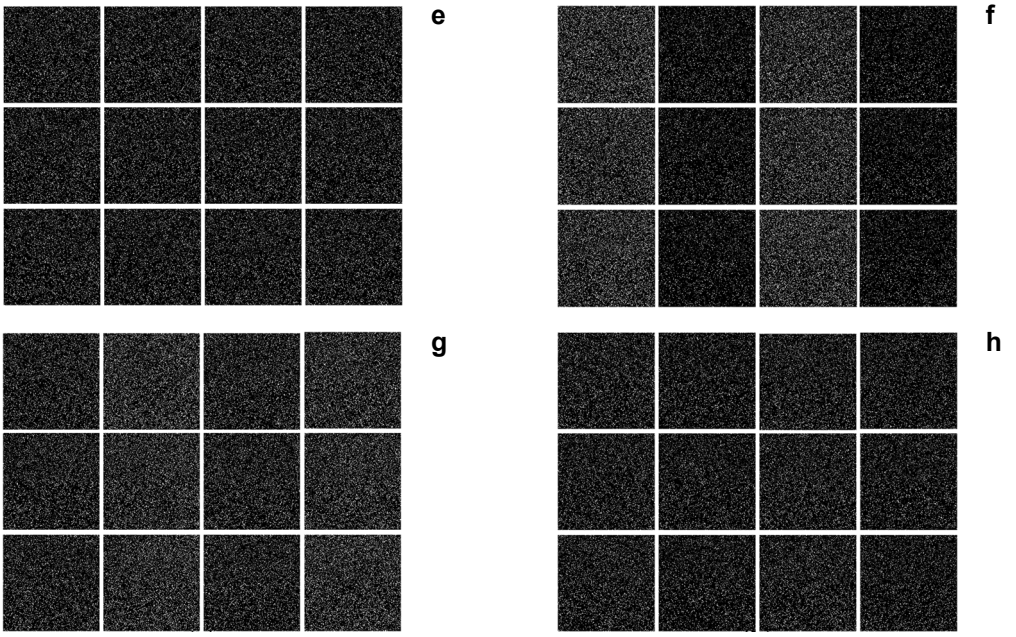

Fig. 5. Continued.

keys of DMPFrFT (periodicity (M_L, M_R) = (16, 21), order (α_L, α_R) = ($-0.34 + 10^{-8}$, $-0.73 + 10^{-7}$), vectors ($\mathbf{m}_L - 1$, $\mathbf{n}_L - 1$) and ($\mathbf{m}_R + 1$, $\mathbf{n}_R + 1$)). It is obvious that small deviations to the previously mentioned keys lead to non-visible images, ensuring a high level of security.

3.4. Occlusion and noise attacks

Furthermore, we evaluated the robustness of the proposed method to occlusion and noise attacks. The mean squared error (MSE) is expressed as

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left| I_E(x, y) - I(x, y) \right|^2 \tag{8}$$

where I_E, I, M, and N have the same definition as the PSNR.

Figure 6**a** shows an encrypted image occluded by 10%, and Fig. 6**b** shows the reconstructed images of Fig. 6**a** with all the correct keys. Figure 6**c** shows an encrypted image occluded by 15%, and Fig. 6**d** shows the reconstructed images of Fig. 6**c** with all the correct keys. Figure 7 shows the MSE values of Figs. 6**b** and 6**d**. The average MSE values with 10% and 15% occlusion were 0.0352 and 0.0546, respectively. Figure 8**a** shows an encrypted image polluted with zero-mean white additive Gaussian noise of standard deviation 0.05, and Fig. 8**b** shows reconstructed images of Fig. 8**a** with all the correct keys. Figure 8**c** shows an encrypted image polluted with zero-mean

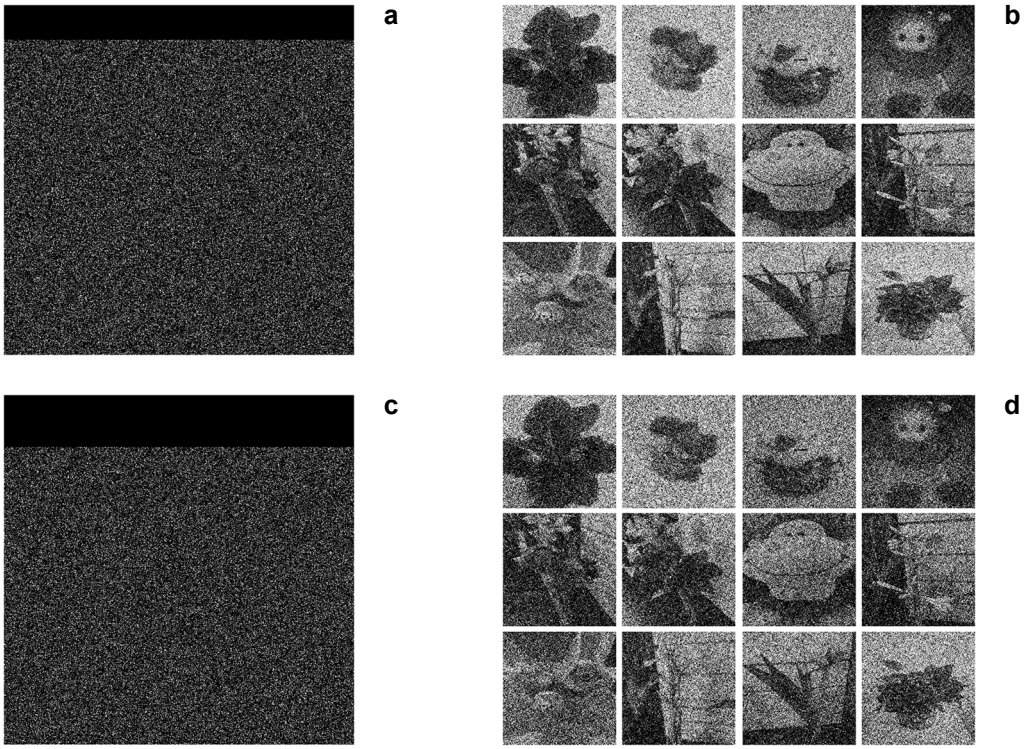

Fig. 6. Robustness to occlusion attacks: (**a**) encrypted image with 10% occlusion, (**b**) reconstructed images from **a**, (**c**) encrypted image with 15% occlusion, (**d**) reconstructed images from **c**.

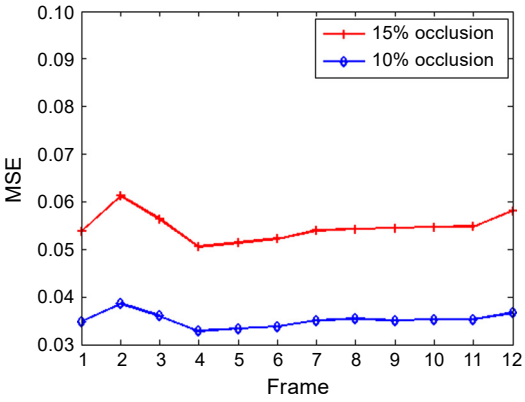

Fig. 7. MSE with 10% and 15% occlusion.

white additive Gaussian noise of standard deviation 0.1, and Fig. 8**d** shows reconstructed images of Fig. 8**c** with all the correct keys. Figure 9 shows the MSE values of Figs. 8**b** and 8**d**. The average MSE values with Gaussian noise of standard deviation 0.05 and 0.1 were 0.0020 and 0.0072, respectively.

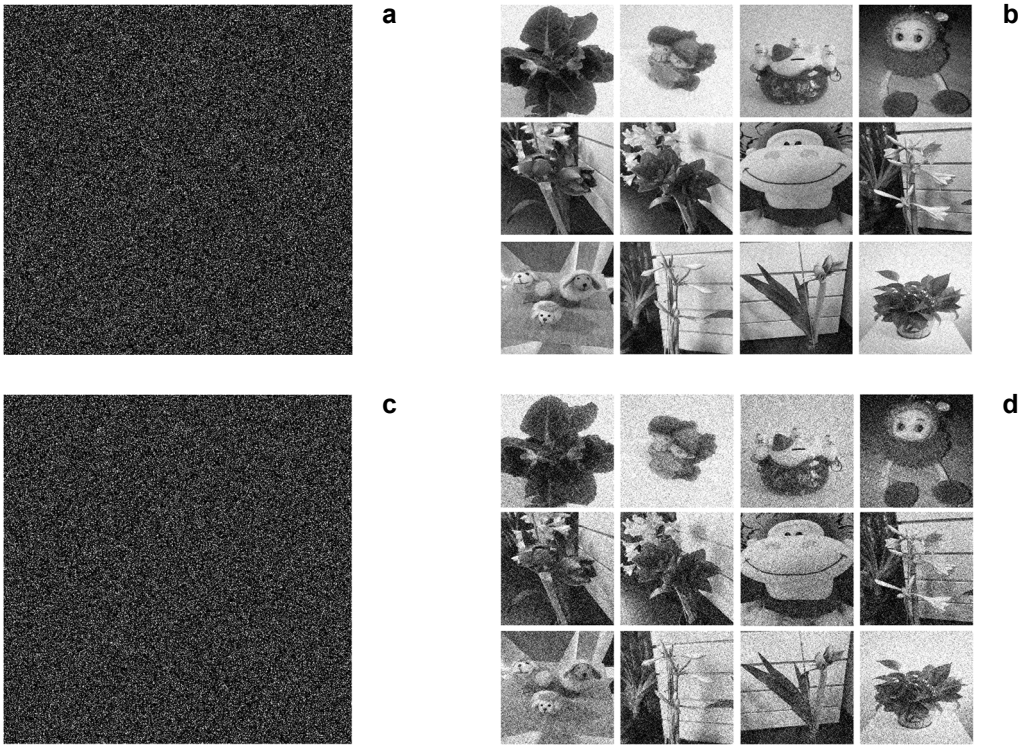

Fig. 8. Robustness to noise attacks: (**a**) encrypted image with Gaussian noise of standard deviation 0.05, (**b**) reconstructed images from **a**, (**c**) encrypted image with Gaussian noise of standard deviation 0.1, (**d**) reconstructed images from **c**.

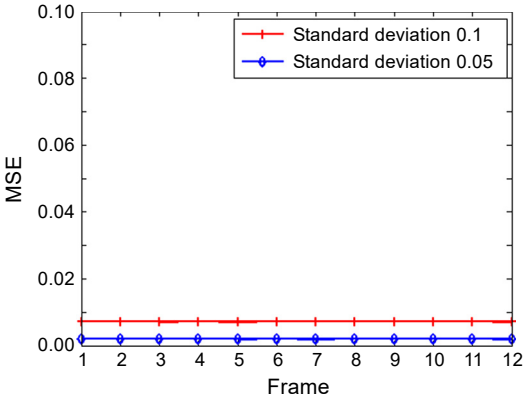

Fig. 9. MSE with Gaussian noise of standard deviation 0.05 and 0.1.

All the results regarding occlusion and noise attacks reveal that even if attacks on the reconstructed images lead to a certain decrease in quality, the images can be identified unambiguously. Thus, the proposed method is robust to image pollution.

4. Conclusion

We proposed a new multiple-image encryption method for the DMPFrFT scheme, using complex encoding, theta modulation, and spectral fusion. Complex encoding is used to encode all pairs of original images separately into a complex signal. Using the combination of theta modulation and spectral fusion, the spectrum of each complex signal can then be scattered and multiplexed into one spectral image, and the multiplexed signal that is transformed back to the spatial domain is encrypted in DMPFrFT domain. To the best of the authors' knowledge, this is the first time that complex encoding, theta modulation and spectral fusion have been integrated into DMPFrFT scheme. The proposed method solves the crosstalk problem among multiple images and improves the multiplexing capacity of multiple images for convenient transmission and storage. Moreover, the security of the proposed method is further enhanced with the parameters of chaotic pixel scrambling, and the proposal resists certain attacks. Numerical simulations were performed to vindicate the performance of the proposed method.

Acknowledgment – This research was funded by the Education Department Foundation of Heilongjiang Province of China (12541584) and by the Natural Science Foundation of Heilongjiang Province of China (C2018050).

References

[1] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[2] Qin Y., Gong Q., Wang Z.P., *Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme*, Optics Express **22**(18), 2014, pp. 21790–21799, DOI: 10.1364/OE.22.021790.

[3] Kumar R., Bhaduri B., *Optical image encryption in Fresnel domain using spiral phase transform*, Journal of Optics **19**(9), 2017, article 095701, DOI: 10.1088/2040-8986/aa7cb1.

[4] Xi S.X., Wang X.L., Song L.P., Zhu Z.Q., Zhu B.W., Huang S., Yu N.N., Wang H.Y., *Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram*, Optics Express **25**(7), 2017, pp. 8212–8222, DOI: 10.1364/OE.25.008212.

[5] Deng X.P., Zhu X., *A simple and practical color image encryption with the help of QR code*, Optica Applicata **45**(4), 2015, pp. 513–521, DOI: 10.5277/oa150407.

[6] Ren G.H., Han J.A., Fu J.H., Shan M.G., *Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform*, Optical Review **25**(6), 2018, pp. 701–707, DOI: 10.1007/s10043-018-0464-x.

[7] Lang J., Tao R., Wang Y., *Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function*, Optics Communications **283**(10), 2010, pp. 2092–2096, DOI: 10.1016/j.optcom.2010.01.060.

[8] He W.Q., Peng X., Meng X.F., *Optical multiple-image hiding based on interference and grating modulation*, Journal of Optics **14**(7), 2012, article 075401, DOI: 10.1088/2040-8978/14/7/075401.

[9] Sui L.S., Zhou B., Ning X.J., Tian A.L., *Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain*, Optics Express **24**(1), 2016, pp. 499–515, DOI: 10.1364/OE.24.000499.

[10] HUANG J.J., HWANG H.E., CHEN C.Y., CHEN C.M., *Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain*, Optics and Laser Technology **44**(7), 2012, pp. 2238–2244, DOI: 10.1016/j.optlastec.2012.02.032.

[11] CHEN W., *Optical multiple-image encryption using three-dimensional space*, IEEE Photonics Journal **8**(2), 2016, article 6900608, DOI: 10.1109/JPHOT.2016.2550322.

[12] SUI L.S., ZHANG X., HUANG C.T., TIAN A.L., ASUNDI A.K., *Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms*, Optics and Lasers in Engineering **113**, 2019, pp. 29–37, DOI: 10.1016/j.optlaseng.2018.10.002.

[13] CHEN Q., SHEN X.J., *Multiple images encryption method via spiral phase mask rotations under a JTC system*, Journal of Modern Optics **66**(5), 2019, pp. 486–493, DOI: 10.1080/09500340.2018.1548664.

[14] JOSHI M., CHANDRASHAKHER, SINGH K., *Color image encryption and decryption for twin images in fractional Fourier domain*, Optics Communications **281**(23), 2008, pp. 5713–5720, DOI: 10.1016/j.optcom.2008.08.024.

[15] DEEPAN B., QUAN C., WANG Y., TAY C.J., *Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique*, Applied Optics **53**(20), 2014, pp. 4539–4547, DOI: 10.1364/AO.53.004539.

[16] GONG Q., LIU X.Y., LI G.Q., QIN Y., *Multiple-image encryption and authentication with sparse representation by space multiplexing*, Applied Optics **52**(31), 2013, pp. 7486–7493, DOI: 10.1364/AO.52.007486.

[17] SUI L.S., XIN M.T., TIAN A.L., *Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain*, Optics Letters **38**(11), 2013, pp. 1996–1998, DOI: 10.1364/OL.38.001996.

[18] ZHAO H.Z., LIU J., JIA J., ZHU N., XIE J.H., WANG Y.T., *Multiple-image encryption based on position multiplexing of Fresnel phase*, Optics Communications **286**, 2013, pp. 85–90, DOI: 10.1016/j.optcom.2012.08.056.

[19] WANG H.J., QIN Y., HUANG Y.D., WANG Z.P., ZHANG Y.Y., *Multiple-image encryption and authentication in interference-based scheme by aid of space multiplexing*, Optics and Laser Technology **95**, 2017, pp. 63–71, DOI: 10.1016/j.optlastec.2017.04.019.

[20] MOSSO F., BARRERA J.F., TEBALDI M., BOLOGNINI N., TORROBA R., *All-optical encrypted movie*, Optics Express **19**(6), 2011, pp. 5706–5712, DOI: 10.1364/OE.19.005706.

[21] DU X.J., TAO S.H., *All-optical encrypted movie based on fractional Fourier transform*, Guangxue Jishu/Optical Technique **39**(1), 2013, pp. 68–71.

[22] ZHONG Z., ZHANG Y.J., SHAN M.G., WANG Y., ZHANG Y.B., XIE H., *Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform*, Journal of Optics **16**(12), 2014, article 125404, DOI: 10.1088/2040-8978/16/12/125404.

[23] ALFALOU A., BROSSEAU C., *Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption*, Optics Letters **35**(11), 2010, pp. 1914–1916, DOI: 10.1364/OL.35.001914.

[24] ALFALOU A., BROSSEAU C., ABDALLAH N., JRIDI M., *Simultaneous fusion, compression, and encryption of multiple images*, Optics Express **19**(24), 2011, pp. 24023–24029, DOI: 10.1364/OE.19.024023.

[25] QIN Y., GONG Q., WANG Z.P., WANG H.J., *Optical multiple-image encryption in diffractive-imaging -based scheme using spectral fusion and nonlinear operation*, Optics Express **24**(23), 2016, pp. 26877 –26886, DOI: 10.1364/OE.24.026877.

[26] DENG P.K., DIAO M., SHAN M.G., ZHONG Z., ZHANG Y.B., *Multiple-image encryption using spectral cropping and spatial multiplexing*, Optics Communications **359**, 2016, pp. 234–239, DOI: 10.1016/j.optcom.2015.09.056.

[27] PEI S.C., HSUE W.L., *The multiple-parameter discrete fractional Fourier transform*, IEEE Signal Processing Letters **13**(6), 2006, pp. 329–332, DOI: 10.1109/LSP.2006.871721.

[28] LANG J., TAO R., WANG Y., *The discrete multiple-parameter fractional Fourier transform*, Science China Information Sciences **53**(11), 2010, pp. 2287–2299, DOI: 10.1007/s11432-010-4095-5.

[29] TAO R., LANG J., WANG Y., *Optical image encryption based on the multiple-parameter fractional Fourier transform*, Optics Letters **33**(6), 2008, pp. 581–583, DOI: 10.1364/OL.33.000581.

[30] ALFALOU A., BROSSEAU C., ABDALLAH N., *Simultaneous compression and encryption of color video images*, Optics Communications **338**, 2015, pp. 371–379, DOI: 10.1016/j.optcom.2014.10.020.

[31] ALSAEDI M., *Colored image encryption and decryption using multi-chaos 2D quadratic strange attractors and matrix transformations*, Multimedia Tools and Applications **76**(22), 2017, pp. 24527–24547, DOI: 10.1007/s11042-016-4206-4.

[32] DI H., KANG Y.M., LIU Y.Q., ZHANG X., *Multiple image encryption by phase retrieval*, Optical Engineering **55**(7), 2016, article 073103, DOI: 10.1117/1.OE.55.7.073103.

Received April 8, 2020