Optica Applicata, Vol. LIII, No. 3, 2023
DOI: 10.37190/oa230309

High-security image encryption by multiplexing phase encoding in domains of dual optical transforms

Zhihui Li[1], Bin Gao[1,*], Xiaoou Pan[1], Linlin Li[1], Chenxuan Wang[1], Weizhuo Zuo[1], Yu Ji[2], Shutian Liu[2], Zhengjun Liu[2]

[1]College of Data Science and Technology, Heilongjiang University, Harbin 150080, China

[2]School of Physics, Harbin Institute of Technology, Harbin 150001, China

[*]Corresponding author: gaobin@hlju.edu.cn

A novel optical image encryption is proposed based on multiplexing of the random phase encoding with shift and rotation operations in domains of two transforms, extended fractional Fourier transform (eFrFT) and Fresnel transform. The original image is subjected to eFrFT with the action of the random phase mask. The mask is shifted and rotated to enhance the security of this encryption method. The image obtained from eFrFT is entered into Fresnel diffraction by the use of the phase mask to obtain the final encrypted image. We plan for the phase keys to be multiplexed in order to decrease the amount of keys that need to be stored in an application. Here, the displacement, rotation angle, and wavelength in this system can be used as additional keys to improve the security and reliability of the encryption system. Numerical experiments are conducted to verify the effectiveness and security of the method. The findings demonstrate that the keys are sufficiently sensitive for high security.

Keywords: extended fractional Fourier transform, geometric operations, random phase encoding.

1. Introduction

With the development of information technology, the safe transmission and storage of image data have become vital. Due to its great size and information processing capacity, image encryption technology has become an important means of information security, which has drawn a lot of interest. It is to reconstruct the image information that can be recognized by the naked eye into a noise-like image to achieve the purpose of protecting pattern information. The image encryption technology based on optical systems has the advantages of high-speed parallelism, a huge volume of information, a large key space, and robustness under attack, and has been swiftly developed recently.

The Fourier-domain double random phase encoding (DRPE) was proposed by REFREGIER and JAVIDI [1] and it is a classical work in the field of optical information security [2]. Since then, optical transform technology has been used to develop and expand DRPE-related optical image encryption techniques. UNNIKRISHNAN *et al*. proposed a double random phase coding algorithm based on the fractional Fourier transform with the addition of fractional order as a key [3]. SITU and ZHANG proposed image encryption based on Fresnel transform [4]. YE and ZHOU extended the optical encryption into Hartley domains [5]. CHEN *et al*. designed an encryption technology in gyrator transform domains [6]. In addition, some optical image encryption methods based on interference [7], phase recovery algorithms [8], ghost imaging [9], computational holography [10], digital holography [11], fractional discrete Meixner moments [12], diffraction imaging [13], extended fractional Fourier transform (eFrFT) [14], compressed sensing [15-17], twin decomposition [18], discrete Tchebyshev moments [19] and fractional-order laser hyperchaotic system [20] have been proposed. Here optical transforms [21] and methods for generating random data are combined to design encryption methods. These methods belong to linear operations and have potential risks. As a possible scheme to develop a new method, a cascaded encoding structure [22-26] can enhance security in an optical information hiding system.

As a way of obtaining random data, chaotic systems are used in a variety of image encryption algorithms because of their excellent properties such as high sensitivity to initial values and parameters, hybridization, fast decaying autocorrelation, long-term unpredictability, overall stability, local instability, and pseudo-randomness. The combining optical information security technology with chaos theory [27,28] can construct a more effective and secure encryption algorithm with the advantages of high security. In optical image encryption, firstly, it is applied to dislocation operation in the image encryption process [29]; secondly, it is used to generate a chaotic random phase mask (RPM) [22,25,30]. This also offers a suggestion for the future development of image encryption that we should combine calculation strategy and optical system to improve the performance of image encryption schemes from the aspect of multi-stage operations.

In this work, we present an optical image encryption method that uses phase encoding multiplexing in the eFrFT and Fresnel domains after shifting and rotating. First, a single lens and a spherical mirror are used to accomplish optical transformation techniques. Second, to generate random phase masks, chaotic mapping is used. Then, in order to fulfil the purpose of simplifying the encryption system by using the random phase masks, random phase masks are translated and rotated. For the purpose of illustrating the effectiveness of the suggested encryption approach, some calculated results have been attained.

The rest of this paper is organized as follows. The methods for the encryption scheme are given in Section 2. The implementation process of the encryption scheme is shown in Section 3. The numerical simulation results of the encryption scheme are presented in Section 4. The summaries are listed in the final section.

2. Methods

2.1. An optical system for the proposed encryption method

In Fig. 1, an optical system of proposed encryption is shown. Here optical eFrFT [31,32] is used for constructing the optical experiment. The original image is imported by a spatial light modulator (SLM) and is converted by eFrFT with the lens L2. The beam will transit beam splitter (BS) and RPM. The RPM applied in this paper is in pure phase form. Here, RPM can be rotated and shifted for designing additional keys. In addition, RPM is employed twice for phase encoding. The mirror M1 is to finish the second eFrFT via the reflection structure. The output of the transform is diffracted through BS and enters the charge-coupled device (CCD). And a reference beam is utilized to record the phase distribution of the diffraction pattern. The received random pattern will be regarded as the encrypted image of this method. All distance parameters are marked in Fig. 1.

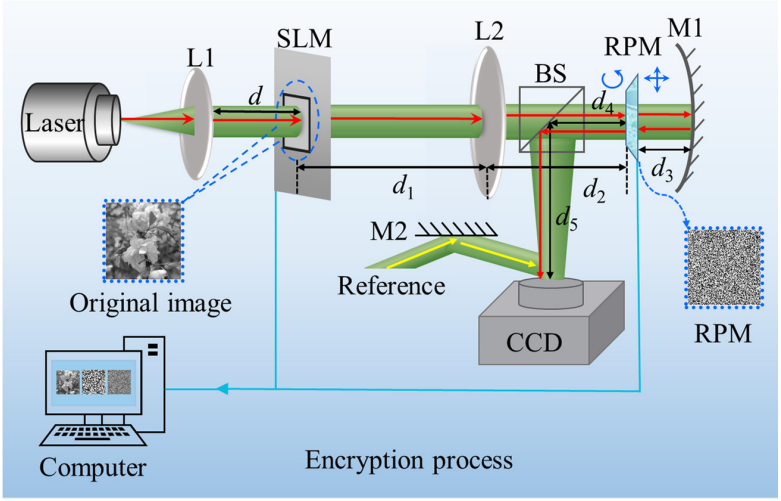

Fig. 1. An optoelectronic hybrid system to implement image encryption process. SLM: spatial light modulator; BM: beam splitter; RPM: random phase mask; L1, L2: lens; M1, M2: mirror.

2.2. Improved Hénon map

The Hénon map [33,34] is a well-known two-dimensional discrete-time system. To further guarantee the security of the system, the Hénon map is improved to operate on the random phase masks after translational and rotational transformations. Its improved version is defined as

$$\begin{cases} x_{n+1} = \left\lfloor \left| (y_n + 1 - \alpha_1 x_n^2) u \right| \right\rfloor \\ y_{n+1} = \left\lfloor \left| \beta_1 x_n v \right| \right\rfloor \end{cases} \tag{1}$$

where α_1 and β_1 are the external control parameters and n is an integer. When $\alpha_1 = 1.4$ and $\beta_1 = 0.3$, the system appears as a strange attractor and is in a chaotic state. The u and v are scaling multipliers based on the size of the original image. From Eq. (1), the x and y sequences can be generated. Then the variable pair (x, y) is mapped as coordinate values from the first random phase mask to the second random phase mask. The initial value of x is determined by the displacement associated with the translational transformation, and the initial value of y is determined by the rotation angle, as shown in Eq. (2), where h and w are the height and width of the original image, respectively. θ is the rotation angle, and $(\Delta x, \Delta y)$ is the displacement. This process further increases the sensitivity of the key and thus the security of the optical system.

$$\begin{cases} x = \dfrac{\Delta x}{2h} + \dfrac{\Delta y}{2w} \\ y = \theta/180 \end{cases} \tag{2}$$

3. Proposed scheme

3.1. Image encryption scheme

As can be seen from Fig. 2, the L2 lens is used for the optical implementation of the first eFrFT. The second eFrFT in the experiment is implemented by the spherical mirror M1, which is in front of the RPM produced by Lozi mapping [35]. The RPM can

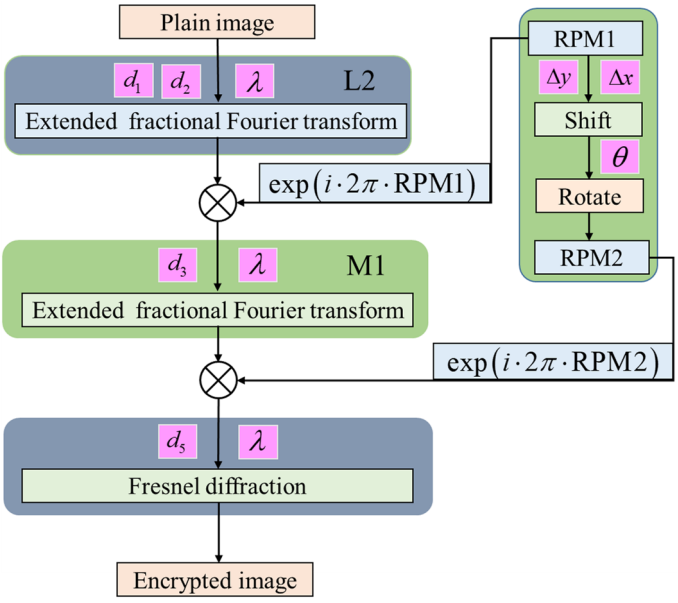

Fig. 2. Schematic diagram of the encryption process.

be shifted and rotated when recording images. This process is implemented by using interpolation on a computer for simulation.

By using the lens L1 and spatial light modulator (SLM), the original image $I(x, y)$ is encoded and irradiated by a uniform beam and placed in the input plane of eFrFT composed of a single lens system. The diffraction process can be expressed as

$$I_0(x_0, y_0) = F_{d,\lambda}[I(x, y)] \tag{3}$$

Here d is the distance from L1 to SLM and λ is the wavelength. Then continued to propagate a distance d_1, the beam passes through a lens L2 and again propagates a distance d_2 to reach the output plane. This process can be addressed as

$$I_1(x_1, y_1) = F_{d_1,\lambda}[I_0(x_0, y_0)] \tag{4}$$

After encoding the image $I_1(x_1, y_1)$ by the random phase mask, the optical field on the right side of the mask is obtained as

$$I_2(x_1, y_1) = I_1(x_1, y_1) \exp[i \cdot 2\pi \cdot \mathrm{RPM1}] \tag{5}$$

where the function RPM1 is a chaotic random phase mask generated by the Lozi mapping. It is then encoded into pure phase form, which can be expressed mathematically as $\exp[i \cdot 2\pi \cdot \mathrm{RPM1}]$. Then the second eFrFT is performed through the spherical mirror M1 to reach the output plane and can be written as

$$I_3(x_2, y_2) = F_{d_3,\lambda}[I_2(x_1, y_1)] \tag{6}$$

Encoding again with the RPM, the light field on the left side of the mask is given as follows:

$$I_4(x_2, y_2) = I_3(x_2, y_2) \exp[i \cdot 2\pi \cdot \mathrm{RPM2}] \tag{7}$$

To obtain the RPM2, the initial RPM is first rotated and translated. Then, the improved Hénon mapping is used. It is also encoded in pure phase form. The shift parameters $(\Delta x, \Delta y)$ and rotation angle θ can be utilized as additional keys to strengthen the encryption system's security. Following the BS operation, the beam propagates to the CCD plane at a distance of d_5, where it finally acquires an encrypted image. It is listed as

$$I_5(x_3, y_3) = F_{d_5,\lambda}[I_4(x_2, y_2)] \tag{8}$$

3.2. Image decryption scheme

The decryption process is the opposite of the encryption process; in order to have the right decrypted image, the proposed scheme must have the right key (RPM, wavelength, shift parameter, and rotation angle) and other right physical characteristics. The flowchart of the decryption process is shown in Fig. 3.

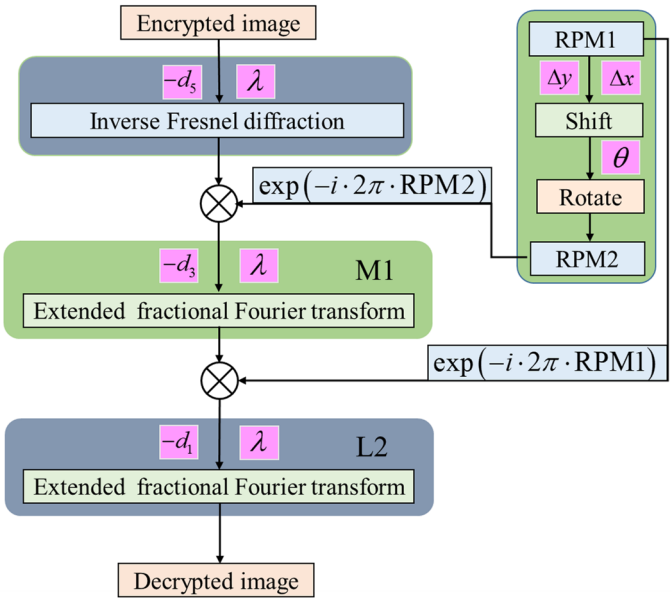

Fig. 3. Schematic diagram of the decryption process.

Firstly, the encrypted image $I_1'(x_2, y_2)$ can be obtained by inverse Fresnel diffraction transformation as

$$I_4'(x_2, y_2) = F_{-d_5, \lambda}[I_5(x_3, y_3)] \tag{9}$$

After modulating $I_4'(x_2, y_2)$ and the complex conjugate encoding of the random phase mask $R_2(x_2, y_2)$ obtained through shift and rotation transformation, $I_3'(x_2, y_2)$ is obtained as shown in the following formula

$$I_3'(x_2, y_2) = I_4'(x_2, y_2)\exp[-i\cdot 2\pi\cdot \mathrm{RPM2}] \tag{10}$$

By implementing the inverse eFrFT of spherical mirror M1 for $I_3'(x_2, y_2)$, and the expression can be obtained as

$$I_2'(x_1, y_1) = F_{-d_3, \lambda}[I_3'(x_2, y_2)] \tag{11}$$

After the complex conjugate encoding of $I_2'(x_1, y_1)$ and the initial RPM $R_1(x_1, y_1)$, the expression can be shown as

$$I_1'(x_1, y_1) = I_2'(x_1, y_1)\exp[-i\cdot 2\pi\cdot \mathrm{RPM1}] \tag{12}$$

The decrypted image is obtained by eFrFT of lens L2 on $I_1'(x_1, y_1)$ as

$$I_0(x_0, y_0) = F_{-d_1, \lambda}[I_1'(x_1, y_1)] \tag{13}$$

4. Numerical simulation and analysis

Several tests are conducted in this part to assess the efficacy of our suggested encryption scheme. The physical parameters used for encryption and their values are listed in Table 1, where λ is the wavelength, d_1, d_2, and d_3 are the distance parameters for performing eFrFT; d_5 is the distance of Fresnel diffraction; θ and $(\Delta x, \Delta y)$ are the rotation angle and shift parameters of RPM. In this paper, RPM is presented in the plural form.

T a b l e 1. The physical parameters in the encryption system.

Parameters	Values	Parameters	Values
λ	632.8 nm	d_2	20 cm
θ	$\pi/6$	d_3	10 cm
$(\Delta x, \Delta y)$	(30 px, 50 px)	d_4	20 cm
d_1	30 cm	d_5	40 cm

As can be seen from Fig. 4, the four original secret images and the RPM are 256 × 256 grayscale images. Their corresponding encrypted image is shown in Fig. 5. As can be seen from Fig. 5, the encrypted image resembles the noise and hides the information of the original image very well. The decryption results of the four ciphertext images are listed in Fig. 6, which are consistent with the original images. As a result, the scheme effectively encrypts and decrypts the original image.

In the numerical simulation, the images from Fig. 4 are used as the original images to be encrypted for the security analysis of the algorithm. The algorithm is assessed in

Fig. 4. (a)–(d) Four original grayscale images, (e) RPM.

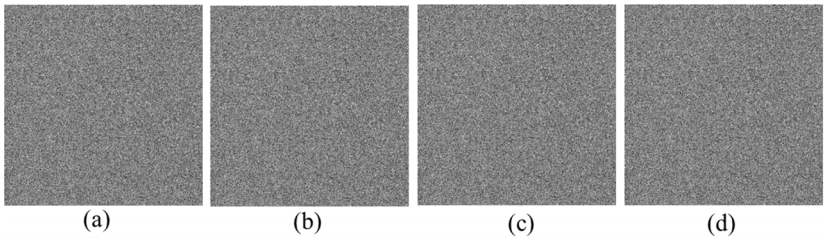

Fig. 5. Four encrypted images.

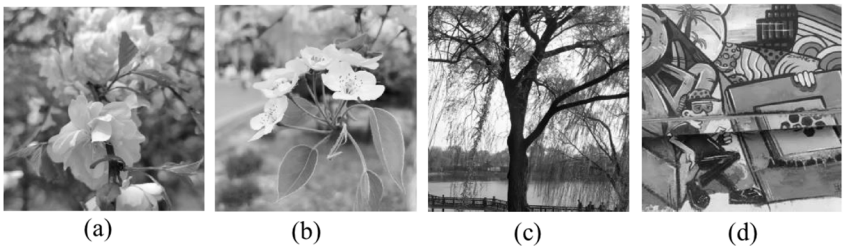

Fig. 6. Four decrypted images.

terms of key sensitivity, noise resistance, and cropping resistance by using the mean square error (MSE) function, and the correlation coefficient (CC). In addition, the anti-statistical analysis is tested by histograms, information entropy, and inter-adjacent pixel correlation to represent.

4.1. Histogram analysis

The grayscale values' statistical correlation characteristics are described by the histogram. Ideally, the encryption algorithm can resist the histogram statistical analysis attack, when the histogram distribution of the ciphertext image is consistent. We acquire the grayscale histograms of the original and ciphertext images following simulation to evaluate the suggested encryption method. As demonstrated in Figs. 7(a)–(d), the

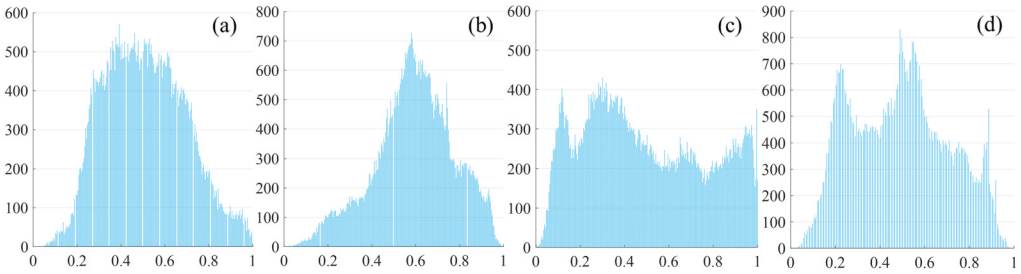

Fig. 7. Histograms of the original image.

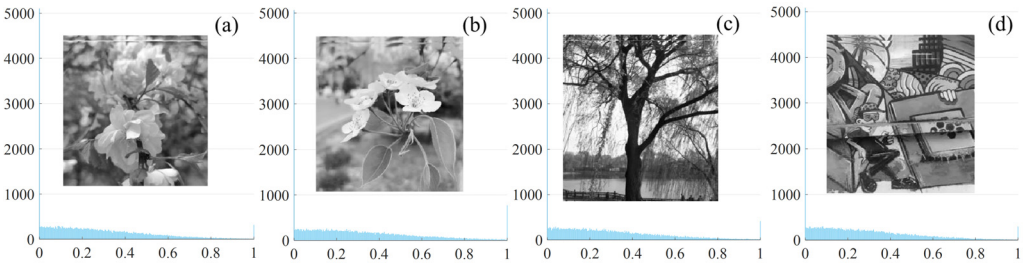

Fig. 8. Histograms of the encrypted image.

histogram distributions of the four original images under test differ and include some pixel information of the respective images with obvious statistical patterns. While the histogram distributions of the corresponding four ciphertext images are uniform and almost identical in appearance, there are no similarities with the original images, as shown in Figs. 8(a)–(d). As a result, it is difficult for the attacker to obtain effective information through the statistical analysis route.

4.2. Entropy analysis

Entropy analysis is a measure of the randomness of the information [36] and calculates the spread of each gray-level pixel in the image. The amount of confusion or ambiguity in information is measured by something called information entropy. In image encryption, a higher information entropy indicates a more uniform distribution of pixel values in an image, so it is the more difficult for an attacker to crack it. The entropy value of a good encryption method [12] is near to 8, whereas that of a bad encryption method is close to 0. Ciphertext images with entropy values close to 8 indicate better performance of the encryption algorithm. As can be seen, the information entropy $H(x)$ is calculated as

$$H(s) = -\sum_{i=0}^{N-1} P(s_i) \log_2 P(s_i) \tag{14}$$

where $P(s_i)$ represents the probability of occurrence of gray value i. In this paper, the images are normalized and their grayscale values are between 0 and 1, so the grayscale histogram is used to count their probabilities during the calculation. The four grayscale images and their entropy values are displayed in Fig. 9. The data tested here are respectively changed to $\lambda = 632.81$ nm, $\theta = 50$, $(\Delta x, \Delta y) = (20, 50)$ based on the original parameters. As can be seen from Fig. 9, all entropy values are greater than 7.6, which

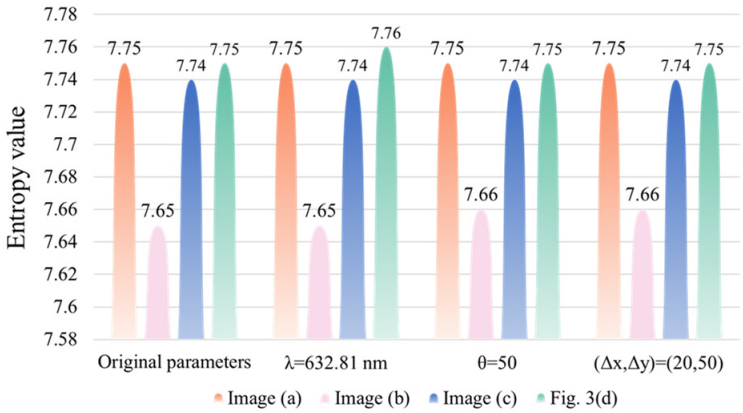

Fig. 9. Entropy values of four images.

is close to the ideal value of 8. This indicates that the ciphertext images have strong randomness and conceal any useful plaintext information. It can withstand information entropy attacks well.

4.3. Pixel correlation analysis

Analyzing two or more variables with correlation to gauge how closely the variables are correlated is known as correlation analysis. An attacker can frequently utilize this attribute to deduce and forecast the gray value of the next pixel to recover the entire plaintext image because one pixel has a tendency to leak information about its nearby pixels. These strong correlations must be broken to avoid statistical attacks. Ordinarily, a plaintext image's nearby pixels have a correlation that is close to 1, while a ciphertext image's neighbors should have a correlation that is close to 0.

The correlation coefficient between neighboring pixels in an image is given as

$$\begin{cases} \rho(x,y) = \dfrac{|\mathrm{cov}(x,y)|}{\sqrt{D(x)}\sqrt{D(y)}} \\ E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \\ \mathrm{cov}(x,y) = \dfrac{1}{N}\sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \end{cases} \tag{15}$$

In the above equation, y is the neighboring pixel of x, N is the total number of pixels in $M \times N$ images, and $\rho(x, y)$ is the correlation between two neighboring pixels. $\mathrm{cov}(x, y)$ is the covariance at two-pixel points of x and y. $D(x)$ is the variance, $E(x)$ and $E(y)$ is the mean. In horizontal, vertical, and diagonal directions, 1000 pairs of neighboring pixels are randomly selected. The correlation pixel distribution of Fig. 4(a) in the horizontal, vertical, and diagonal directions is shown in Figs. 10(a)–(c). The cor-

T a b l e 2. Correlation coefficients of different images.

Image	Horizontal	Vertical	Diagonal
(a)	0.9744	0.9708	0.9542
	0.0077	0.0538	0.0183
(b)	0.9458	0.9652	0.9360
	0.0369	0.0262	0.0270
(c)	0.9105	0.9193	0.8444
	0.0213	0.0499	0.0362
(d)	0.8870	0.9206	0.8134
	0.0205	0.0343	0.0182

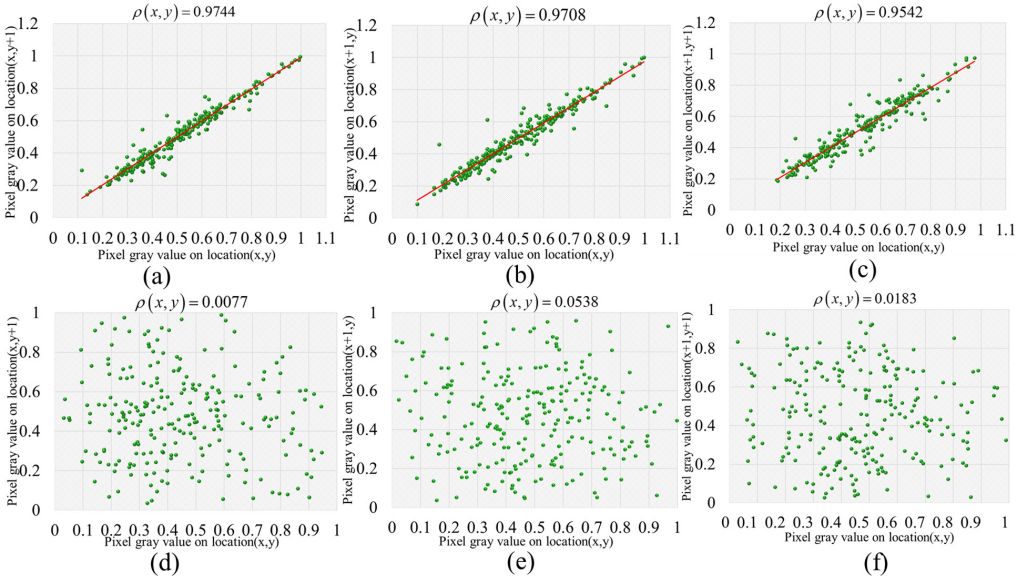

Fig. 10. The correlation plots of the original image and the corresponding encrypted image: (a) horizontal correlation of the original image, (b) vertical correlation of the original image, (c) diagonal correlation of the original image, (d) horizontal correlation of the encrypted image, (e) vertical correlation of the encrypted image, (f) diagonal correlation of the encrypted image.

relation pixel distribution of the encrypted image is shown in Figs. 10(d)–(f). The correlation coefficients of the adjacent pixels of the four grayscale images and their corresponding ciphertext images are listed in Table 2. The distribution of neighboring pixels in the original image is highly concentrated and the correlation coefficient value is close to 1, which indicates that the correlation of the original image is strong, while the distribution of neighboring pixels in the encrypted image is random and the correlation coefficient value is close to 0. As a result, this image encryption scheme can successfully prevent information leakage, making statistical analysis attacks somewhat useless against it.

4.4. Sensitivity analysis

A key indicator of an encryption system's resistance to brute-force attacks is key sensitivity. The sensitivity of the encryption scheme should be evaluated from two aspects. First, slight variations in input keys during encryption should result in entirely distinct ciphertext images; second, slight variations in the correct decryption key during decryption will not effectively recover the original image. Therefore, both the encryption and decryption processes are covered in this section.

In the encryption phase, use key sensitivity (KS) to evaluate the key sensitivity of the encryption phase. The mathematical definition of KS is

$$\mathrm{KS} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} C(m, n) \otimes C'(m, n) \times 100\% \tag{16}$$

$$C(m, n) \otimes C'(m, n) = \begin{cases} 1, & C(mn) \neq C'(m, n) \\ 0, & \text{otherwise} \end{cases} \tag{17}$$

where $M \times N$ is the total number of image pixels in the image. The range C and C' are two cipher images corresponding to the same original image, but with a small change in the key value. The sensitivity analysis of the wavelength is listed in Fig. 11. The two values of wavelength, 632.8 and 632.9 nm, are used in the test. Two ciphertext images at different wavelengths are shown in Figs. 11(a) and (b). Their difference is drawn in Fig. 11(c). Here the value of ρ is 0.0021, which is almost close to 0, and the KS values of the two ciphertext images reach 100%. It can be seen that the ciphertext image generated by key encryption is completely different with only minor changes. Therefore, key changes have a significant impact on the suggested encryption technique.

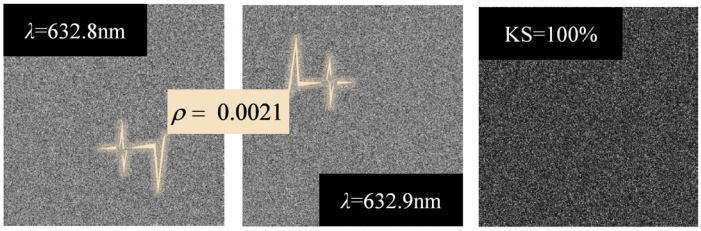

Fig. 11. Sensitivity analysis of wavelength: (a) encrypted image 1, (b) encrypted image 2, (c) difference between encrypted image 1 and encrypted image 2.

Similarly, Fig. 12 shows the various encryption outcomes with various RPMs. In this instance, the correlation coefficient between the two encrypted images is virtually zero (0.0020); its KS value is 100%. RPM is hence sensitive in this scheme's encryption stage.

In the decryption stage, MSE is used to evaluate the quality of a recovered image. MSE is defined as

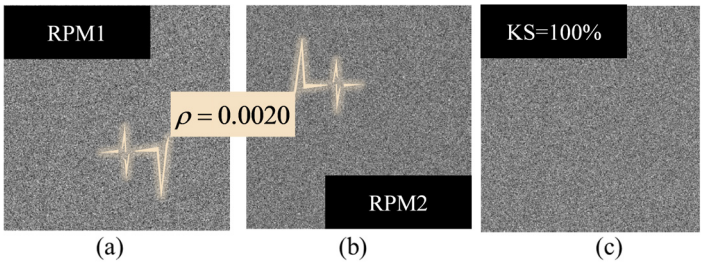

Fig. 12. Sensitivity analysis of RPM: (a) encrypted image 1, (b) encrypted image 2, (c) difference between encrypted image 1 and encrypted image 2.

$$\mathrm{MSE} = \mathrm{mse}(I_o, I_r) = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} \left| I_o(m, n) - I_r(m, n) \right|^2 \tag{18}$$

where I_o is the original image, and I_r is the recovered image. (M, N) is the size of the image. The rotation angle, shift, and wavelength parameters of random phase keys were all subjected to sensitivity analysis. The MSE plots and correlation coefficient plots for the wavelengths are presented in Figs. 13(a) and (b), respectively. Similarly, the rotation angle is shown in Figs. 14(a) and (b). Figure 15 shows the two-dimensional plot of the shift amount $(\Delta x, \Delta y)$. From Figs. 13(a) and (b), it can be seen that none of the correct decryption results can be obtained when the wavelength deviation is 0.01 nm. Figures 14(a) and (b) can be obtained that the correct decrypted image is not obtained even with a deviation of 0.01 of the rotation angle.

The results in Fig. 15 for the sensitivity of the shift parameter are likewise promising. The parameters' MSE values rise significantly and their correlation coefficient values fall sharply when they are vary marginally from the correct values. This analysis

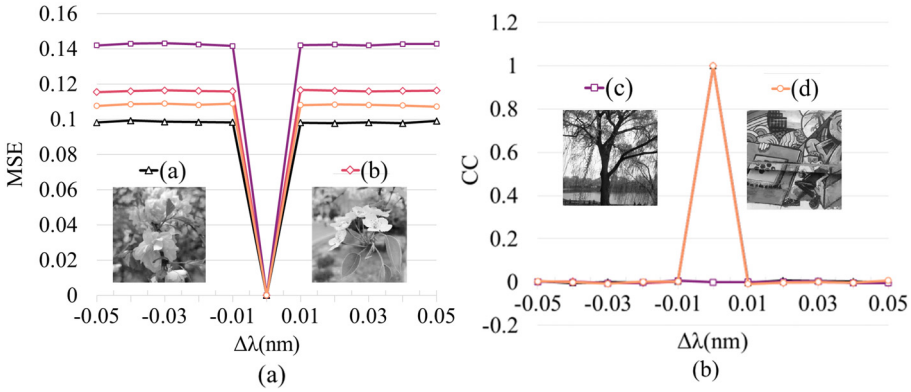

Fig. 13. Sensitivity analysis of wavelength: (a) MSE plot, (b) CC plot.

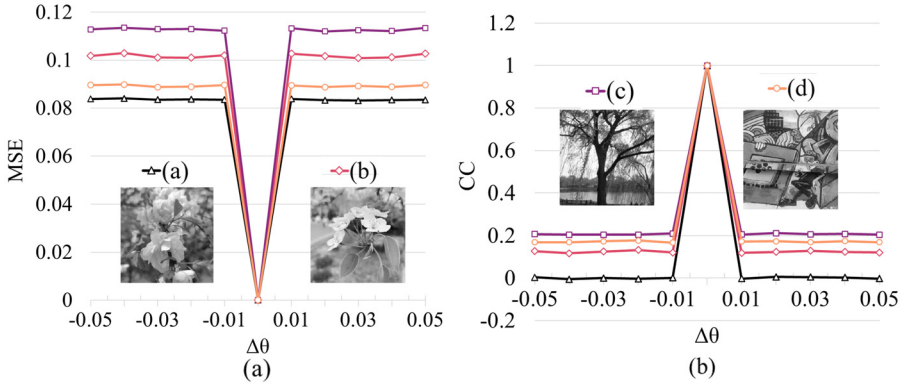

Fig. 14. Sensitivity analysis of rotation angle: (a) MSE plot, (b) CC plot.

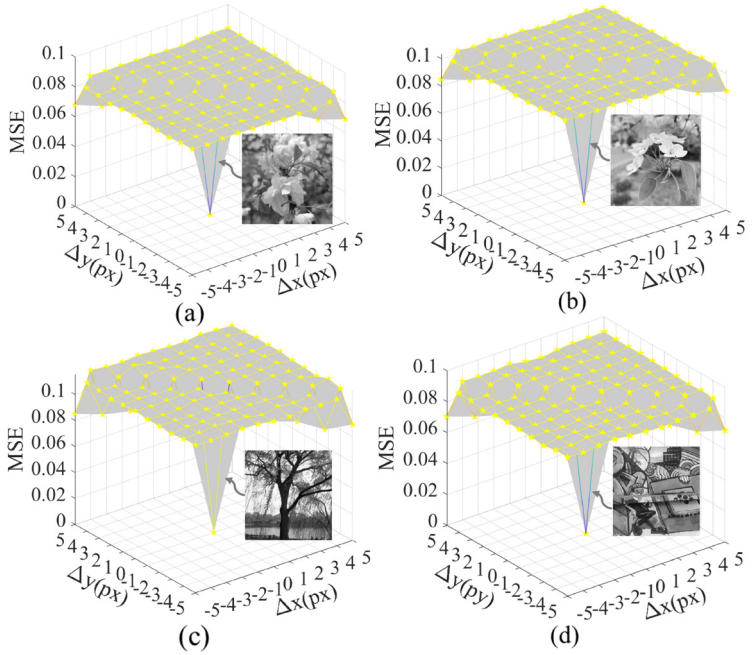

Fig. 15. Sensitivity analysis chart of displacement amount.

demonstrates that when keeping other relevant parameters constant, one of the keys cannot get the correct decrypted image in the event of deviation or error. Therefore, the proposed optical image encryption scheme proposed in this paper is sensitive to the change of key.

By altering the RPM throughout the decryption process, the decryption outcome can be seen. The decryption result graphs for a correct phase mask and an incorrect

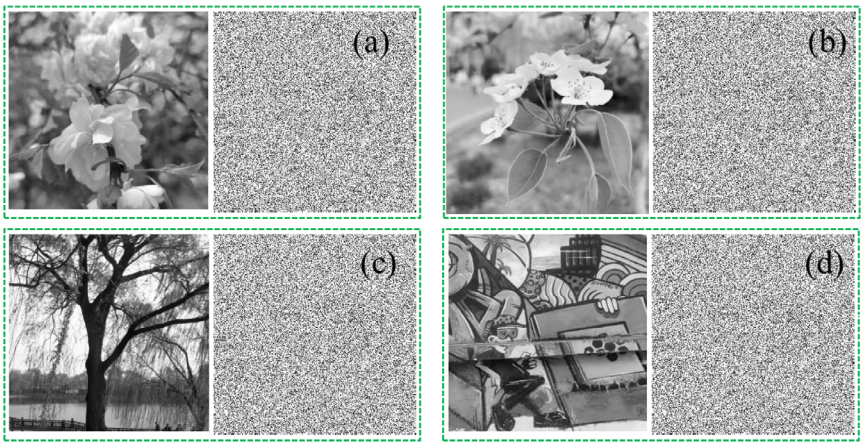

Fig. 16. Four decrypted images under different RPM.

phase mask are shown in Figs. 16(a)–(d), respectively. It is clear from the comparative results in Fig. 16 that the phase mask is sensitive enough to serve as a key.

4.5. Analysis of noise attack

The communication channels over which the image information is transferred are responsible for the addition of some noise in the form of degradation or distortion [37]. To corrupt the useful information, the attacker may introduce noise into the encrypted image so that the user cannot successfully recover the original image after decryption [38]. In this situation, it is important to know if the decryption method can still recover the essential details of the original image from the distorted ciphertext image. Therefore, we need to evaluate the robustness of the encryption algorithm in the face of noise attacks. We apply the following noise treatment to the encrypted image as

$$C' = C(1 + kG) \tag{19}$$

where C denotes the ciphertext image, C' denotes the ciphertext image affected by noise, k is the coefficient of the noise intensity, and G denotes Gaussian random noise with a mean of 0. Figures 17(a)–(f) show the decrypted images corresponding to the Gaussian noise-affected ciphertext images when the noise intensity factor is set to 0, 0.2, 0.4, 0.6, 0.8, 1.0, respectively. The MSE values of these decrypted images and the original images are 0, 0.0058, 0.0224, 0.0488, 0.0856, and 0.1347. From the simulation results obtained in Fig. 17, it can be seen that the decrypted image can be recognized even when the noise intensity reaches the maximum value of 1.0.

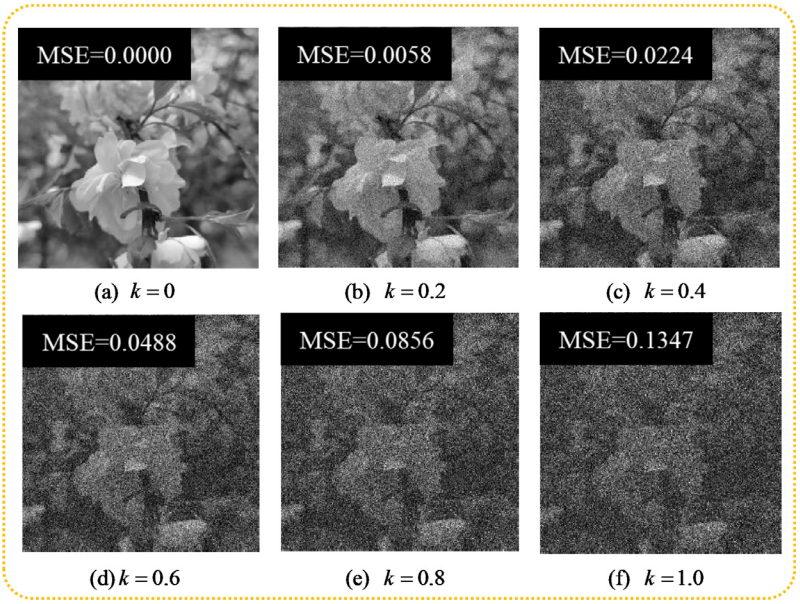

Fig. 17. Decryption results for varying Gaussian noise strength k.

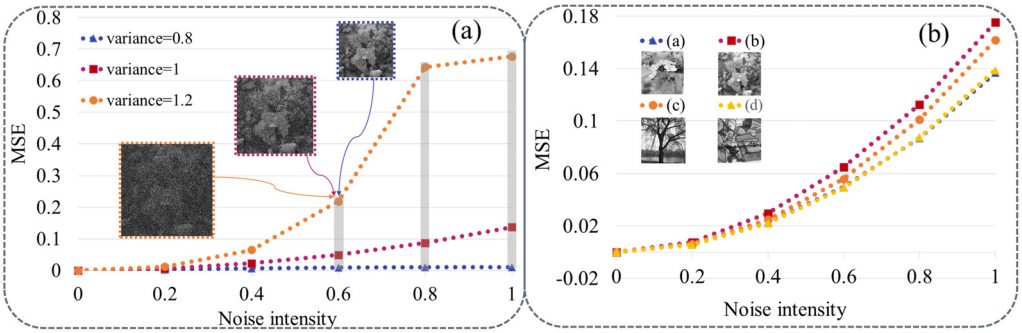

Fig. 18. (a) MSE plots for varying noise intensities with different variances, (b) MSE plots for different images with varying noise intensities.

Figure 18(a) represents the graphs of different noise intensities for a mean of 1 and variances of 0.8, 1.0, and 1.2. As can be seen, even though the decrypted image is no longer visible when the variance hits 1.2 and the noise intensity is 0.6, it still retains its fixed contour information. The four original images and their corresponding decrypted images are shown in Fig. 18(b) as MSE plots with varying noise intensities at a mean value of 0 and a variance of 1. Although the decryption effect decreases significantly after the strength of Gaussian noise is greater than 0.5, it can be seen that the algorithm has good resistance to Gaussian noise.

The correlation coefficients of the decrypted images under the influence of Gaussian noise are listed in Table 3, where the mean is 0, the variance is 1 and the noise intensity is 0.4. We can observe from the data in Table 3 that the four decrypted photos still have high quality. Therefore, it can be known that the encryption system is robust to Gaussian noise attacks.

T a b l e 3. Correlation coefficient between adjacent pixels of four decrypted images. (The tested encrypted image is Fig. 4(a)–(d) with mean 0, variance 1, and $k = 0.4$.)

Image	(a)	(b)	(c)	(d)
Horizontal	0.6222	0.5316	0.7196	0.6027
Vertical	0.5157	0.5735	0.7146	0.6563
Diagonals	0.5313	0.4467	7.7444	0.6217

4.6. Analysis of occlusion attack

The occlusion attack refers to the loss of data or cropping of a portion of an image due to noisy channels. The cryptosystem should be capable of recovering the appropriate amount of information even after some occlusion in data. An effective method to gauge an encryption system's robustness is its capacity to withstand a specific level of occlusion assault. As illustrated in Figs. 19(a1)–(c1), we simulate ciphertext pictures in this research with information loss of 12.5%, 25%, and 50% (the lost information is replaced with a 0 value). Their decrypted images are as shown in Figs. 19(a2)–(c2),

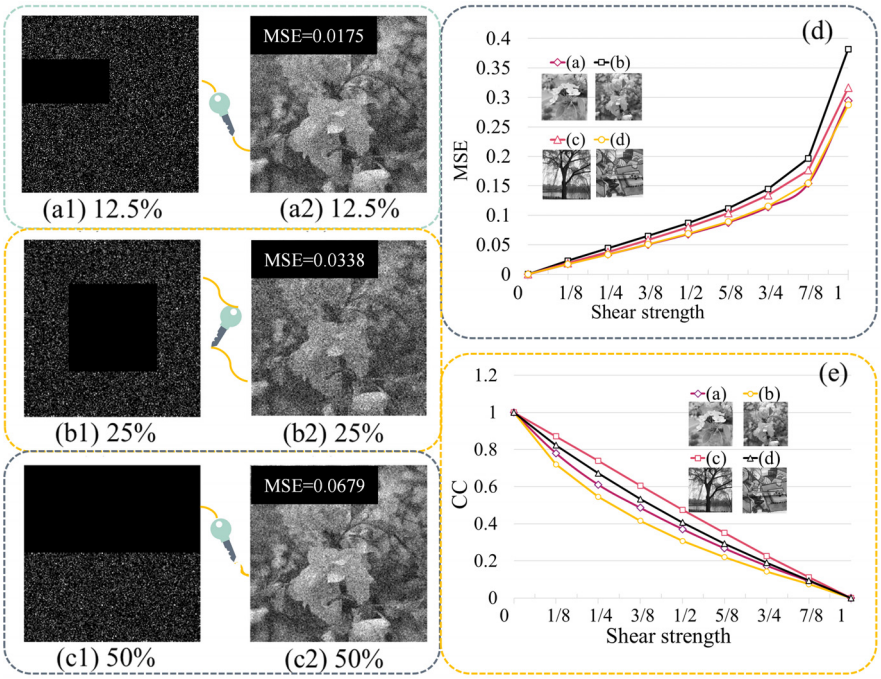

Fig. 19. Analysis chart of occlusion attack.

respectively. Figures 19(d) and (e) show the MSE plot and correlation coefficient plot under different masking strengths of four images, respectively. From the simulation results, it can be seen that the feature information of the original image can still be obtained from the decrypted image, even if some information of the ciphertext image is lost. This shows that the encryption method has strong robustness to the occlusion attack.

5. Conclusion

A new effective optical encryption system is designed using a cascaded eFrFT with the Fresnel transform. The method uses wavelength, shift parameters, and rotation angle as extra security keys to strengthen the system's security. Among them, single-lens and spherical-mirror optical systems are used to implement the eFrFT. In order to implement the chaotic random phase mask, Lozi mapping is adopted. Hénon mapping is also applied to operate on the shifted rotational transformed random phase mask, where the operation is in turn related to the wavelength, shift parameter, and rotation angle, further increasing the robustness of the encryption system. The random phase mask is multiplexed, which reduces the amount of key storage required, gets rid of the requirement to store an additional random phase mask, and makes the encryption procedure less complicated. Experimental results demonstrate the feasibility and effectiveness of the scheme.

Acknowledgment
This work was supported by the National Natural Science Foundation of China (Nos. 61975044, 12074094, 11874132); Interdisciplinary Research Foundation of HIT (No. IR2021237).

Declaration of Competing Interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767
[2] LIU S., GUO C., SHERIDAN J.T., *A review of optical image encryption techniques*, Optics & Laser Technology **57**, 2014: 327-342. https://doi.org/10.1016/j.optlastec.2013.05.023
[3] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000: 887-889. https://doi.org/10.1364/OL.25.000887
[4] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004: 1584-1586. https://doi.org/10.1364/OL.29.001584
[5] YE H.-S., ZHOU N.-R., GONG L.-H., *Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion*, Signal Processing **175**, 2020: 107652. https://doi.org/10.1016/j.sigpro.2020.107652
[6] CHEN J., ZHU Z., FU C., YU H., ZHANG L., *Gyrator transform based double random phase encoding with sparse representation for information authentication*, Optics & Laser Technology **70**, 2015: 50-58. https://doi.org/10.1016/j.optlastec.2015.01.016
[7] SUI L., ZHANG X., HUANG C., TIAN A., KRISHNA ASUNDI A., *Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms*, Optics and Lasers in Engineering **113**, 2019: 29-37. https://doi.org/10.1016/j.optlaseng.2018.10.002
[8] LIU Z., GUO C., TAN J., LIU W., WU J., WU Q., PAN L., LIU S., *Securing color image by using phase-only encoding in Fresnel domains*, Optics and Lasers in Engineering **68**, 2015: 87-92. https://doi.org/10.1016/j.optlaseng.2014.12.022
[9] SUI L., PANG Z., CHENG Y., CHENG Y., XIAO Z., TIAN A., QIAN K., ANAND A., *An optical image encryption based on computational ghost imaging with sparse reconstruction*, Optics and Lasers in Engineering **143**, 2021: 106627. https://doi.org/10.1016/j.optlaseng.2021.106627
[10] WANG W., WANG X., XU B., CHEN J., *Optical image encryption and authentication using phase-only computer-generated hologram*, Optics and Lasers in Engineering **146**, 2021: 106722. https://doi.org/10.1016/j.optlaseng.2021.106722
[11] SU Y., XU W., LI T., ZHAO J., LIU S., *Optical color image encryption based on fingerprint key and phase-shifting digital holography*, Optics and Lasers in Engineering **140**, 2021: 106550. https://doi.org/10.1016/j.optlaseng.2021.106550
[12] EL OGRI O., KARMOUNI H., SAYYOURI M., QJIDAA H., *A novel image encryption method based on fractional discrete Meixner moments*, Optics and Lasers in Engineering **137**, 2021: 106346. https://doi.org/10.1016/j.optlaseng.2020.106346
[13] GONG Q., WANG H., QIN Y., WANG Z., *Modified diffractive-imaging-based image encryption*, Optics and Lasers in Engineering **121**, 2019: 66-73. https://doi.org/10.1016/j.optlaseng.2019.03.013
[14] LIU Z., CHEN H., BLONDEL W., SHEN Z., LIU S., *Image security based on iterative random phase encoding in expanded fractional Fourier transform domains*, Optics and Lasers in Engineering **105**, 2018: 1-5. https://doi.org/10.1016/j.optlaseng.2017.12.007
[15] ZHOU N., JIANG H., GONG L., XIE X., *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018: 72-79. https://doi.org/10.1016/j.optlaseng.2018.05.014

[16] YE H.-S., DAI J.-Y., WEN S.-X., GONG L.-H., ZHANG W.-Q., *Color image encryption scheme based on quaternion discrete multi-fractional random transform and compressive sensing*, Optica Applicata **51**(3), 2021: 349-364. https://doi.org/10.37190/oa210304

[17] WAN S., GONG Q., WANG H., MA S., QIN Y., *Compressed optical image encryption in the diffractive -imaging-based scheme by input plane and output plane random sampling*, Optica Applicata **52**(1), 2022: 51-66. https://doi.org/10.37190/oa220104

[18] KUMAR J., SINGH P., YADAV A., *Asymmetric double-image encryption using twin decomposition in fractional Hartley domain*, Optica Applicata **52**(1), 2022: 21-35. https://doi.org/10.37190/oa220102

[19] DUAN C.F., ZHOU J., GONG L.H., WU J.Y., ZHOU N.R., *New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method*, Optics and Lasers in Engineering **150**, 2022: 106881. https://doi.org/10.1016/j.optlaseng.2021.106881

[20] LI X., MOU J., CAO Y., BANERJEE S., *An optical image encryption algorithm based on a fractional -order laser hyperchaotic system*, International Journal of Bifurcation and Chaos in Applied Sciences and Engineering **32**(3), 2022: 2250035. https://doi.org/10.1142/S0218127422500353

[21] NISHCHAL N.K., *Optical Cryptosystems*, IOP Publishing, UK, 2019.

[22] SU Y., TANG C., CHEN X., LI B., XU W., LEI Z., *Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map*, Optics and Lasers in Engineering **88**, 2017: 20-27. https://doi.org/10.1016/j.optlaseng.2016.07.012

[23] NISHCHAL N.K., JOSEPH J., SINGH K., *Fully phase-encrypted memory using cascaded extended fractional Fourier transform*, Optics and Lasers in Engineering **42**(2), 2004: 141-151. https://doi.org/10.1016/j.optlaseng.2003.10.004

[24] JAVIDI B., CARNICER A., YAMAGUCHI M., NOMURA T., PÉREZ-CABRÉ E., MILLÁN M.S., NISHCHAL N.K., TORROBA R., BARRERA J.F., HE W., PENG X., STERN A., RIVENSON Y., ALFALOU A., BROSSEAU C., GUO C., SHERIDAN J.T., SITU G., NARUSE M., MATSUMOTO T., JUVELLS I., TAJAHUERCE E., LANCIS J., CHEN W., CHEN X., PINKSE P.W.H., MOSK A.P., MARKMAN A., *Roadmap on optical security*, Journal of Optics **18**(8), 2016: 083001. https://doi.org/10.1088/2040-8978/18/8/083001

[25] SINGH N., SINHA A., *Optical image encryption using fractional Fourier transform and chaos*, Optics and Lasers in Engineering **46**(2), 2008: 117-123. https://doi.org/10.1016/j.optlaseng.2007.09.001

[26] YADAV S., SINGH H., *Image encryption algorithm based on rear-mountedphase mask and random decomposition*, Optica Applicata **52**(2), 2022: 195-212. https://doi.org/10.37190/oa220204

[27] LUAN G., ZHONG Z., SHAN M., *Optical multiple-image encryption in discrete multiple-parameter fractional Fourier transform scheme using complex encoding, theta modulation and spectral fusion*, Optica Applicata **51**(1), 2021: 121-134. https://doi.org/10.37190/oa210110

[28] ZHOU L., ZHOU H., MA Y., ZHOU N.-R., *Double-image encryption scheme based on the phase-truncated multiple-parameter Fresnel transform*, Optica Applicata **52**(2), 2022: 163-177. https://doi.org/10.37190/oa220202

[29] LIU Z., LI S., LIU W., WANG Y., LIU S., *Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding*, Optics and Lasers in Engineering **51**(1), 2013: 8-14. https://doi.org/10.1016/j.optlaseng.2012.08.004

[30] FARAH M.A.B., GUESMI R., KACHOURI A., SAMET M., *A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation*, Optics & Laser Technology **121**, 2020: 105777. https://doi.org/10.1016/j.optlastec.2019.105777

[31] YAN C., JIN W., *Double-lens extended fractional Fourier transform*, Applied Optics **45**(32), 2006: 8315-8321. https://doi.org/10.1364/AO.45.008315

[32] HUA J., LIU L., LI G., *Extended fractional Fourier transforms*, Journal of the Optical Society of America A **14**(12), 1997: 3316-3322. https://doi.org/10.1364/josaa.14.003316

[33] CASAS G.A., RECH P.C., *Multistability annihilation in the Hénon map through parameters modulation*, Communications in Nonlinear Science and Numerical Simulation **17**(6), 2012: 2570-2578. https://doi.org/10.1016/j.cnsns.2011.10.031

[34] SONIS M., *Once more on Hénon map: Analysis of bifurcations*, Chaos, Solitons & Fractals **7**(12), 1996: 2215-2234. https://doi.org/10.1016/s0960-0779(96)00081-1

[35] AZIZ-ALAOUI M.A., ROBERT C., GREBOGI C., *Dynamics of a Hénon-Lozi-type map*, Chaos, Solitons & Fractals **12**(12), 2001: 2323-2341. https://doi.org/10.1016/S0960-0779(00)00192-2

[36] GHADIRLI H.M., NODEHI A., ENAYATIFAR R., *An overview of encryption algorithms in color images*, Signal Processing **164**, 2019: 163-185. https://doi.org/10.1016/j.sigpro.2019.06.010

[37] KAUR G., AGARWAL R., PATIDAR V., *Image encryption using fractional integral transforms: Vulnerabilities, threats, and future scope*, Frontiers in Applied Mathematics and Statistics **8**, 2022: 1039758. https://doi.org/10.3389/fams.2022.1039758

[38] KAUR M., KUMAR V., *A comprehensive review on image encryption techniques*, Archives of Computational Methods in Engineering **27**, 2020: 15-43. https://doi.org/10.1007/s11831-018-9298-8

Received November 24, 2022
in revised form January 30, 2023