




Optical image encryption based on Fourier ptychography and plaintext-related chaotic random phase mask

Jiaxin Li¹ · Yonghui Wang¹ · Wenjun Xu² · Fei Li^{1,3} · Shuaiqi Liu^{1,3} · Yonggang Su^{1,3} 

Received: 9 October 2023 / Accepted: 9 December 2023
© The Author(s), under exclusive licence to The Optical Society of India 2023

Abstract In this paper, we propose an optical image encryption based on LED-illuminated Fourier ptychography (FP) and plaintext-related chaotic random phase mask (CRPM). In this image encryption scheme, the plaintext-related CRPMs are generated by chaotic Lozi map and secure hash algorithm (SHA-256). During the encryption process, the input original image undergoes encryption, resulting in a series of noise-like low-resolution images using two CRPMs and Fourier ptychography methods. In the decryption process, the original image can be reconstructed and decrypted from a series of low-resolution encrypted images using Fourier ptychography phase retrieval algorithm with correct keys. In this proposed encryption scheme, the initial values and parameters of the chaotic system, which dependent on plaintext, replace the random phase masks as the keys. The random phase masks are used as intermediate variables, facilitating the transmission and management of secret keys. In addition, the chaotic parameter keys are linked to the plaintext image. When the plaintext image changes, the chaotic parameter keys can be dynamically updated in real-time, thereby enhancing the security of the image encryption scheme. Further analyze the feasibility, security, and robustness of the image encryption scheme through numerical simulation experiments.

Keywords Optical image encryption · Fourier ptychography · Chaotic random phase mask · Chaotic Lozi map

Introduction

Images serve as a medium for transmitting information in daily life. However, they are susceptible to illegal copying, theft, and tampering during the transmission process. So, it becomes essential to protect the security of image information. Image encryption technology is an important means to protect the security of image information, and researchers continually propose and improve various image encryption schemes. Among them, optical image encryption has been widely used because of its advantages of high-speed parallelism, large dimensions of key space, large amounts of information data and parallel processing [1, 2]. Among various optical image encryption schemes, the most representative is the double random phase encoding (DRPE) [3] proposed Refregier and Javidi in 1995. In this encryption scheme, two random phase masks are placed in the input plane and the Fourier plane respectively to encrypt the original image into a stationary white noise. Based on this, the researchers have extended DRPE into various transform domains such as the fractional Fourier transform (FrFT) domain [4–6], Fresnel transform (FrT) domain [7, 8], Gyator transform (GT) domain [9–11], linear canonical transform (LCT) domain [12, 13], and have proposed a series of effective image encryption schemes.

In DRPE-based encryption schemes, the transmission of random phase mask keys, which are of the same size as the encrypted image, to the receiver for decrypting the original image poses challenges in terms of key management and transmission [14]. To solve this problem, researchers have

✉ Fei Li
lifei@hbu.edu.cn

✉ Yonggang Su
ygsu0726@163.com

¹ College of Electronic and Information Engineering, Hebei University, Baoding 071000, China

² College of Science, Hebei Agricultural University, Baoding 071001, China

³ Machine Vision Technology Innovation Center of Hebei Province, Baoding 071000, China

proposed some encryption schemes based on chaotic random phase encoding (CRPE), in which the random phase masks are generated using chaotic maps, and the chaotic parameters can replace the whole random phase masks as secret keys. For example, Faragallah et al. [15] proposed an optical double image encryption scheme based on Fresnel transform and chaotic map, in which the random phase masks were generated by the baker map and the Arnold 'scat map. Su et al. [16] proposed a color image encryption scheme based on chaotic fingerprint phase mask, in which the random phase masks were generated by Henon map. Farah et al. [17] proposed an optical image encryption scheme based on fractional Fourier transform and DNA sequence operation, in which the random phase masks were generated by the iterative Lorenz map. Singh et al. [18] proposed an optical image encryption scheme based on Gyator transform, in which the random phase masks were generated by Logistic map, Tent map and Kaplan-Yorke map.

However, the chaotic random phase masks used in the optical image encryption scheme mentioned above are not associated with the plaintext, and the same key is used to encrypt different images. Once the secret keys are leaked, all images encrypted by this system are at risk of leakage. In addition, Fourier ptychography (FP) [19, 20] is a new computational imaging technique developed in recent years. FP reduces the requirement of spatial coherence as the images are captured in spatial domain [21]. This means that we can use a partially coherent LED matrix to achieve multi-angle lighting [22, 23]. Additionally, compared to traditional lamination imaging, Fourier ptychography introduces the concept of aperture synthesis. By capturing a series of low-resolution intensity images, it is able to recover large field of view and high-resolution light field information. It has been applied in quantitative phase imaging in 3D [24], digital pathology and cytometry [25–27], aberration metrology [28–30], electron microscopy [31, 32] and other fields. In 2019, Pan et al. [33] first applied the FP with LED illumination to the field of

Fig. 1 Schematic of the generation procedure of CRPM

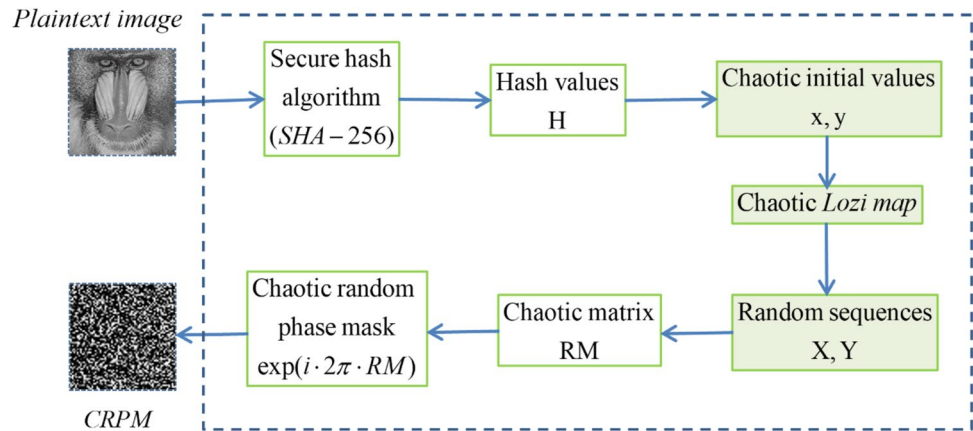
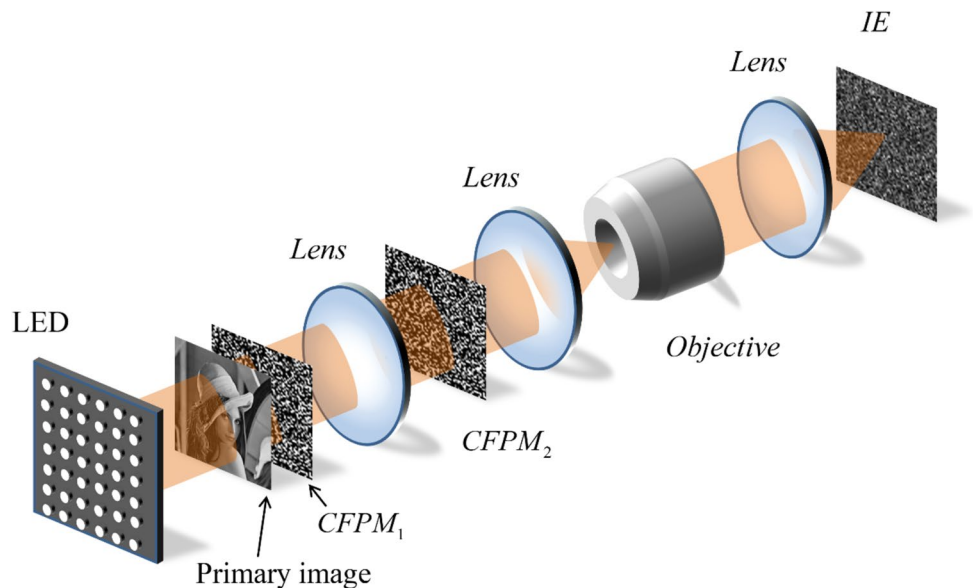


Fig. 2 Schematic of optical image encryption based on LED-illuminated Fourier ptychography and plaintext-related chaotic random phase mask



optical image encryption. They combined it with traditional DRPE, proposed a linear space-variant optical cryptosystem based on LED-illuminated Fourier ptychography to realize grayscale image encryption. In this paper, we propose an optical image encryption based on LED-illuminated Fourier ptychography and plaintext-related chaotic random phase mask. In our proposed encryption scheme, the plaintext-related chaotic random phase masks (CRPMs) are generated by chaotic Lozi map [34] and secure hash algorithm (SHA-256) [35]. During the encryption process, the input original image undergoes encryption, resulting in a series of noise-like low-resolution images using two CRPMs and Fourier ptychography methods. During the decryption process, the input original image can be reconstructed and decrypted from a series of low-resolution encrypted images by using Fourier ptychography phase retrieval algorithm [36, 37] with correct keys. In this proposed encryption scheme, the initial values and parameters of the chaotic system, which dependent on plaintext, replace the random phase masks as the keys. The random phase masks are used as intermediate variables, facilitating the transmission and management of secret keys. In addition, the chaotic parameter keys are associated with the plaintext image. When the plaintext image changes, the chaotic parameter keys can be dynamically updated in real time, thereby enhancing the security of the image encryption scheme.

The rest of this paper is organized as follows. “**Plaintext-related chaotic random phase masks**” provides a detailed

description of the generation of the plaintext-related CRPMs. “**The proposed image encryption scheme**” introduces the encryption-decryption process of the proposed scheme. “**Experiment results and analysis**” presents the numerical simulations of the proposed scheme. Lastly, “**Conclusions**” concludes the paper.

Plaintext-related chaotic random phase masks

In this paper, the plaintext-related CRPMs are generated by the chaotic Lozi map and SHA-256. The generation process shown in Fig. 1 mainly consists of the following steps:

Step 1: Calculate the hash value H of the plaintext image using SHA-256:

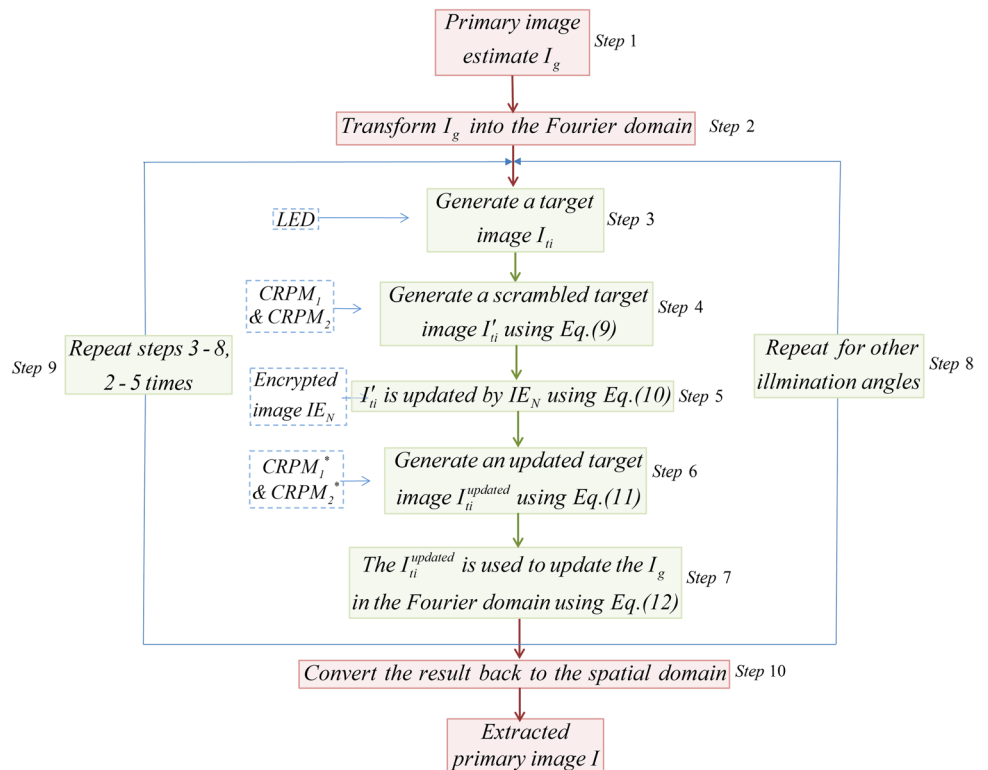
$$H = [h_1, h_2, \dots, h_{64}] \tag{1}$$

Step 2: Generate the initial values of the chaotic Lozi map through the following way:

$$\begin{cases} x = x_0 + \text{hex2dec}(H(h_i : h_{i+4})) \times 10^{-16} \\ y = y_0 + \text{hex2dec}(H(h_j : h_{j+4})) \times 10^{-16} \end{cases} \tag{2}$$

where, i, j are positive integers ranging from $[1, 64]$, x_0, y_0 are initial values of the Lozi map, x, y are generated initial values of the Lozi map, $\text{hex2dec}(h)$ is used to convert a hexadecimal number h to a decimal number.

Fig. 3 Flowchart of the LED-illuminated Fourier ptychography recovery algorithm



Step 3: Assume that the size of the CRPMs to be generated is $M \times N$, then the chaotic Lozi map with initial values of x , y and parameters of $\alpha = 1.75$, $\beta = 0.33$ should iterate $(M \times N)/2$ times:

$$\begin{cases} X = \{x_1, x_2, \dots, x_{(M \times N)/2}\} \\ Y = \{y_1, y_2, \dots, y_{(M \times N)/2}\} \end{cases} \quad (3)$$

Step 4: Limit the value of each element in the two random sequences to the interval $[0,1]$ through the following way:

$$\begin{cases} x'_k = \text{double}(\text{unit8}(x_k \times 1000 \bmod 256))/255 \\ y'_k = \text{double}(\text{unit8}(y_k \times 1000 \bmod 256))/255 \end{cases} \quad (4)$$

where $k = 1, 2, \dots, (M \times N)/2$; \bmod is the symbol for modulus operation; $\text{unit8}(\cdot)$ represents the operation of converting a variable to an unsigned integer.

Step 5: Combine the two random sequences consisting x'_k and y'_k to create a new random sequence Z :

$$Z = \{x'_1, x'_2, \dots, x'_{(M \times N)/2}; y'_1, y'_2, \dots, y'_{(M \times N)/2}\} \quad (5)$$

Step 6: Convert the random sequence Z into a 2D random matrix RM of size $M \times N$:

$$RM = \text{reshape}(Z, M, N) \quad (6)$$

Step 7: The CRPM can be generated through the following way:

$$CRPM = \exp(i \cdot 2\pi \cdot RM) \quad (7)$$

The initial value for the Lozi map can be generated by altering the values of i and j . By repeating steps 3–6, we can obtain a series of different plaintext-dependent CRPMs.

The proposed image encryption scheme

Encryption process

The encryption process, as shown in Fig. 2, can be implemented using some optoelectronic devices. The complex image and the chaotic random phase mask can be added to the optical path through spatial light modulators (SLM). The complex image is illuminated by an LED light source, and encoding with two CRPMs. The encoded image is then recorded by a CCD camera as a series of low-resolution encrypted images resembling noise. These images are stored in a computer using phase-shifting or off-axis digital holography techniques. The encryption process is mainly divided into the following steps:

The encoded image is then recorded by a CCD camera as a series of low-resolution encrypted images resembling noise.

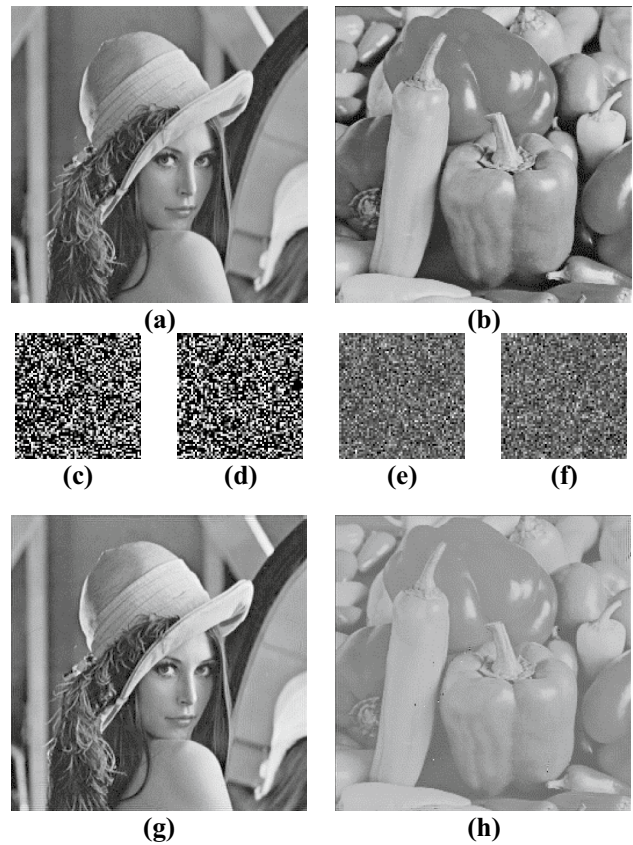


Fig. 4 (a)–(b) The input amplitude and input phase of the high-resolution input original images, (c)–(d) CFPMs generated by (a), (e)–(f) two encrypted images, (g)–(h) the amplitude portion and phase portion of the original image decrypted with the correct keys

These images are stored in a computer using phase-shifting or off-axis digital holography techniques.

Step 1: Using a plaintext image as the input amplitude and any image as the input phase, generated a high-resolution complex image of size 256×256 as the input original image I . In which, the plaintext image represents the image we want to encrypt, while the other image is only used to construct the high-resolution complex image.

Step 2: Illuminate the LED and select a sub-region I_N in the Fourier domain of the original image I , equivalent to a low-pass filter of the coherent imaging system. The position of the low-pass filter is selected to correspondingly illuminate different LED elements. I_N is modulated by two chaotic random phase masks CRPM1 and CRPM2 in the Fourier domain, which is expressed as:

$$IE_N = \left| \text{IFT}(\text{CTF} \cdot \text{pupil}(\text{IFT}(\text{FT}(I_N \cdot \text{CRPM}_1) \cdot \text{CRPM}_2))) \right| \quad (8)$$

where, $N = 1 \dots 225$, CTF is the coherent optical transfer function of the objective lens, pupil is the pupil function for

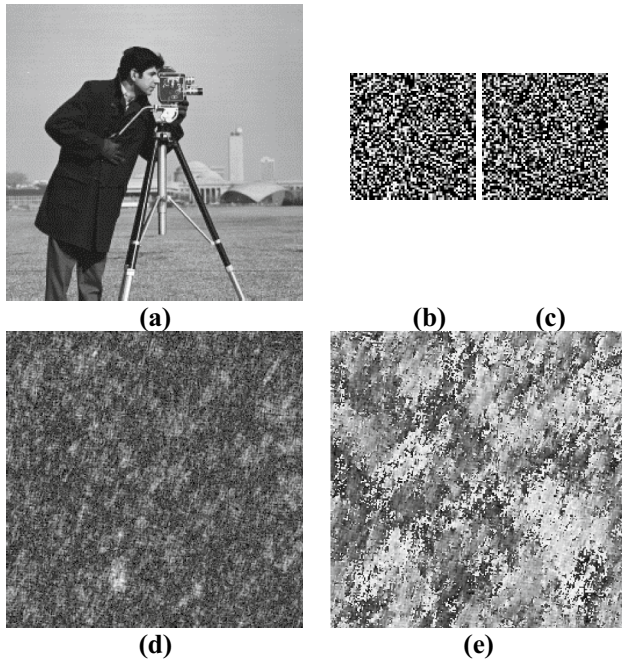


Fig. 5 (a) “Cameraman” image, (b)–(c) CRPMs generated by (a), (d)–(e) the amplitude portion and phase portion of the original image decrypted using error CRPMs

defocus aberration and the defocus distance is set to $10\ \mu\text{m}$, $FT(\cdot)$ represents the Fourier transform, $IFT(\cdot)$ represents the inverse Fourier transform, IE_N are encrypted images.

Step 3: Illuminate other LED elements, repeat step 2 until obtain encrypted images corresponding to all LED elements.

Decryption process

With the correct secret key, we can reconstruct and decrypt the original image using Fourier ptychography phase retrieval algorithm. The decryption process, as shown in Fig. 3, mainly consists of the following steps:

Step 1: The decryption process commences with an initial guess in spatial domain of the original image I_g .

Step 2: The initial guess I_g is transformed to the Fourier domain obtain the Fourier spectrum of the initial guess.

Step 3: The reconstructed update sequence is configured according to the energy criteria, prioritizes images with higher total energy of the encrypted image. In this approach, we start from the image corresponding to the center of the Fourier spectrum (the image 113), and end with the image corresponding to the edge of the spectrum (the image 225). Following this order, we select subregions in the Fourier spectrum of I_g to obtain the target image I_{ii} .

Step 4: The target image I_{ii} is modulated by the chaotic random phase mask CRPM1 and CRPM2 in the Fourier domain to obtain the scrambled target image I_{ii}' :

$$I_{ii}' = IFT(FT(I_{ii} \cdot CRPM_1) \cdot CRPM_2) \tag{9}$$

Step 5: Introducing the encrypted image IE_N , the scrambled target image I_{ii} is updated by the following equation to obtain the updated scrambled target image $I_{ii}'^{updated}$:

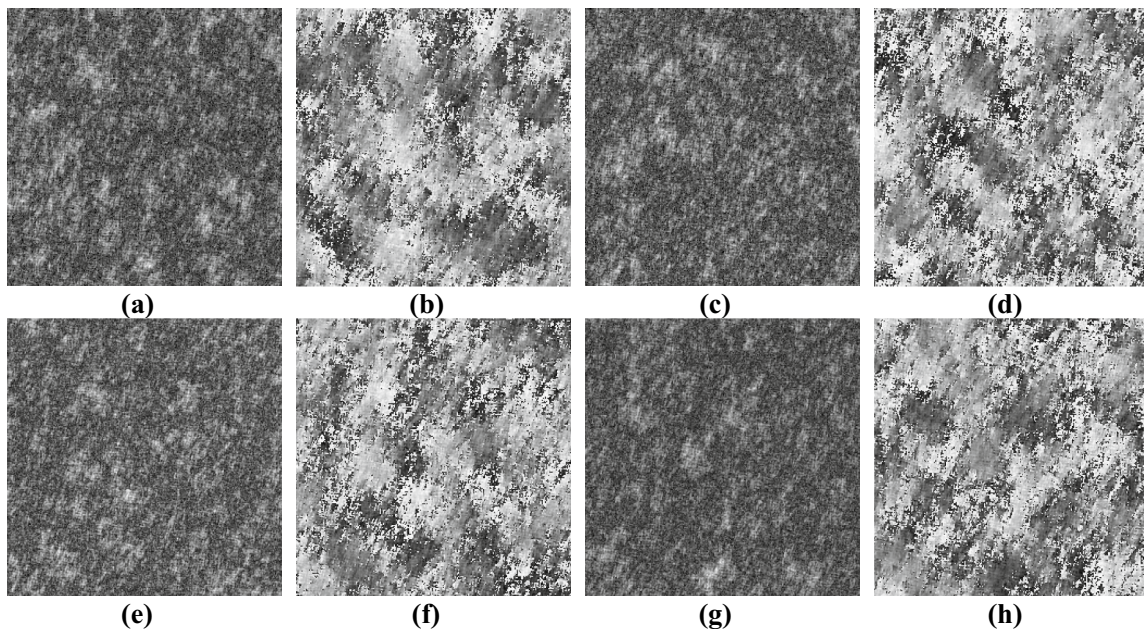


Fig. 6 The amplitude portion and phase portion of the original image decrypted using one incorrect chaotic original initial value or parameters (a)–(b) $x'_0 = 0.34 + 10^{-15}$, (c)–(d) $y'_0 = 0 + 10^{-15}$, (e)–(f) $\alpha' = 1.75 + 10^{-15}$, (g)–(h) $\beta' = 0.33 + 10^{-15}$

$$I_{ii}^{updated} = FT(IE_N \cdot \exp(1i \cdot \text{angle}(I_m))) \cdot CTF \cdot \frac{1}{pupil} \tag{10}$$

where $I_m = IFT(I_{ii} \cdot CTF \cdot pupil)$.

Step 6: The updated scrambled target image $I_{ii}^{updated}$ is modulated by the conjugate of chaotic random phase mask CRPM1 and CRPM2 to obtain the updated target image $I_{ii}^{updated}$:

$$I_{ii}^{updated} = IFT(FT(I_{ii}^{updated}) \cdot CRPM_2^*) CRPM_1^* \tag{11}$$

Step 7: The updated target image $I_{ii}^{updated}$ updates the estimate of the original image in the Fourier domain by:

$$FT(I_g^{updated}) = I_{ii}^{updated} + (1 - CTF) \cdot I_g \tag{12}$$

Step 8: The update process is repeated for all illumination angles, at which point the entire high-resolution image

in Fourier space has been modified by all low-resolution intensity measurements.

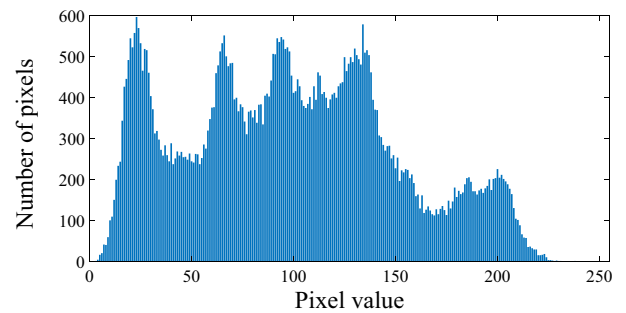
Step 9: Repeat steps 3–8, usually we repeat this process 2–5 times.

Step 10: At the end of the above iterative recovery process, the convergent solution in Fourier space is converted back to the spatial domain, and the original image is reconstructed and decrypted.

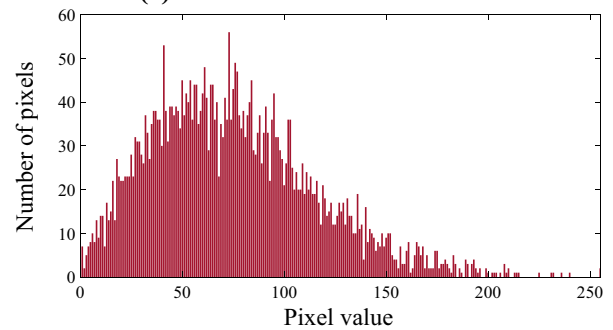
Table 1 The correlation coefficients between adjacent pixels in original image and two encrypted images selected randomly

Directions	Original image	Encrypted image1	Encrypted image 2
Horizontal	0.9751	-0.0026	0.0140
Vertical	0.9573	0.0058	0.0072
Diagonal	0.9363	0.0077	0.0075

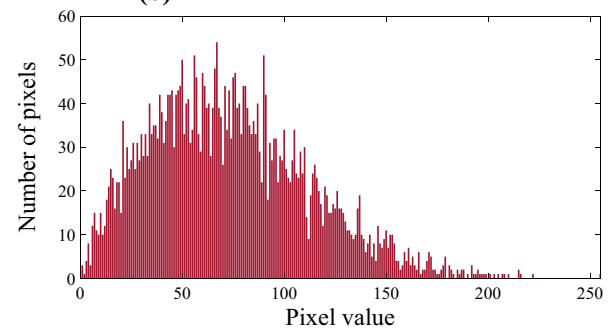
Fig. 7 (a) Original image and histogram, (b)–(c) two encrypted images and histograms



(a)



(b)



(c)

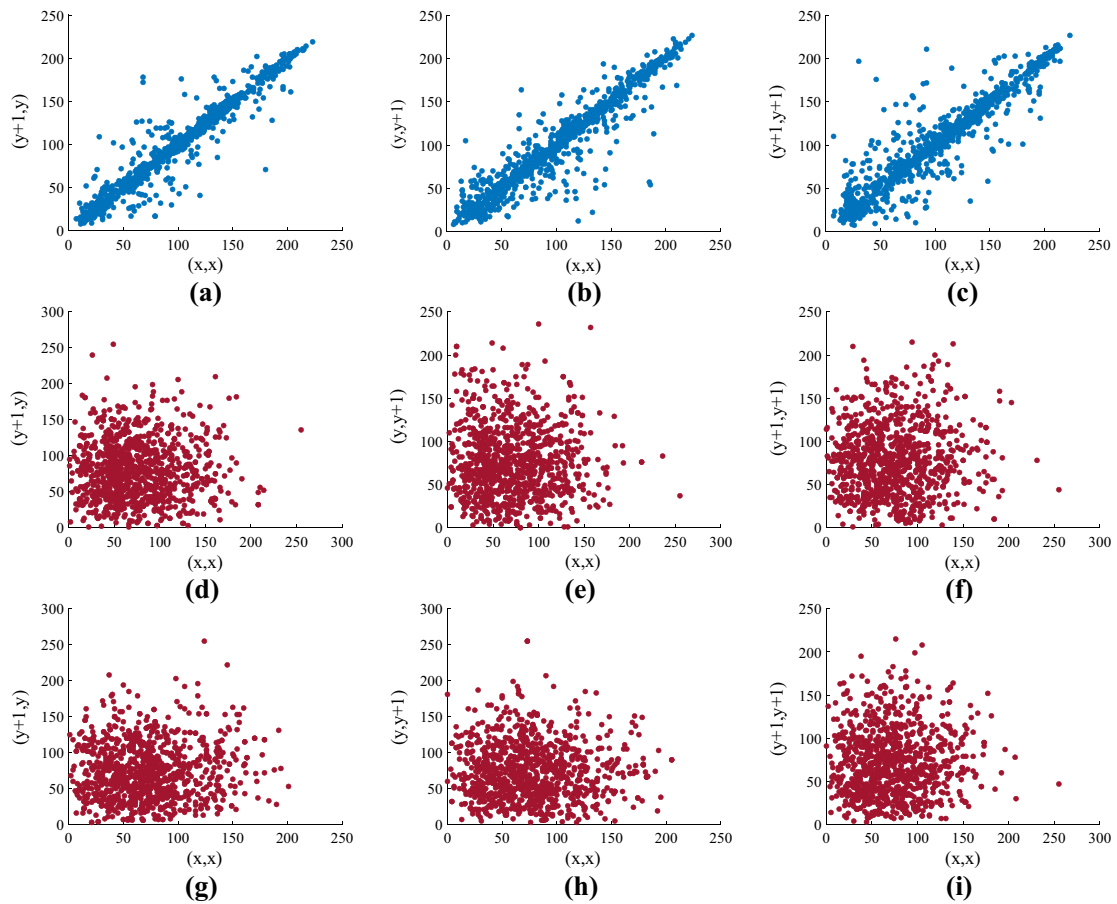


Fig. 8 Correlations between adjacent pixels in horizontal, vertical, and diagonal directions (a)–(c) original image, (d)–(i) two encrypted images

Experiment Results and analysis

Feasibility analysis

In order to verify the feasibility, security and robustness of the proposed scheme. We conducted a series of simulation experiments using MATLAB 2018b. In these simulation experiments, the LED matrix contains 15×15 elements, resulting in a total of 225 different illumination angles. Set the initial value of the Lozi chaos map to $x_0 = 0.34$, $y_0 = 0$, the chaotic parameter is set to $\alpha = 1.75$, $\beta = 0.33$. The images to be encrypted is shown in Fig. 4a, so use Fig. 4a "Lena" as input amplitude and Fig. 4b "Peppers" as input phase to generate high-resolution input original images. Use Fig. 4a to generate two CRPMs as shown in Fig. 4c–d. We need to deal with two types of image dimensions in this experiment, namely 256×256 high-resolution image and 64×64 low-resolution image. The high-resolution input original image is encrypted into 225 low-resolution encrypted images by using two CRPMs

and Fourier ptychography methods, two of the encrypted images shown in Fig. 4e–f. We can be found that there is no information about the original image in Fig. 4e–f. The amplitude part and phase part of the decrypted original image reconstructed with the correct keys are shown in Fig. 4g, h. The encryption process took 0.6725 s and the decryption process took 1.0345 s. To quantify the similarity between the original image and the decrypted image, the correlation coefficient (CC) and structural similarity (SSIM) are introduced. The larger the CC and SSIM, the more similar the two images are.

The CC is defined as:

$$CC(I, I_d) = \frac{E\{[I - E(I)][I_d - E(I_d)]\}}{\{E\{[I - E(I)]^2\}\{E\{[I_d - E(I_d)]^2\}\}}^{\frac{1}{2}} \quad (13)$$

where I is the original image, I_d is the decrypted image, $E\{\bullet\}$ is an expectation operator.

The SSIM is defined as:

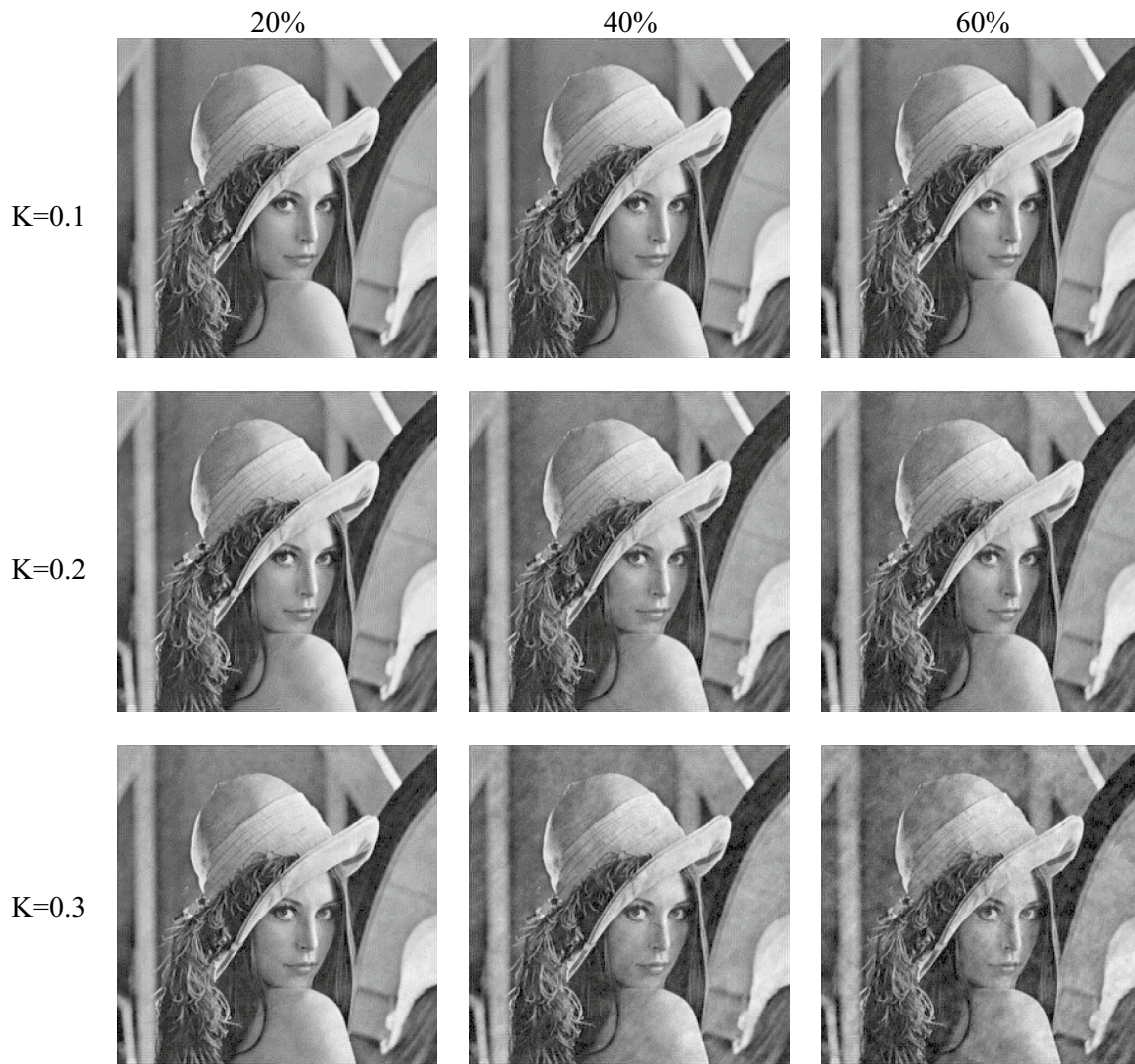


Fig. 9 Decrypted images from the Gaussian noise contaminated encrypted images

$$SSIM(I, I_d) = \frac{(2\mu_I\mu_{I_d} + C_1)(2\sigma_{II_d} + C_2)}{(\mu_I^2 + \mu_{I_d}^2 + C_1)(\sigma_I^2 + \sigma_{I_d}^2 + C_2)} \quad (14)$$

where μ_I and μ_{I_d} denote the mean of the image I and I_d , respectively; σ_I and σ_{I_d} denote the variance of the image I and I_d , respectively; σ_{II_d} denotes the covariance of the image I and I_d ; and C_1 and C_2 are two constants.

The visual observation of Fig. 4a, g shows that they are very similar. The CC value between them is 0.9994, the SSIM value between them is 0.9963, indicating that the original image can be well restored.

Security analysis

In order to verify the security of the scheme proposed in this paper, the wrong keys are used in decryption process. First,

use the image shown in Fig. 5a (change the generated initial values x, y) to generate the CRPMs, the original initial value is still set to $x_0 = 0.34, y_0 = 0$ and the chaotic parameter is still set to $\alpha = 1.75, \beta = 0.33$. The generated CRPMs are shown in Fig. 5b–c. The amplitude portion and phase portion of the original image reconstructed and decrypted using the CRPMs shown in Fig. 5b–c is shown in Fig. 5d–e. The CC and SSIM between Figs. 4a and 5d are 0.0047 and 0.0029. It can be seen that when the plaintext image is wrong, the valid original image cannot be recovered.

Secondly, use the wrong chaotic original initial value and parameters of Lozi map to decrypt. Figure 6 respectively represent the amplitude portion and phase portion of the original image decrypted with one incorrect chaotic original initial value or parameters, respectively. The CC between Figs. 6a, c, e, g and 4a are 0.0038, 0.0033, 0.0026

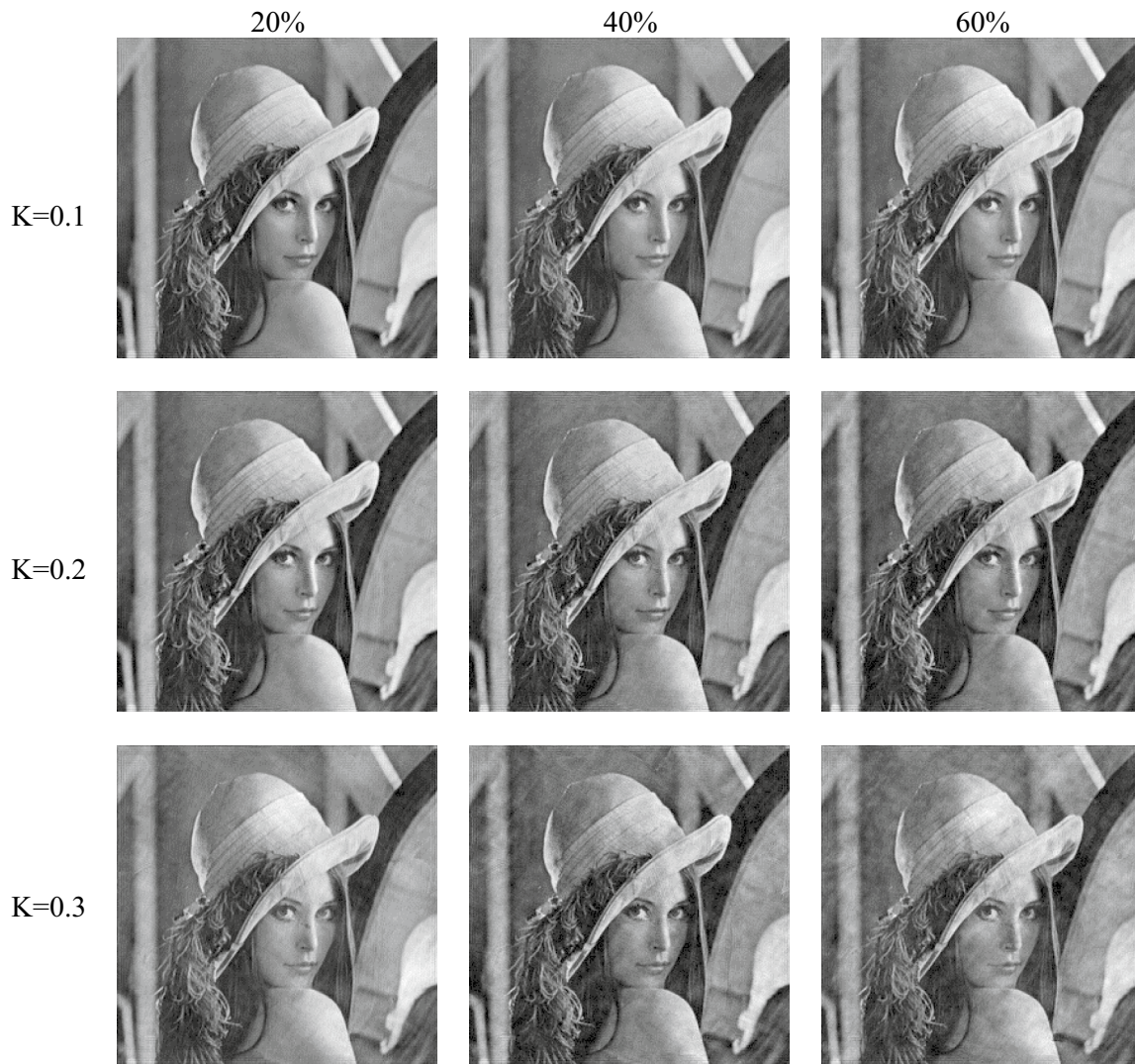


Fig. 10 Decrypted images from the salt & pepper noise contaminated encrypted images

and 0.0067. The SSIM between Figs. 6a, c, e, g and 4a are 0.0021, 0.0055, 0.0013 and 0.0019. It can be seen from the above results that the effective original image cannot be recovered even if any of the chaotic original initial values and parameters change slightly. Therefore, the chaotic original initial values and parameters can be used as the secret keys of the image encryption scheme proposed in this paper.

In addition, attackers may use statistical analysis methods to infer the content or key information of images, in order to test the robustness of the image encryption scheme proposed in this paper against statistical analysis attacks. As shown in Fig. 7, we first plot histograms of the original image and two randomly selected encrypted images. It can be seen from Fig. 7a–c that the histogram of the original image has more peaks and fluctuations, while the histogram of the encrypted images exhibits more uniform characteristics, and there are obvious differences between them. We also randomly select

1000 pairs of adjacent pixels from the horizontal, vertical and diagonal directions of the original image and the two encrypted images, and use the formula in Ref. [38] to calculate the correlation coefficient between adjacent pixels, as shown in Table 1. Furthermore, Fig. 8 shows the correlation between adjacent pixels of the original image and the two encrypted images in three directions. It can be seen that the correlation of adjacent pixels in the three directions of the original image is strong, while the correlation of adjacent pixels in the three directions of the two encrypted images is extremely low. Therefore, the image encryption scheme proposed in this paper is highly robust to statistical analysis attacks.

Fig. 11 Decrypted images from the speckle noise contaminated encrypted images

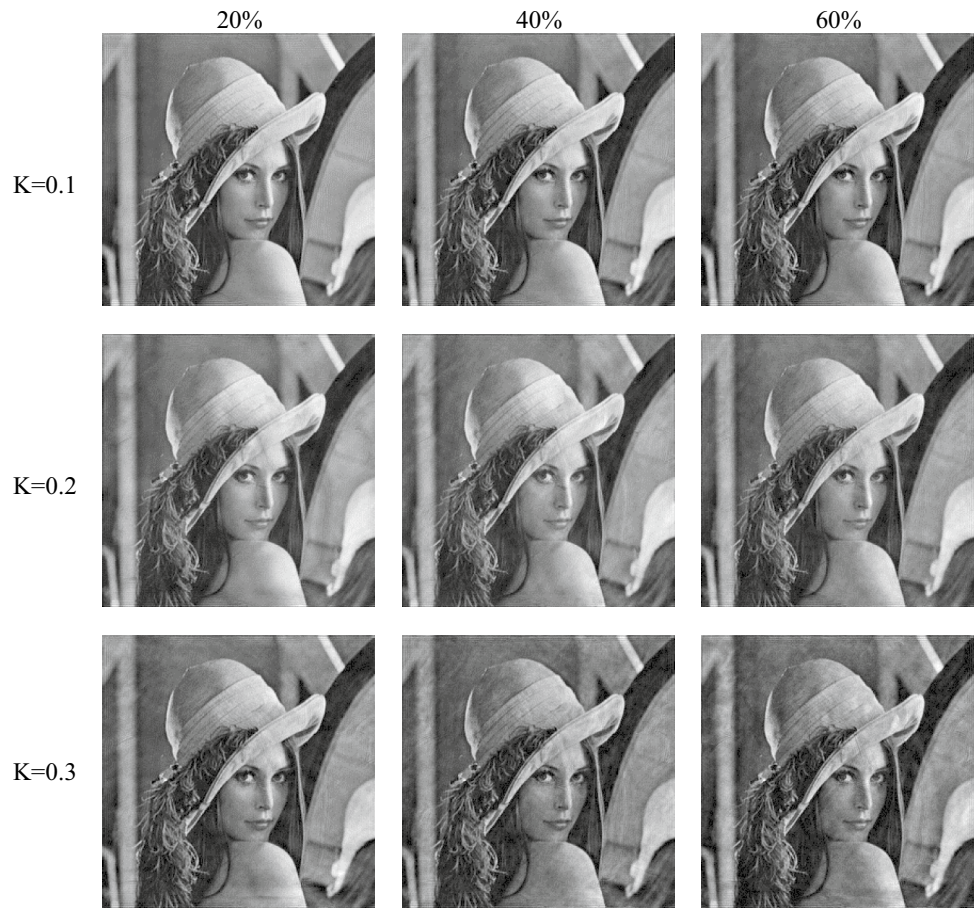


Table 2 CC values between original image and decrypted image with Gaussian noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.9964	0.9961	0.9956
0.2	0.9946	0.9926	0.9903
0.3	0.9934	0.9848	0.9737

Table 3 SSIM values between original image and decrypted image with Gaussian noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.8461	0.8324	0.8146
0.2	0.8006	0.7609	0.7180
0.3	0.7312	0.6630	0.5878

Table 4 CC values between original image and decrypted image with salt & pepper noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.9952	0.9923	0.9912
0.2	0.9929	0.9890	0.9852
0.3	0.9839	0.9779	0.9634

Table 5 SSIM values between original image and decrypted image with salt & pepper noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.8164	0.7779	0.7468
0.2	0.7638	0.6988	0.6723
0.3	0.7045	0.6166	0.5483

Robustness analysis

Encrypted images may be subject to noise pollution or data loss during transmission. To test the robustness of the

proposed image encryption scheme against noise attacks in this paper, noise is introduced in the following manner:

Table 6 CC values between original image and decrypted image with speckle noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.9950	0.9933	0.9920
0.2	0.9847	0.9842	0.9890
0.3	0.9850	0.9791	0.9719

Table 7 SSIM values between original image and decrypted image with speckle noise attack

Embedding intensity K	The proportion of images attacked by noise		
	20%	40%	60%
0.1	0.8143	0.7832	0.7640
0.2	0.7038	0.6785	0.6594
0.3	0.6981	0.6309	0.6004

$$IE' = IE + (1 + K \cdot G) \tag{15}$$

where, IE' represents the attacked encrypted images, K represents the embedding intensity, and G represents generated noise. In the experiments, we utilized Gaussian noise,

speckle noise, and salt & pepper noise. We added noise at 20%, 40%, and 60% (45 images, 90 images, 135 images) levels to 225 encrypted images. The decrypted images obtained with the correct keys when the embedding intensity K is 0.1, 0.2, 0.3, respectively, are shown in Figs. 9, 10 and 11. The CC and SSIM corresponding to the decrypted image and the original image are shown in Tables 2, 3, 4, 5, 6 and 7. The above results show that when the noise embedding intensity is constant, the quality of decrypted images deteriorates with the increase of the number of noise-polluted encrypted images. Similarly, when the number of noise-polluted encrypted images is constant, the quality of decrypted images deteriorates with the increase of noise embedding intensity. However, when the noise embedding intensity is increased to 0.3 and 60% (135 images) of the encrypted images are contaminated, the original images can still be recovered well. Therefore, the image encryption scheme proposed in this paper has high robustness against noise attacks.

During the transmission of encrypted images, partial data loss may occur. We conducted the following simulation experiments to verify the robustness of the image encryption scheme proposed in this paper against data loss. Similarly, we randomly selected 20%, 40%, and 60% (45 images, 90 images, 135 images) of the 225 encrypted images and set some pixel values of the selected images to 0 to simulate data loss. When

Fig. 12 Decrypted images from data loss attack

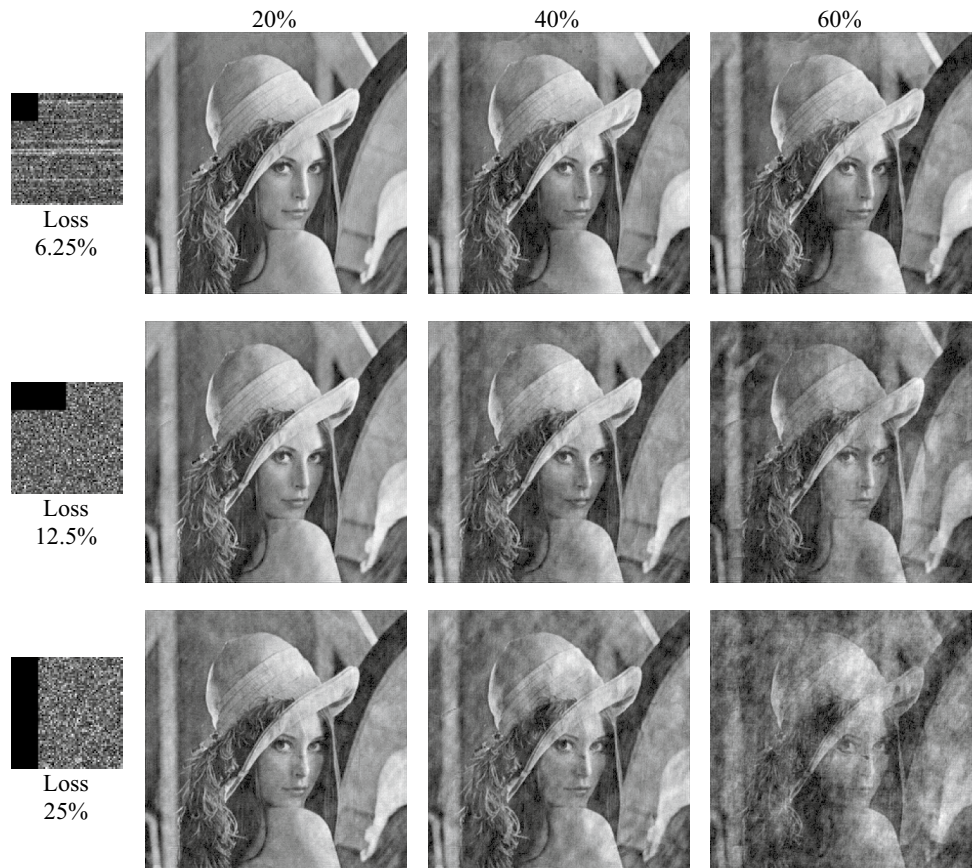


Table 8 CC values between original image and decrypted image with data loss attack

Data loss percentages	The proportion of images attacked by data loss		
	20%	40%	60%
6.25%	0.9914	0.9622	0.9552
12.5%	0.9783	0.9617	0.9112
25%	0.9677	0.9410	0.8596

Table 9 SSIM values between original image and decrypted image with data loss attack

Data loss percentages	The proportion of images attacked by data loss		
	20%	40%	60%
6.25%	0.7603	0.6785	0.6445
12.5%	0.6580	0.6725	0.6594
25%	0.5698	0.5115	0.4809

the data loss rate is 5%, 10%, 15%, the decrypted images obtained by using the correct keys are shown in Fig. 12. The CC and SSIM corresponding to the decrypted image and the original image are shown in Tables 8 and 9. The above results show that when the ratio of data loss is constant, the quality of decrypted images deteriorates with the increase of the number of encrypted images with data loss. Similarly, when the number of encrypted images with data loss is constant, the quality of decrypted images deteriorates with the increase of the proportion of data loss. However, when the data loss rate is increased to 25% and 60% of the encrypted images are subject to data loss attacks, the original images can still be recovered well. Therefore, the image encryption scheme proposed in this paper has high robustness against data loss attacks.

Conclusions

This paper presents an optical image encryption based on LED-illuminated Fourier ptychography and plaintext-related chaotic random phase mask. In this image encryption scheme, the plaintext-related CRPMs are generated by chaotic Lozi map and secure hash algorithm. During the encryption process, the input original image undergoes encryption, resulting in a series of noise-like low-resolution images using two CRPMs and Fourier ptychography methods. In the decryption process, the input original image can be reconstructed and decrypted from a series of low-resolution encrypted images

by using Fourier ptychography phase retrieval algorithm with correct keys. In this proposed encryption scheme, the initial values and parameters of the chaotic system, which depend on plaintext, replace the random phase masks as the keys. The random phase masks are used as intermediate variables, facilitating the transmission and management of secret keys. In addition, the chaotic parameter keys are associated with the plaintext image. When the plaintext image changes, the chaotic parameter keys can be dynamically updated in real time, the security of the image encryption scheme is further improved. The experimental results indicate that the image encryption scheme proposed in this paper can successfully recover high-resolution complex amplitude images as the original image, has high feasibility. In cases of any incorrect key, it is impossible to recover a valid original image, ensuring a high level of security. Additionally, the image encryption scheme is also highly robust against statistical attacks, noise pollution and data loss attacks.

Acknowledgements This work was supported by National Natural Science Foundation of China (62172139), Natural Science Foundation of Hebei Province (F2022201055, F2020201025, F2019201151), Key Research and Development Project in Hebei Province (21327405D), Project Funded by China Postdoctoral (2022M713361), Foundation of Hebei Education Department (QN2020224), Natural Science Interdisciplinary Research Program of Hebei University (DXK202102), Advanced Talents Incubation Program of Hebei University (521000981370), Open Project Program of the National Laboratory of Pattern Recognition (NLPR) (202200007). This work was also supported by the High-Performance Computing Center of Hebei University.

References

1. R. Ma, Y. Li, H. Jia, Y. Shi, X. Xie, T. Huang, Optical information hiding with non-mechanical ptychography encoding. *Opt. Lasers Eng.* **141**, 106569 (2021). <https://doi.org/10.1016/j.optlaseng.2021.106569>
2. I. Kim, J. Jang, G. Kim, J. Lee, T. Badloe, J. Mun, J. Rho, Pixelated bifunctional metasurface-driven dynamic vectorial holographic color prints for photonic security platform. *Nat. Commun.* **12**(1), 3614 (2021). <https://doi.org/10.1038/s41467-021-23814-5>
3. P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**(7), 767–769 (1995). <https://doi.org/10.1364/OL.20.000767>
4. S.S. Yu, N.R. Zhou, L.H. Gong, Z. Nie, Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. *Opt. Lasers Eng.* **124**, 105816 (2020). <https://doi.org/10.1016/j.optlaseng.2019.105816>
5. M.A.B. Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt. Lasers Eng.* **121**, 105777 (2020). <https://doi.org/10.1016/j.optlaseng.2019.105777>

6. X. Wang, Y. Su, Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. *Sci. Rep.* **10**(1), 18556 (2020). <https://doi.org/10.1038/s41598-020-75562-z>
7. E. Kumari, S. Mukherjee, P. Singh, R. Kumar, Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain. *Results Opt.* **1**, 100005 (2020). <https://doi.org/10.1016/j.rio.2020.100005>
8. S. Dou, X. Shen, B. Zhou, L. Wang, C. Lin, Experimental research on optical image encryption system based on joint Fresnel transform correlator. *Opt. Lasers Eng.* **112**, 56–64 (2019). <https://doi.org/10.1016/j.optlastec.2018.11.004>
9. X. Sun, Z. Shao, Y. Shang, M. Liang, F. Yang, Multiple-image encryption based on cascaded gyator transforms and high-dimensional chaotic system. *Multimed. Tools. Appl.* **80**, 15825–15848 (2021). <https://doi.org/10.1007/s11042-021-10550-7>
10. Z. Shao, X. Liu, Q. Yao, N. Qi, Y. Shang, J. Zhang, Multiple-image encryption based on chaotic phase mask and equal modulus decomposition in quaternion gyator domain. *Signal Processing: Image Communication* **80**, 115662 (2020). <https://doi.org/10.1016/j.image.2019.115662>
11. Anshula, H. Singh, Cryptanalysis for double-image encryption using the DTLM in frequency plane with QR decomposition and gyator transform. *Opt. Rev.* **28**(6), 596–610 (2021). <https://doi.org/10.1007/s10043-021-00705-0>
12. Z.J. Huang, S. Cheng, L.H. Gong, N.R. Zhou, Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform. *Opt. Lasers Eng.* **124**, 105821 (2020). <https://doi.org/10.1016/j.optlaseng.2019.105821>
13. A. Sangwan, H. Singh, A secure asymmetric optical image encryption based on phase truncation and singular value decomposition in linear canonical transform domain. *Int. J. Opt.* **2021**, 1–19 (2021). <https://doi.org/10.1155/2021/5510125>
14. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M.S. Millán, A. Markman, Roadmap on optical security. *J. Opt.* **18**(8), 083001 (2016). <https://doi.org/10.1088/2040-8978/18/8/083001>
15. O.S. Faragallah, A. Afifi, I.F. Elashry, E.A. Naeem, H.M. El-Hoseny, H.S. El-sayed, A.M. Abbas, Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform. *Opt. Quant. Electron.* **53**(6), 305 (2021). <https://doi.org/10.1007/s11082-021-02864-5>
16. Y. Su, W. Xu, J. Zhao, L. Chen, X. Tian, Optical color image encryption based on chaotic fingerprint phase mask in various domains and comparative analysis. *Appl. Opt.* **59**(2), 474–483 (2020). <https://doi.org/10.1364/AO.59.000474>
17. M.A.B. Farah, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt. Laser Technol.* **121**, 105777 (2020). <https://doi.org/10.1016/j.optlastec.2019.105777>
18. N. Singh, A. Sinha, Gyator transform-based optical image encryption, using chaos. *Opt. Lasers Eng.* **47**(5), 539–546 (2009). <https://doi.org/10.1016/j.optlaseng.2008.10.013>
19. P.C. Konda, L. Loetgering, K.C. Zhou, S. Xu, A.R. Harvey, R. Horstmeyer, Fourier ptychography: current applications and future promises. *Opt. Express* **28**(7), 9603–9630 (2020). <https://doi.org/10.1364/OE.386168>
20. G. Zheng, C. Shen, S. Jiang, P. Song, C. Yang, Concept, implementations and applications of Fourier ptychography. *Nat. Rev. Phys.* **3**(3), 207–223 (2021). <https://doi.org/10.1038/s42254-021-00280-y>
21. G. Zheng, X. Ou, R. Horstmeyer, J. Chung, C. Yang, Fourier ptychographic microscopy: a gigapixel superscope for biomedicine. *Opt. Photon. News* **25**(4), 26–33 (2014). <https://doi.org/10.1364/OPN.25.4.000026>
22. P. Kumar, A. Fatima, N.K. Nishchal, Image encryption using phase-encoded exclusive-OR operations with incoherent illumination. *J. Opt.* **21**(6), 065701 (2019). <https://doi.org/10.1088/2040-8986/ab173b>
23. P. Kumar, N.K. Nishchal, Enhanced exclusive-OR and quick response code-based image encryption through incoherent illumination. *Appl. Opt.* **58**(6), 1408–1412 (2019). <https://doi.org/10.1364/AO.58.001408>
24. M. Sun, L. Shao, J. Zhang, High-resolution 3D Fourier ptychographic reconstruction using a hemispherical illumination source with multiplexed-coded strategy. *Biomed. Opt. Express* **13**(4), 2050–2067 (2022). <https://doi.org/10.1364/BOE.452363>
25. R. Horstmeyer, X. Ou, G. Zheng, Digital pathology with Fourier ptychography. *Comput. Med. Imag. Graph.* **42**, 38–43 (2015). <https://doi.org/10.1016/j.compmedimag.2014.11.005>
26. D.L. Wakefield, R. Graham, K. Wong, S. Wang, C.C. Yu, Cellular analysis using label-free parallel array microscopy with Fourier ptychography. *Biomed. Opt. Express* **13**(3), 1312–1327 (2022). <https://doi.org/10.1364/BOE.451128>
27. Y. Gao, J. Chen, A. Wang, A. Pan, C. Ma, B. Yao, High-throughput fast full-color digital pathology based on Fourier ptychographic microscopy via color transfer. *Sci. China Phys. Mech. Astron.* **64**, 114211 (2021). <https://doi.org/10.1007/s11433-021-1730-x>
28. T. Kamal, L. Yang, W.M. Lee, In situ retrieval and correction of aberrations in moldless lenses using Fourier ptychography. *Opt. Express* **26**(3), 2708–2719 (2018). <https://doi.org/10.1364/OE.26.002708>
29. J. Chung, G.W. Martinez, K.C. Lencioni, S.R. Sadda, C. Yang, Computational aberration compensation by coded-aperture-based correction of aberration obtained from optical Fourier coding and blur estimation. *Optica* **6**, 647–661 (2019). <https://doi.org/10.1364/OPTICA.6.000647>
30. M. Xiang, A. Pan, J. Liu, T. Xi, X. Guo, F. Liu, X. Shao, Phase diversity-based Fourier ptychography for varying aberration correction. *Front. Phys.* **10**, 129 (2022). <https://doi.org/10.3389/fphy.2022.848943>
31. A. Pan, C. Zuo, B. Yao, High-resolution and large field-of-view Fourier ptychographic microscopy and its applications in biomedicine. *Rep. Prog. Phys.* **83**(9), 096101 (2020). <https://doi.org/10.1088/1361-6633/aba6f0>
32. J. Sun, Q. Chen, J. Zhang, Y. Fan, C. Zuo, Single-shot quantitative phase microscopy based on color-multiplexed Fourier ptychography. *Opt. Lett.* **43**(14), 3365–3368 (2018). <https://doi.org/10.1364/OL.43.003365>
33. A. Pan, K. Wen, B. Yao, Linear space-variant optical cryptosystem via Fourier ptychography. *Opt. Lett.* **44**(8), 2032–2035 (2019). <https://doi.org/10.1364/OL.44.002032>
34. E. Araujo, L.D.S. Coelho, Particle swarm approaches using Lozi map chaotic sequences to fuzzy modelling of an experimental thermal-vacuum system. *Appl. Soft Comput.* **8**(4), 1354–1364 (2007). <https://doi.org/10.1016/j.asoc.2007.10.016>
35. N.K. Nishchal, *Optical cryptosystems* (IOP Publishing, Bristol, 2019). <https://doi.org/10.1088/978-0-7503-2220-1>
36. C. Guo, C. Wei, J. Tan, K. Chen, S. Liu, Q. Wu, Z. Liu, A review of iterative phase retrieval for measurement and encryption. *Opt. Lasers Eng.* **89**, 2–12 (2017). <https://doi.org/10.1016/j.optlaseng.2016.03.021>

37. F. Wittwer, J. Hagemann, D. Brückner, S. Flenner, C.G. Schroer, Phase retrieval framework for direct reconstruction of the projected refractive index applied to ptychography and holography. *Optica* **9**(3), 295–302 (2022). <https://doi.org/10.1364/OPTICA.447021>
38. Y. Su, C. Tang, X. Chen, B. Li, W. Xu, Z. Lei, Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. *Opt. Lasers Eng.* **88**, 20–27 (2017). <https://doi.org/10.1016/j.optlaseng.2016.07.012>

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.