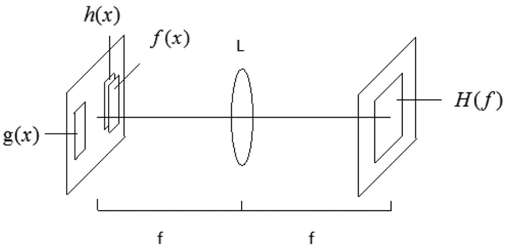
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Image Encryption System Based on Joint Transformation Correlation and Ptychography

Volume 12, Number 2, April 2020

Yuan Zhong
Linfei Chen
Wenwen Gan
Yuanqian Liu



DOI: 10.1109/JPHOT.2019.2921354
1943-0655 © 2019 IEEE

Image Encryption System Based on Joint Transformation Correlation and Ptychography

Yuan Zhong, Linfei Chen, Wenwen Gan, and Yuanqian Liu

School of Science, Hangzhou Dianzi University, Hangzhou 310018, China

DOI:10.1109/JPHOT.2019.2921354

Manuscript received March 26, 2019; revised May 15, 2019; accepted May 31, 2019. Date of publication June 5, 2019; date of current version March 9, 2020. This research was supported in part by the Natural Science Foundation of Zhejiang Province under Grant LY19A040010, in part by the National Natural Science Foundation of China under Grant 61505046, in part by the Construction Project of Postgraduate Core Course in Hangzhou Dianzi University Grant HXKC2017019. Corresponding author: Linfei Chen (e-mail: chenlinfei2004@163.com).

Abstract: In this paper, a new image encryption system based on joint transformation correlation principle and ptychologographic iterative engine is proposed. When the encryption is performed, the original image can be divided into several parts by using the scanning movement of the probe. Each part is encrypted by the joint transformation correlation technology, and the ciphertexts are finally transmitted in the form of many encrypted images. The receiver uses the working principle of the joint transform correlator to decrypt and reconstructs the image by using the ptycholographic iterative engine, which can integrate multiple images with less information into one high-precision decrypted image. Computer simulations prove its possibility.

Index Terms: Optical image encryption, ptychography, joint transformation correlation, Fourier transform.

1. Introduction

In the fields of medicine and materials science, it is necessary to carry out high-precision analysis of samples. However, the current optical detectors usually only receive the intensity information of the beam, and the phase information cannot be received by the detector, thus part of the information will be lost. In fact, the phase information is largely affected by the three-dimensional structure or refractive index of the sample, so the phase information is also one of the important information for analyzing the sample.

Phase imaging technology can be roughly divided into the following two methods due to the method of extracting the phase. One is qualitative imaging of the sample, the main purpose is to achieve observations, and the other is quantitative imaging of samples. The concept of coherent diffraction imaging (CDI) was proposed around 1970. Its specific iterative algorithm was proposed by Gerchberg and Saxton in 1971 and it was called the GS algorithm. After that, the improvement of the algorithm was completed by Misell *et al*, who proposed the error reduction algorithm and the hybrid input and output algorithm [1]. However, these algorithms all have problems such as small field of view, slow convergence rate, and blurred images. In 2004, Rodenburg *et al* overcame these kinds of problems and proposed an algorithm for recovering images called the ptycholographic

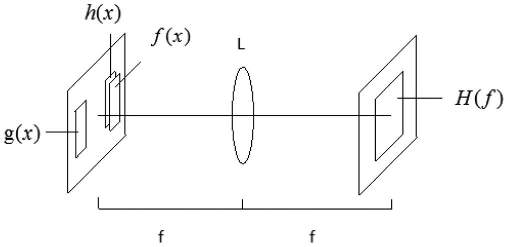


Fig. 1. JTC optical encryption principle.

iterative engine (PIE). We record many diffraction images by regular movement of the probe [2], and reconstruct the sample by using an iterative algorithm. Moving the probe makes the diffraction images overlapped, and it results in a large amount of data redundancy, which greatly improves the image quality and convergence speed when the image is restored [3]. At present, PIE imaging technology has been applied and developed in many fields [4]–[8].

Image encryption technology developed rapidly after 1995 when Refregier and Javidi proposed double random phase encryption technology [9]. Because this system is efficient and it has the features of fast response and high degree of parallelism, many scholars have been attracted to research it [10]–[17]. However, these optical systems require a very accurate spatial position, and it will reduce the fault tolerance of the entire system. In addition, these systems cannot output by printing directly. So Nomura and Javidi proposed a new system called Joint Transform Correlator (JTC) to encrypt and process optical images [18]. JTC encryption technology allows the sample image to be on the same plane as the random phase plate without strict regulations. This brings great convenience to the operation and solves the operational difficulties that require high-precision alignment [19], [20]. At the same time, it also has the resistance to some attacks.

The encryption method introduced in this article is encrypting images by PIE and JTC. We will receive many low resolution diffraction images by PIE [21], then these images are encrypted into different ciphertexts by JTC systems. After receiving the ciphertexts, the receiver needs to decrypt each image with different keys, and sorts the decrypted images in a certain order and restores the sample images by PIE [22], [23]. The system has a large number of keys because it combines the features of PIE and JTC encryption. Compared with the traditional optical encryption methods, this technology expands the key space. It not only has the keys of the traditional random phase masks, but also has the keys of the probe and the phase mask positions. We need all the correct keys to recover the image, which makes the system much more secure. PIE and JTC are easy to integrate with other systems for more functionality. PIE-based encryption can effectively record complex amplitude images, so it can provide new ideas for the encryption of various original images in the field of materials, biology, medical and other fields. And through our simulation, we can find that it has the features of high resolution, low shadow, fast convergence and easy operation.

2. Basic Theory

2.1 Image Encryption Based on Joint Transform Correlation System

Fig. 1 is a schematic diagram of JTC encryption technique based on double random phase. We describe it in a one-dimensional form for convenience. Here we let $f(x) = \exp[i2\pi n_1(x)]$ and $g(x) = \exp[i2\pi n_2(x)]$ be two random phase masks. When the image $h(x)$ passes through the first random phase mask $f(x)$, we can obtain $\varphi(x) = h(x)f(x)$, which is placed at $x = a$, and the second random phase mask g(x) is at $x = b$. When the parallel light is irradiated, the CCD can receive the joint power spectrum density, and it is the encrypted ciphertext $H(f)$.

$$H(f) = \left|FT[\varphi(x-a) + g(x-b)]\right|^2, \tag{1}$$

where $FT[]$ is the Fourier transform.

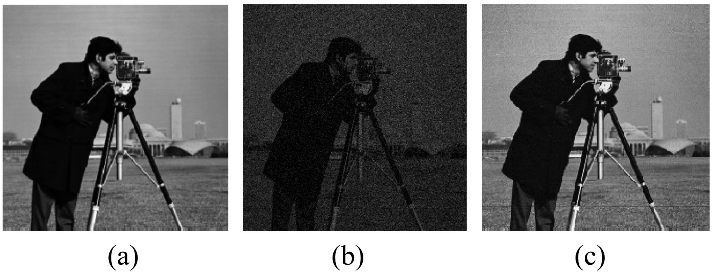


Fig. 2. Comparison results of the decrypted images of the JTC system before and after the improvement.

Decrypting the encrypted image requires another 4f system. We place the second random phase mask at $x = b$ of the input plane, and place the joint power spectrum at the back focal plane of the first lens. Then the decrypted information can be obtained at the output plane and the formula is as follows:

$$\xi(f) = H(f)G(f)\exp(-i2\pi bf). \tag{2}$$

Then we perform an inverse Fourier transform on $\xi(f)$ to get $\varepsilon(x)$:

$$\varepsilon(x) = IFT[\xi(f)]. \tag{3}$$

Where $IFT[]$ is inverse Fourier transform, and $G(f)$ is the Fourier transform result corresponding to $g(x)$. And we can get the information at the output plane.

Although the image can be encrypted and decrypted, the decrypted image has serious noise and cannot completely recover the details of the image, so it should be optimized. Noise is due to the autocorrelation and cross-correlation of information, so we should remove the nonlinear and zero-order terms of the system [24]. The encrypted image with the nonlinear term and the zero-order term removed is:

$$H_2(f) = \frac{H(f) - |\psi(f)|^2 - |G(f)|^2}{|G(f)|^2}. \tag{4}$$

Then we place the new image at the location of the ciphertext in the decryption system. Under the illumination of the parallel light, the following expression will be obtained:

$$\xi_2(f) = H_2(f)G(f)\exp(-i2\pi bf). \tag{5}$$

We can get the information of the decrypted image we need at $x = a$ on the output place. At the same time, the nonlinear term and the zero-order term are also removed, which greatly improves the quality of the decrypted image. Fig. 2 is a comparison result of the decrypted images of the JTC system before and after the improvement. Where Fig. 2(a) is the original image, Fig. 2(b) is the decrypted image before the improvement, and Fig. 2(c) is the decrypted image after the improvement.

2.2 Ptychography System

PIE proposed by Rodenburg *et al* is an improvement to traditional imaging CDI [25]. Unlike CDI, it replaces a single diffraction image with many diffraction images. It uses the movement of the sample relative to the aperture to eliminate the blurring problem of a single diffraction image [26].

PIE is a method of recording sample diffraction images [27], so there is no need for an imaging lens, which can break through the extreme resolution of lens imaging. At the same time, the imaging method avoids the interference device in the holographic imaging, and relies on the deconvolution operation to obtain the phase information of the image to recover the original image.

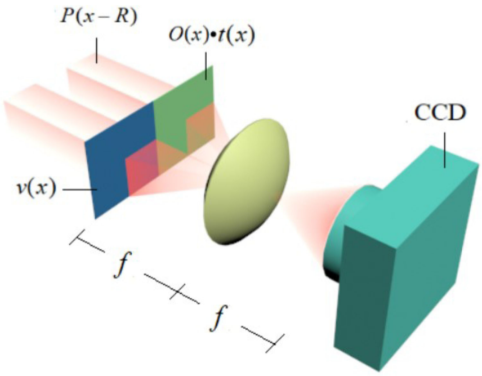


Fig. 3. Encryption system based on PIE and JTC.

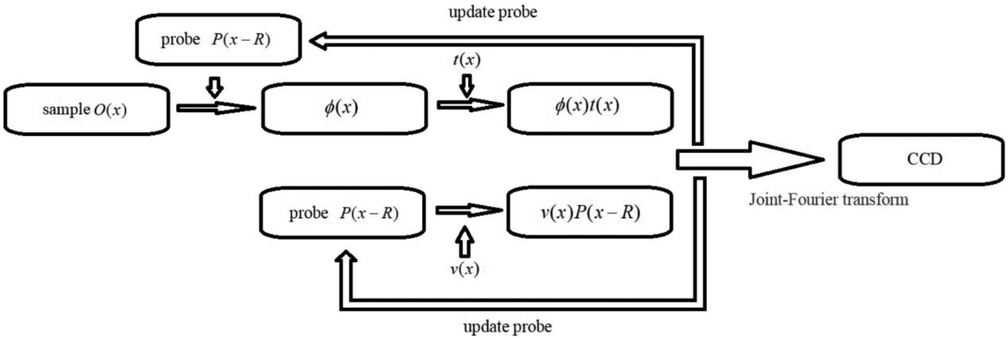


Fig. 4. Encryption flow chart.

The PIE often uses a focusing device such as an aperture diaphragm to turn the illumination into a regular, energy-concentrated beam that illuminates a portion of the sample. This beam is called a light probe. The optical probe scans the sample in a regular manner according to a certain rule, and the distance of each movement should not be greater than the width of the whole probe to reach overlapping effects [28]. After illuminating the sample, the transmitted light diffracts over a distance and is recorded by CCD. We rely on these diffraction images to achieve the reduction of the sample, which is the method of PIE [29].

3. New Image Encryption System Based on Joint Transformation Correlation and Ptychography

Joint Transform ptycholography encryption system combines PIE with JTC image encryption technology and each diffraction image in the PIE is encrypted by JTC. The reconstructed image needs to be decrypted with the corresponding key and then restored according to the PIE. Fig. 3 is a device diagram of the encryption system and Fig. 4 is a flow chart for the encryption. The encrypted ciphertext is received and saved by the CCD, and the ciphertext recipient can reconstruct image by using the ciphertext information on the computer according to the method proposed in this paper. We describe it in a one-dimensional form for convenience and the specific steps are as follows.

1) First, we give the initial guess to $O_g(x)$ for the sample $O(x)$ to be recovered, such as the full 1 matrix and the subscript g indicates that this function is a function of guessing. The distance of the light probe moves each time is R (R is a value smaller than the width of the optical probe), the optical probe can be expressed as $P(x-R)$.

2) The outgoing light after the light probe illuminates the sample can be expressed as [30]

$$\phi_g(x) = O_g(x)P(x-R). \tag{6}$$

3) Here we let $t(x)$ and $v(x)$ be two random phase masks, $t(x) = \exp[i2\pi m_1(x)]$, $v(x) = \exp[i2\pi m_2(x)]$. When the image $\phi_g(x)$ passes through the first random phase mask $t(x)$, the input image is obtained as $k_g(x) = \phi_g(x)t(x)$. It is placed at the $x = a$, while the second random phase mask $v(x)$ is placed at $x = b$ on the input plane. We can get the joint power spectral density at the back focal plane of the lens:

$$E_g(u) = \left|FT[k_g(x-a) + v(x-b)]\right|^2. \tag{7}$$

4) Denoising it with the method in JTC encryption:

$$E_{g2}(u) = \frac{E_g(u) - \left|K(u)\right|^2 - \left|V(u)\right|^2}{\left|V(u)\right|^2}, \tag{8}$$

where $|K(u)|^2$ and $|V(u)|^2$ are the autocorrelation power spectral densities of $k_g(x)$ and $v(x)$, respectively.

5) Replace the amplitude of $E_{g2}(u)$ by the intensity of the diffraction image, but preserve the phase, we can obtain,

$$E_{c2}(u) = \sqrt{I}\,\frac{E_{g2}(u)}{\left|E_{g2}(u)\right|}. \tag{9}$$

where I is the intensity of the diffraction image and subscript c means the function is after the correction.

6) Decrypt image using JTC decryption method:

$$D_{c2}(u) = E_{c2}(u)V(u)\exp(-i2\pi bu), \tag{10}$$

$$d_{c2}(x) = IFT[D_{c2}(u)]. \tag{11}$$

7) At the position of $x = a$, we can find the information we need. And then according to the phase plate $t(x)$, we can get the decrypted information, which is recorded as $\phi_c(x)$.

8) Update the sample function with the update function:

$$O_{g+1}(x) = O_g(x) + \frac{\left|P(x-R)\right|}{\left|P_{\max}(x-R)\right|}\,\frac{P^*(x-R)}{[\left|P(x-R)\right|^2 + \alpha]} \times \beta[\phi_c(x) - \phi_g(x)]. \tag{12}$$

where α adjusts the denominator to make it non-zero, β is used to adjust the ratio between the old and new values in the update function and generally it can be set 1. $|P_{\max}(r-R)|$ represents the maximum value of the amplitude in $P(r-R)$, which is used to eliminate the influence of the unevenness of the illumination on the system.

9) Move the optical probe and use the updated sample function as the initial guess for the next sample. Continue the above steps 2–8 to update the guess sample.

10) When the probe traverses the entire sample, an iterative process is completed and the sample function is all updated once. The updated sample function is used as the initial guess at the beginning of the next iteration. Fig. 5 is a flow chart for performing an iteration.

4. Numerical Simulations

We use simulations to analyze the effects of the proposed method. The experimental platform is matlab (R2016a), the size of the original image is 256 × 256 pixels, and the size of the probe used for encryption is 150 × 150 pixels. Each probe moves at a distance of 52 pixels, and the sequence is scanned from left to right and from top to bottom, so the CCD will receive 9 encrypted images. Fig. 6(a)–6(i) are all images obtained after encryption in the experiment. Fig. 7(a)–7(d) are the original image for the experiment, the first random phase plate, the second random phase

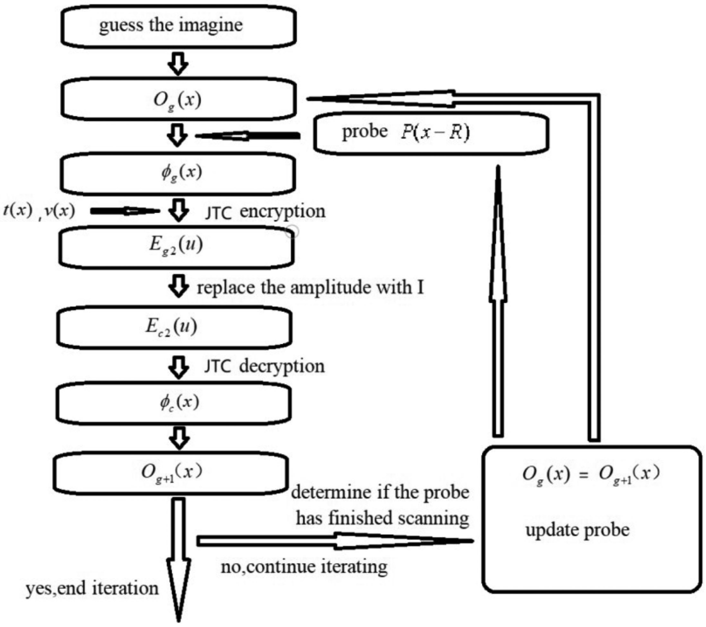


Fig. 5. Flowchart of the decryption process with one iteration.

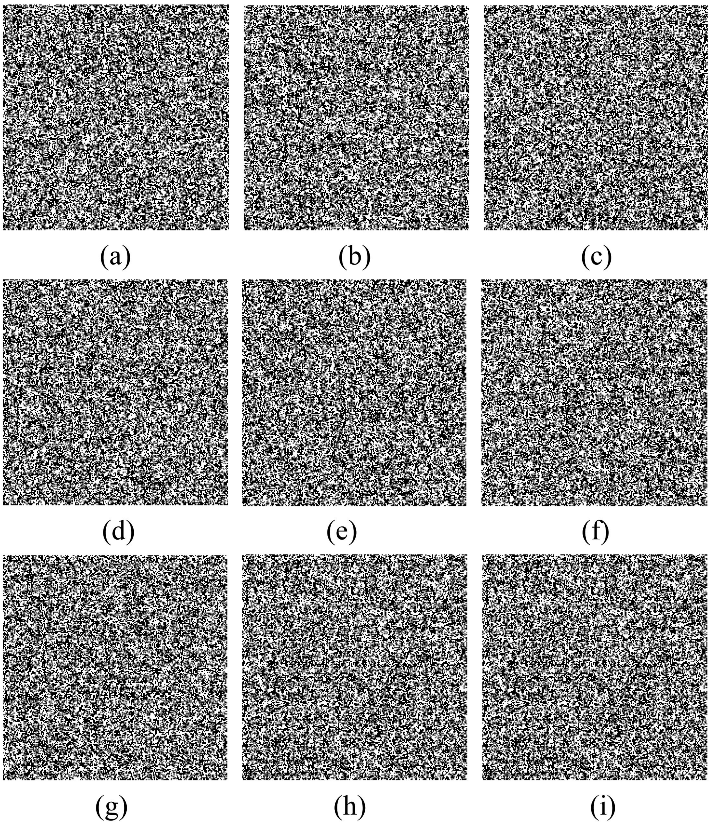


Fig. 6. All the encrypted images after PIE.

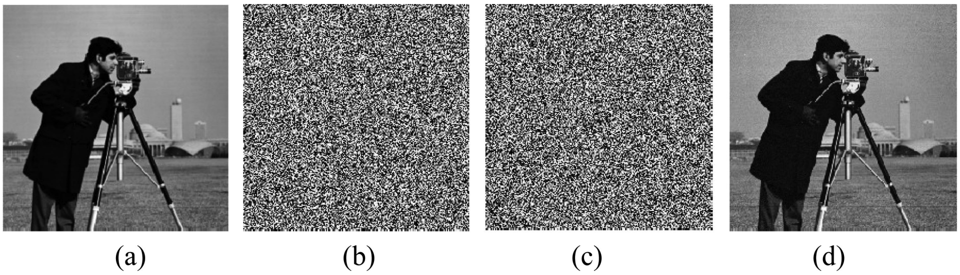


Fig. 7. Encryption and decryption images. (a) Original image, (b) the first phase plate, (c) the second phase plate, (d) the decrypted image.

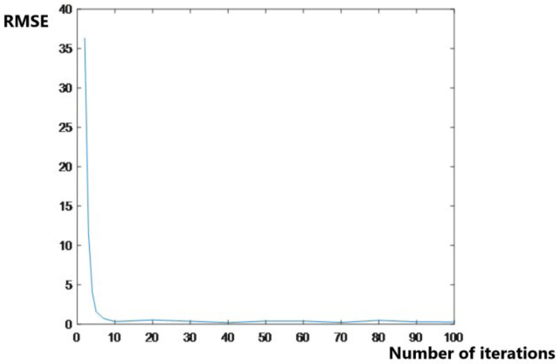


Fig. 8. Relationship between the number of iterations and the RMSE.

plate, and the reconstructed image, respectively. It can be seen from the simulation that the effect of encryption and decryption of the image is very obvious, and the encrypted image cannot distinguish any information at all.

In order to analyze the image restoration effect more intuitively, we introduce the root mean square error (RMSE), which is used to evaluate the image decryption quality or the image restoration quality. The parameter is expressed as follows:

$$RMSE = \sqrt{\frac{\sum_{y=1}^{N} \sum_{x=1}^{M} [I_1(x, y) - I_0(x, y)]^2}{M \times N}}. \tag{13}$$

where $I_0(x, y)$ and $I_1(x, y)$ represent the original image and the reconstructed image, respectively, and $M \times N$ represents the pixel size of the image. The smaller the value of RMSE, the closer the restored image is to the original image and the better the quality is. Fig. 8 is a graph showing the relationship between the number of iterations and RMSE when restoring an image. We can see that as the number of iterations increases, the RMSE decreases rapidly. When the number of iterations reaches a certain number, as the number of iterations increases, the RMSE remains almost unchanged, and it can be judged that convergence has been reached at this time. Fig. 7(d) shows the image after decryption and reconstruction, and its RMSE value is 0.3285, which better proves the effect of image restoration.

When two random phase plates are wrong, decrypting in the same way will result in an erroneous result, as shown in Fig. 9. It can be found that no matter whether one of the phase plate information is wrong or the two phase plates information are wrong, the original image cannot be decrypted and reconstructed.

When the encrypted image is cut, it will affect the image decryption and reconstruction. The simulation here is that all ciphertexts are cut to the same extent and at the same position. The

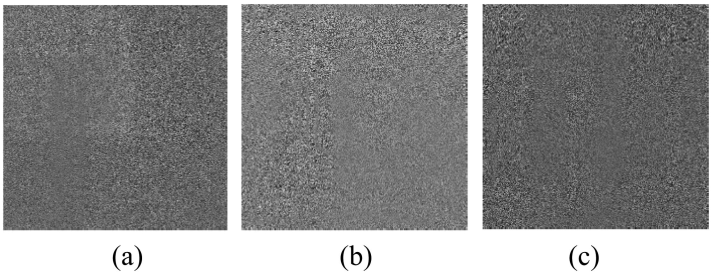


Fig. 9. Wrong decrypted images. (a) The first phase plate is wrong, (b) the second phase plate is wrong, (c) two phase plates are both wrong.

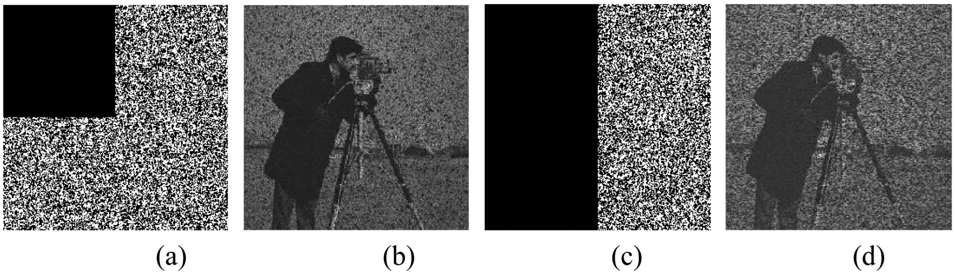


Fig. 10. Simulation results when the ciphertext is cut by different situations. (a), (c) are different shear degrees and (b), (d) are the results.

experimental results are shown in Fig. 10. Fig. 10(a)–10(d) show the reconstructed images when the ciphertexts are subjected to different degrees of clipping. Although some of the information is lost in the ciphertexts, the main information of the reconstructed image can still be effectively identified. It can be seen that the system is robust to shearing and the information contained in the ciphertexts are not concentrated in one place and image restoration is only related to the amount of clipping rather than position.

The above is the impact of JTC encryption technology on the system security. Although PIE is an image recovery and reconstruction technology, when it is used to an encryption system, the scanning process of the probe also plays a certain role in the security of the system. If the parameters used in the reconstruction process are inconsistent with the parameters used in the encryption, the reconstructed image will not be the best recovery state, and even the main information of the image cannot be discerned at all. Because each image has a corresponding position during the recovery process and has partial information of adjacent images, when the image information fails to be in the corresponding position for various reasons, the common information portion of the adjacent image will overlaps, resulting in the inability to recover the correct image. Fig. 11 shows the image obtained by decrypting and reconstructing the probe in the wrong scan order. We can't get the information of the original image and it indicates that the order of the probes has an impact on the security of the encryption system. We must use the correct probe scan order to get the decrypted image. It can be seen that if the probe moving distance is reduced during encryption, the number of movements of the probe is increased, and the out-of-order scanning will greatly increase the unpredictability of the system, and the security of the system will also be improved. However, the number of ciphertexts that need to be transmitted will be greatly increased, and we require more stable transmission.

Not only the scan order of the probe, but also the shape and size of the probe can be the key of the system. Fig. 12 shows the shape of the probe changed to 39 × 256 pixels, and the reconstructed image is decrypted after each probe moves by 27 pixels. Because the information is different due to the shape of the probe, it will have a big impact on image recovery, even unable to recover the

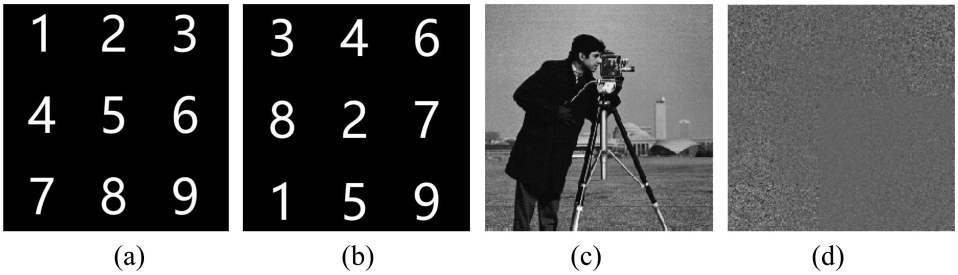


Fig. 11. Decrypted images when the probe sequence is wrong. (a)–(b) Probe sequences, (c)–(d) corresponding decrypted images.

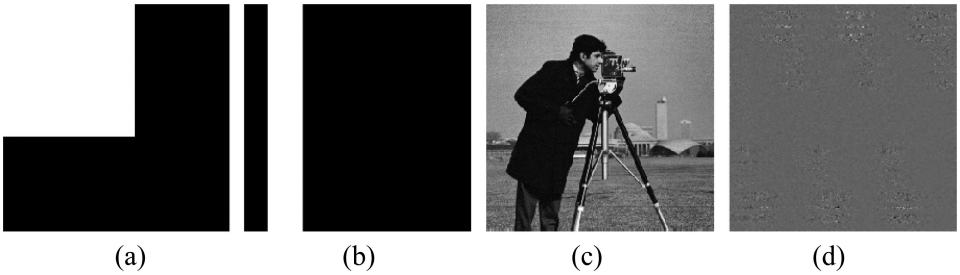


Fig. 12. Decrypted images when the probe shape size is wrong. (a)–(b) 2 different shapes of probes, (c)–(d) their corresponding decrypted images.

image. As we can see from the Fig. 12(d), we can't get an identifiable image, so the shape of the probe is also one of the keys of the system.

5. Conclusion

This paper proposes an image encryption system based on JTC and PIE. The method avoids optical interference and has no strict requirements on the spatial arrangement of the components, which simplifies the arrangement and operation. The system has a large number of keys, and the image can be restored only when all the keys are correct, so that the system has better security. The output of the system is in the form of images, which has good compatibility with the transmission system and other systems, and it is easy to play a role in other fields.

References

[1] D. L. Misell, "A method for the solution of the phase problem in electron microscopy," *J. Phys. D.*, vol. 6, no. 1, pp. L6–L9, 1973.

[2] J. N. Clark, X. Huang, R. J. Harder, and I. K. Robinson, "Continuous scanning mode for ptychography," *Opt. Lett.*, vol. 39, no. 20, pp. 6066–6069, 2014.

[3] L. Bian, J. Suo, G. Situ, G. Zheng, F. Chen, and Q. Dai, "Content adaptive illumination for Fourier ptychography," *Opt. Lett.*, vol. 39, no. 23, pp. 6648–6651, 2014.

[4] A. M. Maiden, M. J. Humphry, F. C. Zhang, and J. M. Rodenburg, "Superresolution imaging via ptychography," *J. Opt. Soc. Amer. A*, vol. 28, no. 4, pp. 604–612, 2011.

[5] W. Chen, Z. L. Jiang, C. Liu, and J. Q. Zhu, "Depth resolved imaging by 3PIE with dual-beam illumination," *Acta Optica Sinica*, vol. 36, no. 8, 2016, Art. no. 0811002.

[6] W. H. Xu, H. F. Xu, Y. Luo, T. Li, and Y. S. Shi, "Optical watermarking based on single-shot-ptychography encoding," *Opt. Exp.*, vol. 24, no. 24, pp. 27922–27936, 2016.

[7] J. Zhang, Z. Wang, T. Li, A. Pan, Y. Wang, and Y. Shi, "3D object hiding using three-dimensional ptychography," *J. Opt.*, vol. 18, no. 9, 2016, Art. no. 095701.

[8] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, 2013.

[9] B. Javidi and P. Refregier, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[10] X. G. Wang, G. Q. Zhou, C. Q. Dai, and J. L. Chen, “Optical image encryption with divergent illumination and asymmetric keys,” *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7801908.

[11] H. Chen, C. Tanougast, Z. J. Liu, W. Blondel, and B. Hao, “Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform,” *Opt. Lasers Eng.*, vol. 107, pp. 62–70, 2018.

[12] Y. Qin and Y. Y. Zhang, “Information encryption in ghost imaging with customized data container and XOR operation,” *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7802208.

[13] L. Sui, Y. Cheng, B. Li, A. Tian, and A. Asundi, “Optical image encryption via high-quality computational ghost imaging using iterative phase retrieval,” *Laser Phys. Lett.*, vol. 15, no. 7, 2018, Art. no. 075204.

[14] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.

[15] W. Chen and X. Chen, “Optical color-image verification using multiple-pinhole phase retrieval,” *J. Opt.*, vol. 16, no. 7, 2014, Art. no. 075403.

[16] A. J. Osorio *et al.*, “Improved decryption quality with a random reference beam cryptosystem,” *Opt. Lasers Eng.*, vol. 112, pp. 119–127, 2019.

[17] H. Chen *et al.*, “Opto-digital spectrum encryption by using Baker mapping and gyrator transform,” *Opt. Lasers Eng.*, vol. 66, pp. 285–293, 2015.

[18] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” *Opt. Eng.*, vol. 39, no. 8, pp. 2031–2035, 2000.

[19] L. M. Cecilia and I. Claudio, “Optical encryption using phase-shifting interferometry in a joint transform correlator,” *Opt. Lett.*, vol. 31, no. 17, pp. 2562–2564, 2006.

[20] J. J. Cai, X. J. Shen, and C. Fan, “Joint transform correlator-based optical cryptosystem with innovative arrangement of input,” *Opt. Lasers Eng.*, vol. 110, pp. 431–436, 2018.

[21] X. Huang, H. Yan, R. Harder, Y. H. Wu, I. Robinson, and Y. Chu, “Optimization of overlap uniformness for ptychography,” *Opt. Exp.*, vol. 22, no. 10, pp. 12634–12644, 2014.

[22] P. Sidorenko and O. Cohen, “Single-shot ptychography,” *Optica*, vol. 3, no. 1, pp. 9–14, 2016.

[23] F. Pfeiffer, “X-ray ptychography,” *Nature Photon.*, vol. 12, no. 1, pp. 9–17, 2018.

[24] J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, “Improved decryption quality and security of a joint transform correlator-based encryption system,” *J. Opt.*, vol. 15, no. 2, 2013, Art. no. 025401.

[25] A. M. Maiden and J. M. Rodenburg, “An improved ptychographical phase retrieval algorithm for diffractive imaging,” *Ultramicroscopy*, vol. 109, no. 10, pp. 1256–1262, 2009.

[26] Y. Zhang, W. Jiang, and Q. Dai, “Nonlinear optimization approach for Fourier ptychographic microscopy,” *Opt. Exp.*, vol. 23, no. 26, pp. 33822–33835, 2015.

[27] J. M. Rodenburg, “Ptychography and related diffractive imaging methods,” *Adv. Imag. Elect. Phys.*, vol. 150, no. 7, pp. 87–184, 2008.

[28] X. Li *et al.*, “Optical encryption via monospectral integral imaging,” *Opt. Exp.*, vol. 25, no. 25, pp. 31516–31527, 2017.

[29] H. M. L. Faulkner and J. M. Rodenburg, “A phase retrieval algorithm for shifting illumination,” *Appl. Phys. Lett.*, vol. 85, no. 20, pp. 4795–4797, 2004.

[30] P. Li and A. Maiden, “Multi-slice ptychographic tomography,” *Sci. Rep.*, vol. 8, no. 1, 2018, Art. no. 2049.