Optics Communications 431 (2019) 203–209

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain

Chao Wu [a], Ying Wang [a], Ye Chen [a], Jun Wang [a,*], Qiong-Hua Wang [b]

[a] Sichuan University, School of Electronics and Information Engineering, Chengdu 610065, China
[b] School of Instrumentation Science and Opto-electronics Engineering, Beihang University, Beijing 100083, China

ARTICLE INFO

Keywords:
Multiple-image encryption
Compressed sensing
Asymmetric encryption
Cylindrical diffraction

ABSTRACT

In this paper, an asymmetric multiple-image encryption algorithm based on compressed sensing and cylindrical diffraction is proposed. Firstly, these multiple gray scale images are compressed by compressed sensing in separately. Then single amplitude ciphertext is obtained by asymmetric operation of phase truncation after cylindrical diffraction. This method not only can achieve multiple-image encryption with a small amount of data, but also can prevent information disclosure. Moreover, the proposed method has high security because it can resist the phase-retrieval attack. Numerical simulations have demonstrated the security and effectiveness of the proposed method.

1. Introduction

In recent years, optical information security has attracted more and more attention owing to the power of high-speed, parallelism, and high encryption dimension of optical encryption [1–3]. In 1995, double random phase encoding (DRPE) based on 4-f system was firstly proposed by Refregier and Javidi which has become a widely adopted optical encryption technique [4].

However, some research results indicated that the DRPE encryption approach is the linear symmetric encryption system which cannot effectively resist various attacks including the chosen-plaintext attack and known-plaintext attack [5–7]. To enhance the security, various methods have been proposed such as the Fresnel transform [8], the fractional Fourier transform [9], the fractional Mellin transform [10], and the gyrator transform [11]. Other methods such as the mixed phase amplitude encoding [12], the pixel randomization processing [13], the phase truncation Fourier transform [14,15], the random sampling [16] and the phase truncation operations [17] have also been proposed to improve the DRPE-based optical security systems. Previously, we proposed asymmetric cylindrical diffraction [18] to ensure the DPRE based cryptosystem will resist phase retrieval attack. Owing to nonlinear characteristics of cylindrical diffraction, the image encryption system based on cylindrical diffraction overcomes the symmetry of the plane diffraction encryption system. Therefore, it can resist the ciphertext-only attack even the plaintext attack, and is not affected by phase-retrieval attack [19]. In addition, the internal radius, height and diffraction distance of the cylindrical diffracted cylinder can be used as an additional key to the encryption system to further improve the security of the system.

Nowadays, single image encryption is not enough to meet people's requirements, so optical encryption systems have evolved into multiple-image encryption in the recent decade. Various techniques for multiple-image encryption have been proposed [20–24]. Unfortunately, for these methods, ciphertext is easy to be cracked, which significantly reduces the security of the method. Recently, Zhao et al. proposed a multiple-image encryption approach based on the position multiplexing of Fresnel phase [25]. The propagation distances of Fresnel phases can generate corresponding encryption keys which are used as encryption filters in typical 4-f system. The advantage of this method is no requiring, iteration and simple structure. Tang et al. proposed a multiple-image encryption scheme with bit-plane decomposition and chaotic maps, which can retrieve lossless original images from the encrypted images [26]. Wu et al. have introduced a novel multiple-image encryption method based on the computational ghost imaging and position multiplexing to improve the multiplexing capacity effectively [27]. However, the problem of data volume in multiple-image encryption has not been improved.

We proposed a new method for multiple-image asymmetric encryption based on compressed sensing (CS) and nonlinear operations in cylindrical diffraction domain. To the best of our knowledge, the cylindrical diffraction has not been used for multiple-image encryption so far. The proposed method uses the cylindrical diffraction to encrypt multiple-images, which can greatly improve the security such as free of phase retrieval attack and information disclosure. At the same time, the adoption of compressed sensing reduces the amount of data, which is more conducive to data transmission and increases the practicability of the system. The asymmetric keys for encryption and decryption also

* Corresponding author.
E-mail address: jwang@scu.edu.cn (J. Wang).

https://doi.org/10.1016/j.optcom.2018.09.034
Received 22 August 2018; Received in revised form 14 September 2018; Accepted 15 September 2018
Available online 19 September 2018

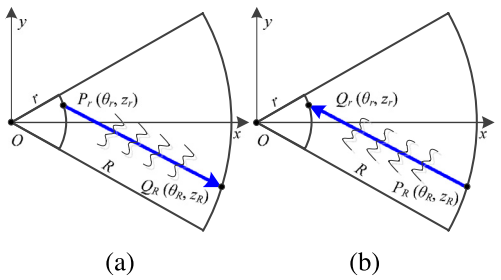

Fig. 1. The schematic diagram of cylindrical diffraction with top-view. (a) IOP Model, (b) OIP Model.

lead to security enhancement. In addition, the final encrypted result to be transmitted is an amplitude-only image which is convenient for recording and saving.

2. Principles of the method

2.1. Phase-truncation in cylindrical diffraction domain (PT-CyD)

The cylindrical diffraction (CyD) is a nonlinear mode of diffraction propagation. As shown in Fig. 1, the object surface and the observation surface are the inner surface and outer surface of two concentric cylinders in separately. And R and r denote the radii of the inner and outer surfaces, respectively. Hence, there are two propagation models which are propagation from inside to outside and from outside to inside as shown in Fig. 1(a) and (b), respectively.

For the inside-out propagation (IOP) model, $P_r(\theta_r, z_r)$ and $Q_R(\theta_R, z_R)$ represent the object and observation points in cylindrical coordinate, respectively. For the outside-in propagation (OIP) model, $P_R(\theta_R, z_R)$ and $Q_r(\theta_r, z_r)$ represent the object and observation points in cylindrical coordinate, respectively. z_r and z_R are in range of $-H/2$ to $H/2$, where H is the height of the cylindrical surface. The diffraction integral formulas of the two models are as follows:

$$\begin{aligned} u_R(\theta_R, z_R) &= C \iint_s u_r(\theta_r, z_r) \frac{\exp(ikd_{P_rQ_R})}{d_{P_rQ_R}} d\theta_r dz_r \\ &= CyD_r(u_r(\theta_r, z_r)) \dots \text{IOP}, \end{aligned} \tag{1}$$

$$\begin{aligned} u_r(\theta_r, z_r) &= C \iint_s u_R(\theta_R, z_R) \frac{\exp(ikd_{P_RQ_r})[r - R\cos(\theta_r - \theta_R)]}{d^2_{P_RQ_r}} \\ &\quad \times d\theta_R dz_R \\ &= CyD_R(u_R(\theta_R, z_R)) \dots \text{OIP}, \end{aligned} \tag{2}$$

$$d = d_{P_rQ_R} = d_{P_RQ_r} = [R^2 + r^2 - 2Rr\cos(\theta_R - \theta_r) + (z_R - z_r)^2]^{1/2}, \tag{3}$$

where k denote the wavenumber of the incident light and C denote a constant. The distance is represented by d which are between two points of P and Q on the object and observation surfaces, respectively. The s denotes the object surface.

Take the OIP model as an example, the principle for the phase-truncation based on cylindrical diffraction is as follows:

$$A(\theta_r, z_r) = PT\{CyD_R[f(\theta_R, z_R) \cdot R_1(\theta_R, z_R)]\}, \tag{4}$$

$$P(\theta_r, z_r) = PR\{CyD_R[f(\theta_R, z_R) \cdot R_1(\theta_R, z_R)]\}, \tag{5}$$

where $PT(\bullet)$, $PR(\bullet)$ and $P(\theta_r, z_r)$ denote the phase truncation operation, the phase reservation operation and the private key in the process of the decryption, respectively.

2.2. Compressed sensing

Compressed sensing [28,29] theory holds that if the signal is sparse, then it can be reconstructed by the sampling point which is far below the sampling theorem. It should be noted that in CS, we do not have any information about the pixel domain of the original signal, only the observation domain information. The most commonly applied model we use currently is getting sparse signal α through a dictionary ψ. ψ is generally a transform base or orthonormal basis, and a is sparse. The correlation calculation can be expressed as

$$\alpha = \psi^T x, \tag{6}$$

where $\psi = [\psi_1, \psi_2, \dots, \psi_N]$ denote an orthonormal basis, and α is the representation of x in ψ.

If there are only k nonzero items in x, then the sparsity of the signal in ψ is k. To enhance the sparsity of the transformed signal, ψ is an over complete dictionary ordinarily. Then measurement(observation) matrix which is $M \times N$ and not related to the ψ is used to get a linear projection measurement, and the measured value of y which is M dimension is obtained.

$$y = \Phi x = \Phi\psi\alpha, \tag{7}$$

where $\Theta = \Phi\psi$, called the perception matrix.

In the process of reconstruction, Θ must satisfy the restricted isometry property (RIP) [30]. The RIP isometric constant δ_k in the measurement matrix is defined to satisfy the minimum value of Eq. (8)

$$(1 - \delta_k)\|x\|_2^2 \le \|\Phi x\|_2^2 \le (1 + \delta_k)\|x\|_2^2, \tag{8}$$

where the $\delta_k \in [0,1]$. If $\delta_k < 1$, the measurement matrix satisfies kth order RIP.

It is important to note that the reconstruction of CS (restoring the original signal x) is the way to solve the underdetermined equations $y = \Phi x$. The common reconstruction algorithms, such as base tracking (BP) [31], orthogonal matching tracking (OMP) [32], and smooth L0 (SL_0) [33], etc. Which has been used to restore x from y.

3. Process of encryption and decryption

3.1. Process of encryption

The proposed multiple-image encryption scheme based on CS and the phase-truncation in cylindrical diffraction is shown as Fig. 2. Take four images for example, assuming $I_i(x, y)$ (i = 1, 2, 3, 4) whose size are 256 × 256 pixels are located at the cylindrical surface with radius of R as input. The specific scheme is organized as follows:

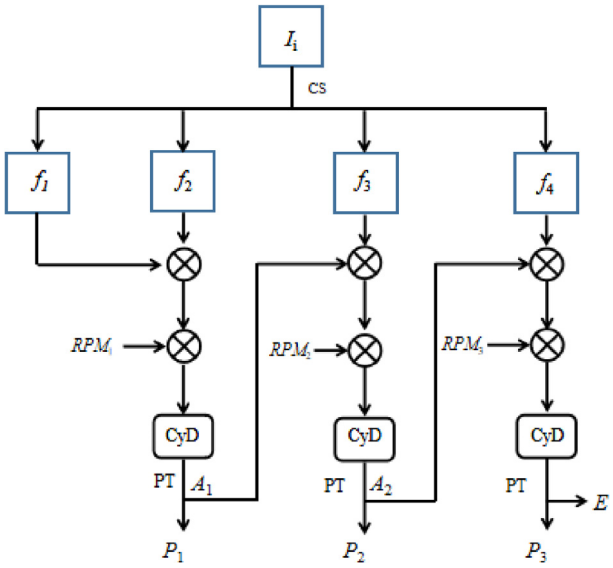

Fig. 2. The process of encryption.

Step 1: performing the CS on the four input images to obtain $f_i(m, n)$ (i = 1, 2, 3, 4) with 256 × 192 pixels. Where we use a measurement

matrix with 192 × 256 pixels to get a projection measurement in the process of CS, and there is a compression ratio of 1/4 for the ciphertext, obviously. Where the compression ratio represents the proportion of reduction for the picture size, relative to the original image.

Step 2: Obtaining $f_{12}(m, n)$ by integrating $f_1(m, n)$ and $f_2(m, n)$, in which $f_1(m, n)$ is the real part and $f_2(m, n)$ is the imaginary part. Then $f_{12}(m, n)$ is modulated by the random phase mask RPM_1. Adopting OIP model for cylindrical diffraction here, and f_{12} is transformed into cylindrical coordinate. The complex amplitude distribution $g_1(\theta_r, z_r)$ is obtained after a cylindrical diffraction operation, which is illuminated by the illuminating light with the wavelength λ.

$$f_{12}(m, n) = f_1(m, n) + j \cdot f_2(m, n), \tag{9}$$

$$g_1(\theta_r, z_r) = CyD_R\{f_{12}(\theta_R, z_R) \cdot RPM_1\}. \tag{10}$$

Step 3: $g_1(\theta_r, z_r)$ perform the phase truncation operation. The amplitudes $A_1(\theta_r, z_r)$ and the phases $P_1(\theta_r, z_r)$ are obtained by $PT(\bullet)$ and $PR(\bullet)$ operations.

$$A_1(\theta_r, z_r) = PT[g_1(\theta_r, z_r)] = PT\{CyD_R[f_{12}(\theta_R, z_R) \cdot RPM_2]\}, \tag{11}$$

$$P_1(\theta_r, z_r) = PR[g_1(\theta_r, z_r)] = PR\{CyD_R[f_{12}(\theta_R, z_R) \cdot RPM_2]\}, \tag{12}$$

where the phase part $P_1(\theta_r, z_r)$ act the private key of decryption.

Step 4: it is similar to Step 2, Integrating the $A_1(\theta_r, z_r)$ (real value) and $f_3(\theta_r, z_r)$ to obtain $f_{13}(\theta_r, z_r)$, Then $f_{13}(\theta_r, z_r)$ is modulated by the random phase mask RPM_2. The complex amplitude distribution $g_2(\theta_R, z_R)$ is obtained after a cylindrical diffraction operation, which is illuminated by the illuminating light with the wavelength λ. $g_2(\theta_R, z_R)$ perform the phase truncation operation. The amplitudes $A_2(\theta_R, z_R)$ and the phases $P_2(\theta_R, z_R)$ are obtained by $PT(\bullet)$ and $PR(\bullet)$ operations. Similarly, the cylindrical diffraction operation and the phase truncation operation are performed once again. For the sake of brevity, the result is directly given as follows:

$$E(\theta_r, z_r) = PT[g_3(\theta_r, z_r)] = PT\{CyD_R[f_{14}(\theta_R, z_R) \cdot RPM_3]\}, \tag{13}$$

$$P_3(\theta_r, z_r) = PR[g_3(\theta_r, z_r)] = PR\{CyD_R[f_{14}(\theta_R, z_R) \cdot RPM_3]\}, \tag{14}$$

where $E(\theta_r, z_r)$ is the ciphertext and $P_3(\theta_r, z_r)$ is also a private key of decryption.

3.2. Process of decryption

The decryption process is displayed in Fig. 3, which is similar to the encryption procedures but in the reversed order. The details of the decryption procedures can be described as follows:

Step 1: the encrypted image $E(\theta_r, z_r)$ is modulated by $P_3(\theta_r, z_r)$. The complex amplitude distribution $g_3'(\theta_R, z_R)$ is obtained after a cylindrical diffraction operation which is illuminated by the illuminating light with the wavelength λ.

$$g_3'(\theta_R, z_R) = CyD_R^{-1}\{E(\theta_r, z_r) \cdot P_3(\theta_r, z_r)\}, \tag{15}$$

where CyD^{-1} denotes the inverse process of CyD.

Step 2: $g_3'(\theta_R, z_R)$ is modulated by RPM_3^*. Taking the imaginary part as $f_4'(\theta_R, z_R)$, and the real part as $A_2'(\theta_R, z_R)$.

$$A_2'(\theta_R, z_R) + j \cdot f_4'(\theta_R, z_R) = g_3'(\theta_R, z_R) \cdot RPM_3^*. \tag{16}$$

Step 3: repeat the related operations until the $f_1'(\theta_R, z_R)$ is obtained. For the sake of brevity, the result is directly given as follows

$$g_2'(\theta_r, z_r) = CyD_r^{-1}\{A_2'(\theta_R, z_R) \cdot P_2(\theta_R, z_R)\}, \tag{17}$$

$$A_1'(\theta_r, z_r) + j \cdot f_3'(\theta_r, z_r) = g_2'(\theta_r, z_r) \cdot RPM_2^*, \tag{18}$$

$$g_1'(\theta_R, z_R) = CyD_R^{-1}\{A_1'(\theta_r, z_r) \cdot P_1(\theta_r, z_r)\}, \tag{19}$$

$$f_1'(\theta_R, z_R) + j \cdot f_2'(\theta_R, z_R) = g_1'(\theta_R, z_R) \cdot RPM_1^*. \tag{20}$$

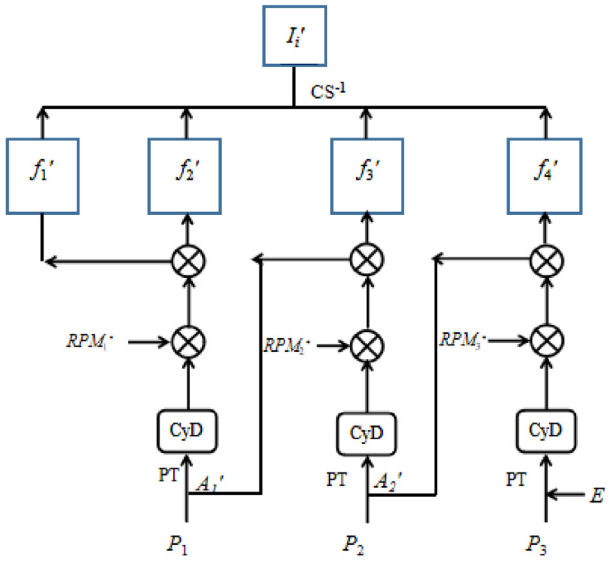

Fig. 3. The process of decryption.

Step 4: perform the CS inverse transform through a reconstruction algorithm, the Basis Pursuit (BP) method is used to obtain four decrypted images in this scheme.

It is obviously to see that the proposed method is an asymmetric multiple-image encryption system which the decryption phase keys P_1, P_2 and P_3 are different from the encryption keys.

3.3. Optical realization

The proposed system is also suggested for optical verification due to its simple optical implementation. A possible implemented device of the proposed scheme shows in Fig. 4. RPM_1, RPM_2 and RPM_3 denote random phase masks. Firstly, the spatial light modulator (SLM) inputs the original image in turn. After compressed and encrypted by CS, $I_1(x, y)$ and $I_2(x, y)$ are added as the real and imaginary parts of complex amplitude respectively. Repeating operation, finally through phase-truncation and phase-reservation operations based on cylindrical diffraction to obtain the encrypted image by CCD.

4. Simulation results

4.1. Encryption and decryption results

The related simulations are performed with Matlab 2017(a) to analyze the performance of proposed scheme on a 64-bit computer. In the procedure of CS, the measurement matrix ψ with 192 × 256 pixels is used to project original images. The original images and corresponding decryption images with 256 × 256 pixels shown in Fig. 5(a)–(d) and Fig. 5(e)–(h), respectively. And Fig. 5(a)–(d) show the keys for decryption and ciphertext. The corresponding decryption images are displayed in Fig. 5 in the PT-CyD method, the outer cylinder R, inner cylinder r and height H are respectively set as 200×10^{-3} mm, 10×10^{-3} mm and 32×10^{-3} mm. And the corresponding wavelength λ is set 12×10^{-6} mm. To evaluate the similarity between the plaintext I_i (i = 1, 2, 3, 4) and the decrypted image I_i' (i = 1, 2, 3, 4), correlation coefficient (CC) and PSNR are used. And the CC values and the PSNR values of the decrypted images show in Table 1.

$$CC = \frac{crco(I, I')}{\sigma_I \times \sigma_{I'}}, \tag{21}$$

$$PSNR = 10\lg\left[\frac{M \times N \times 255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - \mathrm{D}(i,j))^2}\right], \tag{22}$$

where *crco* denotes cross-covariance, and σ denotes standard deviation. The coordinates are omitted here. $M \times N$ denotes the image size.

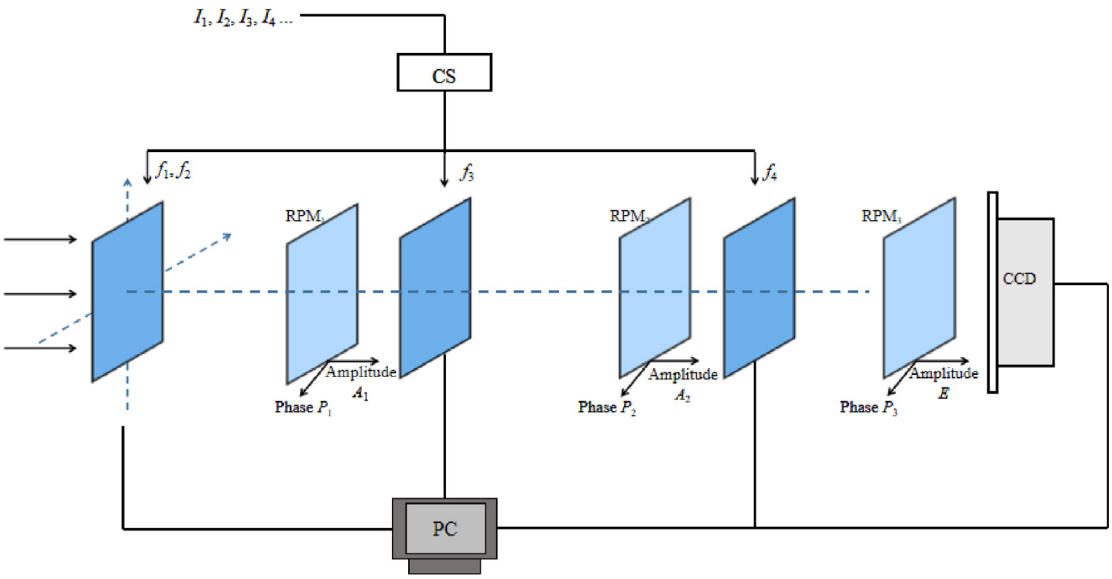

Fig. 4. A possible implemented device of the proposed method: SLM_1 denote spatial light modulator; RPM_1, RPM_2 and RPM_3 denote random phase masks.

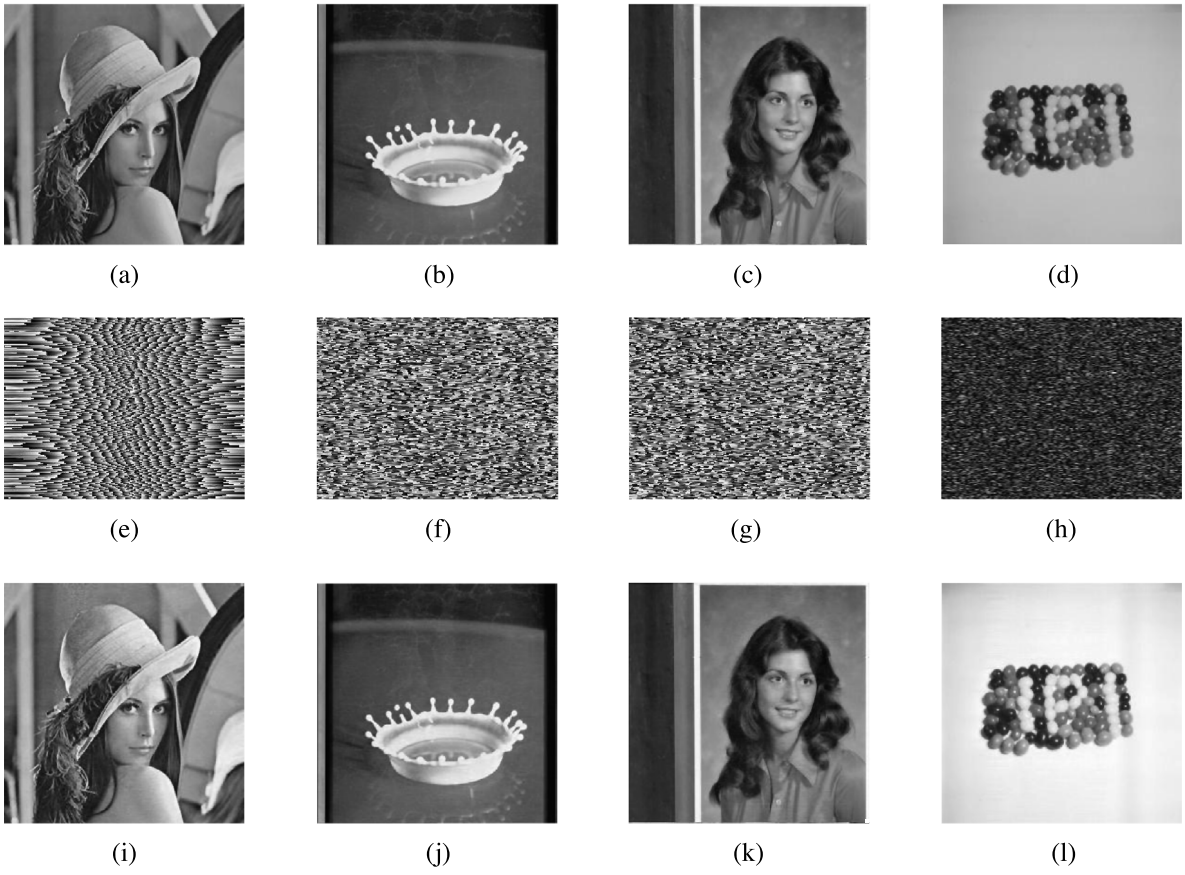

Fig. 5. Results of test images for the proposed algorithm: (a)–(d) original images; (e)–(g) keys for decryption; (h) ciphertext; (i)–(l) decrypted results.

4.2. Histogram

The image histogram is frequently used to evaluate the security and effectiveness of an image encryption algorithm. The histogram of original images and encrypted image are shown in Fig. 6. It is obviously that the histogram of encrypted image is significantly different from that of original image. Therefore, it does not provide any clues to employ statistical attack.

4.3. Security analysis

4.3.1. Key sensitivity analysis

In general, the sensitivity to the secret keys is used to measure whether the encryption system is stable. For the sake of brevity, only the decryption image 'Lena' is displayed in each test process. Fig. 7(a) shows the decrypted images with the inner cylinder r under a tiny deviation Δr while other keys remain correct, i.e., $r + \Delta r$, while keeping other ones

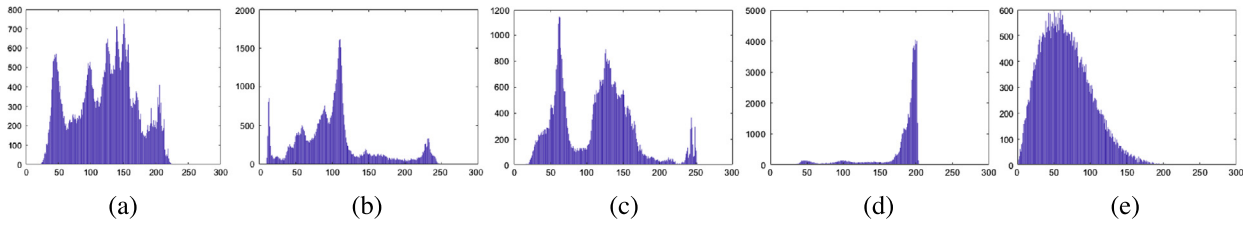

Fig. 6. Histograms: (a)–(d) original images; (e) encrypted image.

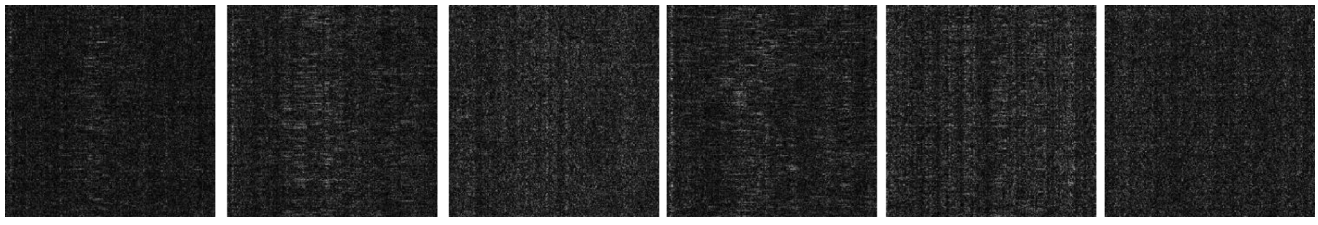

Fig. 7. The decrypted images 'Lena' with incorrect keys: (a) $\Delta r = 0.001 \times 10^{-3}$ mm; (b) $\Delta R = 0.001 \times 10^{-3}$ mm; (c) $\Delta H = 0.0001 \times 10^{-3}$ mm; (d) $\Delta\lambda = 0.001 \times 10^{-6}$ mm; (e) incorrect P_3; (f) incorrect RPM_3.

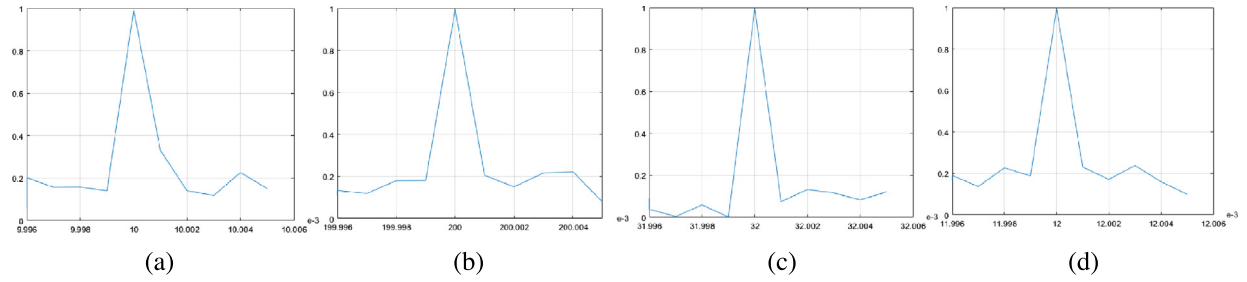

Fig. 8. CC values of the decrypted images with incorrect keys: (a) r; (b) R; (c) H; (d) λ.

unchanged, the correct decrypted image cannot be recovered. Similarly, varying the parameters of R, H, λ, P_3 and the RPM_3 shown in Fig. 7(b)–(f). And the CC values of the decrypted images with incorrect keys are shown in Fig. 8. Obviously, it can be seen that correct decrypted images cannot be obtained when these keys are wrong (see Fig. 7).

4.3.2. Test of information disclosure

In the process of image transmission, information leakage may be unavoidable. In this section, digital simulations are conducted to show the effectiveness of the proposed method under the resource-limited situation. The information disclosure problem of the decryption keys is investigated. When the keys or ciphertext are placed in the verification system, the decrypted images in the output plane can be shown in Fig. 9. When the phase key P_1 and P_2 are placed in the verification system, the reconstructed image by performing a CyD is shown in Fig. 9(a). When the encrypted distribution E, the phase key P_1 and P_2 are located in their corresponding places, the decrypted image with the absence of the phase key P_2 in the verification system is shown in Fig. 9(b). Similarly, the image reconstructed from P_1, P_2 and P_3 with the absence of the encrypted distribution E is illustrated in Fig. 9(c). Fig. 9(d) is the reconstructed image by performing a CyD on the phase key obtained by imaginary part truncation in the Fourier domain. The results show that the above four cases cannot successfully decipher the correct image. For the sake of brevity, only one decryption diagram is displayed in each test process.

4.3.3. Capacity of image encryption

The proposed method can encrypt more images. The process of the 8 pictures is as follows to prove the rationality and feasibility of the method. The amount of time spent in the process of different numbers of pictures is shown in Table 2. It is easy to see that there is not much difference in the time spent on each encryption process. Fig. 10 shows the results of the eight decrypted images. Obviously, the CC values, which represent the average CC values of every decryption result, show that the decryption effect of this method is good.

Table 1
CC values and PSNR values of the decrypted images.

	Lena	Milk	Girl	Candy	Resolution
CC	0.9929	0.9928	0.9947	0.9955	256 × 256
PSNR	35.37	38.97	39.69	40.82	

Table 2
CC values of the decrypted images and the time of encrypted process.

	Four images	Five images	Six images	Seven images	Eight images
Time	0.6012	0.7731	0.9360	1.0010	1.1755
CC	0.9933	0.9944	0.9937	0.9918	0.9921

5. Conclusion

In this paper, an asymmetric multiple-image encryption system based on CS and PT-CyD is proposed. Numerical results demonstrate that the proposed method is feasible and effective for multiple-image encryption. The features of proposed method are as follows. Firstly, it can resist the ciphertext-only attack even the plaintext attack, and is free of phase-retrieval attack and information leakage due to the cylindrical asymmetric diffraction. Secondly, the proposed method can

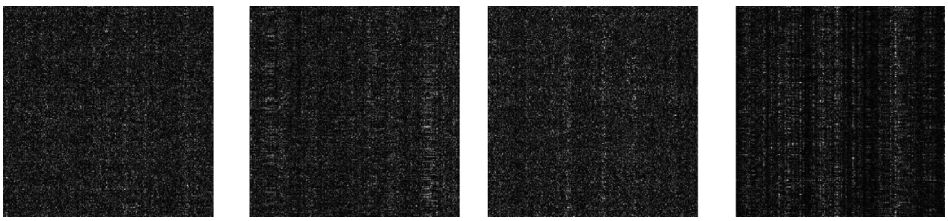

Fig. 9. Image reconstructed from (a) (P_1; P_2), (b) (E; P_1; P_2), (c) (P_1; P_2; P_3), (d) key obtained by imaginary part truncation in the Fourier domain.

Fig. 10. The decrypted images for the encryption process of eight images.

compress the data volume of ciphertext by 1/4 by using CS. The problem of large amount of data in the multiple-image encryption system has partly been solved. Thirdly, the proposed encryption system can encrypt up to eight images which is a large encryption capacity. Lastly, the ciphertext of the proposed scheme is an amplitude-only image, which makes it more convenient for recording and transmitting. Therefore, the proposed encryption scheme has a certain reference value for secure and effective encryption of multiple-images.

Acknowledgments

This research was supported by Sichuan Science and Technology Program, China under Grant 2018GZ0533, and in part by the National Science Foundation of China under Grant 61320106015.

References

[1] S. Liu, Q. Mi, B. Zhu, Optical image encryption with multistage and multichannel fractional Fourier-domain filtering, Opt. Lett. 26 (2001) 1242–1244.
[2] Z. Liu, S. Liu, Random fractional Fourier transform, Opt. Lett. 32 (2007) 2088–2090.
[3] W. Chen, X. Chen, C.J. Sheppard, Optical image encryption based on diffractive imaging, Opt. Lett. 35 (2010) 3817–3819.
[4] B. Javidi, P. Refregier, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[5] X. Peng, H. Wei, P. Zhang, Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain, Opt. Lett. 31 (2006) 3261–3263.
[6] Y. Frauel, A. Castro, T.J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express 15 (2007) 10253–10265.
[7] D. Kong, X. Shen, L. Cao, G. Jin, Phase retrieval for attacking fractional Fourier transform encryption, Appl. Opt. 56 (2017) 3449–3456.
[8] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett. 29 (2004) 1584–1586.
[9] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (2000) 887–889.
[10] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.
[11] N. Singh, A. Sinha, Gyrator transform-based optical image encryption, using chaos, Opt. Lasers Eng. 47 (2009) 539–546.
[12] X.C. Cheng, L.Z. Cai, Y.R. Wang, X.F. Meng, H. Zhang, X.F. Xu, X.X. Shen, G.Y. Dong, Security enhancement of double-random phase encryption by amplitude modulation, Opt. Lett. 33 (2008) 1575–1577.
[13] A.M. Elshamy, A.N.Z. Rashed, A.E.-N.A. Mohamed, O.S. Faragalla, Y. Mu, S.A. Alshebeili, F.E.A. El-Samie, Optical image encryption based on chaotic baker map and double random phase encoding, J. Lightwave Technol. 31 (2013) 2533–2539.
[14] W. Qin, X. Peng, Asymmetric cryptosystem based on phase-truncated Fourier transforms, Opt. Lett. 35 (2010) 118–120.
[15] X. Wang, D. Zhao, Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask, Opt. Lett. 38 (2013) 3684–3686.
[16] X. Wang, W. Chen, X. Chen, Optical information authentication using compressed double random phase encoded images and quick-response codes, Opt. Express 23 (2015) 6239–6253.
[17] X. Deng, D. Zhao, Single-channel color image encryption based on asymmetric cryptosystem, Opt. Laser Technol. 44 (2012) 136–140.
[18] J. Wang, X. Li, Y. Hu, Q.H. Wang, Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding, Opt. Commun. 410 (2018) 468–474.
[19] J. Wang, Q.H. Wang, Y. Hu, Image encryption using compressive sensing and detour cylindrical diffraction, IEEE Photonics J. 10 (2018) 7801014.
[20] P. Deng, M. Diao, M. Shan, Z. Zhong, Y. Zhang, Multiple-image encryption using spectral cropping and spatial multiplexing, Opt. Commun. 359 (2016) 234–239.
[21] W.N. Li, A.H. Phan, M.L. Piao, N. Kim, Multiple-image encryption based on triple interferences for flexibly decrypting high-quality images, Appl. Opt. 54 (2015) 3273–3279.
[22] S. Yuan, X. Liu, X. Zhou, Z. Li, Multiple-image encryption scheme with a single-pixel detector, J. Modern Opt. 63 (2017) 1457–1465.

[23] N.R. Zhou, H. Jiang, L.H. Gong, X.W. Xie, Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging, Opt. Lasers Eng. 110 (2018) 72–79.
[24] D.Z. Kong, L.C. Cao, X.J. Shen, H.J. Zhang, G.F. Jin, Image encryption based on interleaved computer-generated holograms, IEEE Trans. Ind. Inf. 14 (2018) 6.
[25] H. Zhao, J. Liu, J. Jia, N. Zhu, J. Xie, Y. Wang, Multiple-image encryption based on position multiplexing of Fresnel phase, Opt. Commun. 286 (2013) 85–90.
[26] Z. Tang, J. Song, X. Zhang, R. Sun, Multiple-image encryption with bit-plane decomposition and chaotic maps, Opt. Lasers Eng. 80 (2016) 1–11.
[27] J. Wu, Z. Xie, Z. Liu, W. Liu, Y. Zhang, S. Liu, Multiple-image encryption based on computational ghost imaging, Opt. Commun. 359 (2016) 38–43.
[28] D.L. Donoho, Compressed sensing, IEEE Trans. Inform. Theory 52 (2006) 1289–1306.
[29] E.J. Candes, J. Romberg, T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, IEEE Trans. Inform. Theory 52 (2006) 489–509.
[30] E.J. Candes, The restricted isometry property and its implications for compressed sensing, C. R. Math. Acad. Sci. 346 (2008) 589–592.
[31] S. Chen, D.L. Donoho, M.A. Saunders, Atomic decomposition by basis pursuit, SIAM J. Sci. Comput. 58 (2001) 33–61.
[32] E. Liu, V.N. Temlyakov, The orthogonal super greedy algorithm and application in compressed sensing, IEEE Trans. Inform. Theory 58 (2012) 2040–2047.
[33] H. Mohimani, M. Babaie-Zadeh, C. Jutten, A fast approach for overcomplete sparse decomposition based on smoothed l0 norm, IEEE Trans. Signal Process. 57 (2009) 289–301.