Optical Engineering

SPIEDigitalLibrary.org/oe

Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain

Liansheng Sui
Haiwei Lu
Xiaojuan Ning
Yinghui Wang

SPIE

Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain

Liansheng Sui,[a,b,*] Haiwei Lu,[a] Xiaojuan Ning,[a] and Yinghui Wang[a]
[a]Xi'an University of Technology, School of Computer Science and Engineering, Xi'an 710048, China
[b]Shaanxi Key Laboratory for Network Computing and Security Technology, Xi'an 710048, China

Abstract. A double-image encryption scheme is proposed based on an asymmetric technique, in which the encryption and decryption processes are different and the encryption keys are not identical to the decryption ones. First, a phase-only function (POF) of each plain image is retrieved by using an iterative process and then encoded into an interim matrix. Two interim matrices are directly modulated into a complex image by using the convolution operation in the fractional Fourier transform (FrFT) domain. Second, the complex image is encrypted into the gray scale ciphertext with stationary white-noise distribution by using the FrFT. In the encryption process, three random phase functions are used as encryption keys to retrieve the POFs of plain images. Simultaneously, two decryption keys are generated in the encryption process, which make the optical implementation of the decryption process convenient and efficient. The proposed encryption scheme has high robustness to various attacks, such as brute-force attack, known plaintext attack, cipher-only attack, and specific attack. Numerical simulations demonstrate the validity and security of the proposed method. [DOI: 10.1117/1.OE.53.2.026108]

Keywords: double-images encryption; phase-only function; asymmetric cryptosystem.

Paper 131753 received Nov. 18, 2013; revised manuscript received Jan. 20, 2014; accepted for publication Jan. 30, 2014; published online Mar. 4, 2014.

1 Introduction

With the rapid popularity of computer networks, images as an effective carrier of information have been widely used in various fields of modern society and image encryption issues have become an important field for information security. Since Refregier and Javidi[1] proposed the classical optical double-random phase encoding (DRPE) technique, many optical encryption and authentication systems in Fourier transform (FT), Fresnel transform (FrT), fractional Fourier transform (FrFT), and gyrator transform (GT) domains have been proposed during the past decades.[2–11] Moreover, Alfalou and Brosseau[12] pointed out that these techniques can be used for compression operations simultaneously. Though most reported optical encryption techniques based on DRPE have the excellent parallel and multidimensional capability of signal processing, it should be pointed out that these schemes belong to the category of symmetric cryptosystems, where the keys in the encryption process are used for decryption. Some research investigations indicate that these schemes are vulnerable to the conventional attacks because of the inherently linear property of mathematical or optical transformation.[13–15] In order to resist these attacks, Qin and Peng[16] proposed an asymmetric encryption based on the phase-truncated Fourier transform (PTFT), where the decryption keys are different from the encryption keys and the linearity of the cryptosystem is broken by using the nonlinear operation of phase truncation.

*Address all correspondence to: Liansheng Sui, E-mail: liudua2010@gmail.com

Recently, multiple-image encryption based on multiplexing techniques has received increasing attention in the field of information security since Situ and Zhang[17] proposed the multiple-image encryption approaches using wavelength and position multiplexing with Gaussian low-pass filtering. Alfalou and Mansour[18] proposed an encryption scheme which is divided into two security layers, and target images are multiplexed and simultaneous encoded by using the iterative Fourier transformations in the first layer. In subsequent work, Alfalou et al.[19] implemented simultaneous fusion, compression, and encryption of multiple images based on the discrete cosine transform. Wang and Zhao[20] proposed a fully phase image encryption based on superposition principle and hologram, where a real-valued original image is encoded into a phase-only function (POF). Deng and Zhao[21] suggested a multiple-image encryption by using a phase retrieval algorithm and intermodulation in the Fourier domain, which avoids the cross-talk of decrypted images. Hwang et al.[22] proposed a multiple-image encryption and multiplexing approach based on a modified Gerchberg–Saxton algorithm (MGSA) in the FrT domain, which reduces the cross-talks significantly. Chang et al.[23,24] also suggested the position multiplexing encryption using cascaded phase-only masks based on the MGSA.

As a special case, double-image encryption also has attracted much attention in optical cryptosystem. Li and Wang[25] proposed a double-image encryption algorithm based on phase-retrieval technique and GT, where two images can be simultaneously encrypted into a single one as the amplitudes of gyrator. Liu et al.[26] encrypted two original images into the real part and imaginary part of a complex

function, respectively, which are exchanged randomly by using a random binary encoding data generated by chaotic map. Wang and Zhao[27] suggested an asymmetric algorithm to encrypt two covert images into an overt image based on phase retrieval and PTFT, in which the encryption keys are different from those in decryption process. However, Wang and Zhao[28] designed a specific attack by using a two-step iterative amplitude-retrieval approach according to PTFT-based cryptosystems. With this attack, the encrypted information would be revealed when the encryption keys are used as public keys. Subsequently, Wang and Zhao[29] suggested another asymmetric double-image encryption, which has a high level of robustness against this attack. Li and Wang[30] proposed a double-image encryption based on discrete fractional random transform and chaotic maps, which can raise the efficiency when encrypting, storing, or transmitting. Zhang and Xiao[31] designed a double-optical images encryption using discrete Chirikov standard map and chaos-based discrete fractional random transform, where Chirikov standard map is utilized to scramble the pixel positions and intensity values, respectively.

In this article, a double-image encryption scheme is proposed based on an asymmetric technique, in which the encryption and decryption processes are different and the encryption keys are not identical to the decryption ones. The encryption process can be performed digitally, in which the POFs of two plain images are obtained by using the iterative phase retrieval algorithm, and the interim-encrypted matrices generated with POFs are modulated into a complex image with the convolution operation in FrFT domain. Finally, the complex image is transformed to the real-value ciphertext with stationary white-noise distribution. The decryption process can be implemented optically and only two decryption keys produced in the encryption process are used as phase masks, which is convenient and efficient by using the classical DRPE system. Simulation results and security analysis verify that the proposed double-image encryption has a high level of robustness against brute-force attack, known plaintext attack and specific attack.

The rest of this article is organized as follows. In Sec. 2, the basic principles and the processed of encryption and decryption are introduced in detail. In Sec. 3, numerical simulation results and security analysis are given. Finally, the conclusion is given in Sec. 4.

2 Encryption and Decryption Process

2.1 *Phase-Retrieval Algorithm Based on Iterative FrFT*

The Gerchberg–Saxton algorithm (GSA) is a powerful tool which is used in image encryption cryptosystems, which is usually employed to encode plaintext into a POF in the Fourier domain. Though it is sufficient to retrieve the phase function with the FTs back and forth between the object and the Fourier domains, it suffers from some drawbacks such as slow convergence speed in practical applications. In order to solve this problem, a POF-retrieval algorithm shown in Fig. 1 is implemented in Ref. 32.

The FrFT at order α of a two-dimensional function $f(x_i, y_i)$ can be expressed as

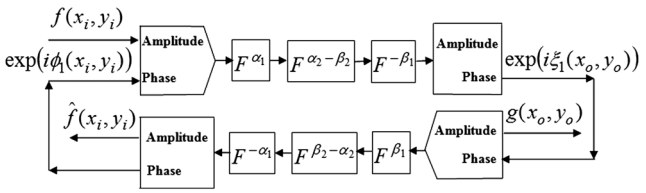


Fig. 1 Diagram of the iterative phase-retrieval process in the fractional Fourier transform domain.

$$f(x_o, y_o) = F^{\alpha}[f_i(x_i, y_i)](x_o, y_o) = \iint_{-\infty}^{+\infty} K(x_i, y_i; x_o, y_o) f(x_i, y_i) \mathrm{d}x_i \mathrm{d}y_i, \tag{1}$$

where (x_i, y_i) and (x_o, y_o) indicate the input and output coordinates, respectively, and the transform kernel is denoted as

$$K(x_i, y_i; x_o, y_o) = A_\phi \exp\{i\pi[(x_i^2 + y_i^2 + x_o^2 + y_o^2)\cot\phi_\alpha - 2(x_i x_o + y_i y_o)\csc\phi_\alpha]\}, \tag{2}$$

$$A_\phi = \frac{\exp[-i\pi\,\mathrm{sgn}(\sin\phi_\alpha)/2 + i\phi_\alpha]}{|\sin\phi_\alpha|}. \tag{3}$$

The A_ϕ is a trivial phase parameter and $\phi_\alpha = \alpha\pi/2$ is the transform angle. The FrFT is linear and has the property that it is index additive

$$F^{\alpha}\{F^{\beta}[f(x, y)]\} = F^{\alpha+\beta}[f(x, y)]. \tag{4}$$

In addition, the FrFT satisfies the Parseval energy conservation theorem

$$\iint_{-\infty}^{+\infty} |F^{\alpha}[f(x_i, y_i)]|^2 \mathrm{d}x_0 \mathrm{d}y_0 = \iint_{-\infty}^{+\infty} |f(x_i, y_i)|^2 \mathrm{d}x_i \mathrm{d}y_i. \tag{5}$$

The POF-retrieval algorithm is based on the iterative FrFT process between two grayscale images proposed firstly in Ref. 33. Images f and g are placed at the input and output planes, respectively, between which are three phase masks placed in three continuous FrFT planes. Let the function h denotes an interim-encrypted image and α_1, α_2, β_1, β_2 denote two different groups of fractional orders. Giving five-phase functions, which are distributed in the interval $[0, 2\pi]$ and denoted by ϕ_1, ϕ_2, ξ_1, ξ_2 and ψ, respectively, the relationship between the images and phase functions is expressed as

$$h\exp(j\psi) = F^{\alpha_2}\{F^{\alpha_1}[f\exp(j\phi_1)]\exp(j\phi_2)\} = F^{\beta_2}\{F^{\beta_1}[g\exp(j\xi_1)]\exp(j\xi_2)\}, \tag{6}$$

where F^{α} denotes FrFT with the fractional order α. Initially, the functions h, ϕ_1, ϕ_2, ξ_1, ξ_2 and ψ are unknown. Equation (6) indicates that the two images satisfy the following relationship:

$$F^{-\beta_1}(F^{\alpha_2-\beta_2}\{F^{\alpha_1}[f\exp(j\phi_1)]\exp(j\phi_2)\}\exp(-j\xi_2)) = g\exp(j\xi_1). \quad (7)$$

According to Eq. (7), the phase functions ϕ_1, ϕ_2, ξ_1 and ξ_2 are obtained with the iterative process, which consists of a number of cycling iterations. Suppose that in the k'th iteration the phase distributions ϕ_1^k, ϕ_2^k, ξ_2^k are known, then the output-complex image $\hat{g}^k$ is expressed as

$$\hat{g}^k = F^{-\beta_1}(F^{\alpha_2-\beta_2}\{F^{\alpha_1}[f\exp(j\phi_1^k)]\exp(j\phi_2^k)\}\exp(-j\xi_2^k)). \quad (8)$$

Its phase and amplitude are expressed as follows

$$\xi_1^k = \arg\{\hat{g}^k\}, \qquad g^k = |\hat{g}^k|. \quad (9)$$

Substituting the phase function ξ_1^k into Eq. (6), the phase functions ξ_2^{k+1}, ϕ_2^{k+1}, ϕ_1^{k+1} in next iteration are updated by

$$\xi_2^{k+1} = \arg\left(\frac{F^{\alpha_2-\beta_2}\{F^{\alpha_1}[f\exp(j\phi_1^k)]\exp(j\phi_2^k)\}}{F^{\beta_1}[g\exp(j\xi_1^k)]}\right), \quad (10)$$

$$\phi_2^{k+1} = \arg\left(\frac{F^{\beta_2-\alpha_2}\{F^{\beta_1}[g\exp(j\xi_1^k)]\exp(j\xi_2^{k+1})\}}{F^{\alpha_1}[f\exp(j\phi_1^k)]}\right), \quad (11)$$

$$\phi_1^{k+1} = \arg[F^{-\alpha_1}(F^{\beta_2-\alpha_2}\{F^{\beta_1}[g\exp(j\xi_1^k)] \times \exp(j\xi_2^{k+1})\}\exp(-j\phi_2^{k+1}))]. \quad (12)$$

In order to decide whether the iteration stops, the correlation coefficient (CC) or the mean square error (MSE) between the iterated image and the original one is used as convergent criterion. These criterions are expressed as

$$\mathrm{CC} = \frac{E\{[g-E(g)][g^k-E(g^k)]\}}{\sqrt{E\{[g-E(g)]^2\}}\sqrt{E\{[g^k-E(g^k)]^2\}}}, \quad (13)$$

$$\mathrm{MSE} = \frac{\sum_0^{M-1}\sum_0^{N-1}[g-g^k]^2}{M\times N}, \quad (14)$$

where g and g^k denote the original image and the iterated one, and $E[\cdot]$ denotes the expected value operator. In the process of iteration, if CC is larger than a predefined threshold which is close to 1 or MSE is lower than a predefined threshold which is close to 0, the iterative process ends. Suppose the number of iteration is K, then the optimized phase functions are obtained as follows:

$$\phi_1 = \phi_1^K, \quad \phi_2 = \phi_2^K, \quad \xi_1 = \xi_1^{K-1}, \quad \xi_2 = \xi_2^K. \quad (15)$$

In Fig. 1, $f(x_i, y_i)$ and $g(x_o, y_o)$ denote the input and output image, respectively. In order to compute the POF of the image $f(x_i, y_i)$, $g(x_o, y_o)$ is constrained to unity amplitude $[g(x_o, y_o) = 1]$. When the convergent criterion between $f(x_i, y_i)$ and its approximation $\hat{f}(x_i, y_i)$ is reached, the resultant pure phase functions $\phi_1(x_i, y_i)$ and $\xi_1(x_o, y_o)$ are obtained, respectively, where the function $\xi_1(x_o, y_o)$ is finally used as the POF of image $f(x_i, y_i)$. At the beginning of the iterative process, the initial phase masks ϕ_1^0, ϕ_2^0, ξ_2^0 are generated randomly.

2.2 *Encryption and Decryption Processes*

The proposed double-image encryption is based on the iterative phase-retrieval algorithm, which belongs to the category of asymmetric cryptosystem. The encryption process is shown in Fig. 2. Let $f_i (i = 1, 2)$ denote two original plaintext images to be encoded, the encryption process is described as follows:

- Given a three initial random phase function ϕ_1^0, ϕ_2^0, ξ_2^0, the iterative phase-retrieval process is performed on the image f_i in the POF-retrieval module. First, the relationship between f_i and the unity amplitude image g is built by using Eq. (6), and then the iterative phase-retrieval process is performed by using Eqs. (10)–(12). The convergent criterion is set to a MSE threshold. When the MSE between f_i and its approximation $\hat{f}_i$ is lower than the threshold, the iteration process ends and the optimized phase functions $\phi_{i,1}$, $\phi_{i,2}$, $\xi_{i,1}$, and $\xi_{i,2}$ are obtained by using Eq. (15). In this process, the fractional orders α_1, α_2 are used for the plaintext image f_i and β_1, β_2 for the unity amplitude image g. In addition, the phase function $\phi_{i,2}$ will be used as the decryption key.
- In the interim image generation module, a complex matrix is produced by using the unity amplitude image g and two corresponding phase functions $\xi_{i,1}$, $\xi_{i,2}$, which is expressed as

$$H_i = h_i\exp(j\psi_i) = F^{\beta_2}\{F^{\beta_1}[g\exp(j\xi_{i,1})]\exp(j\xi_{i,2})\}. \quad (16)$$

- In the phase modulation, two matrices H_i are combined into one complex matrix H by using convolution and the combined matrix H can be written as

$$H = [h_1\exp(j\psi_1)] * [h_2\exp(j\psi_2)], \quad (17)$$

where the symbol * denotes the convolution operation.
- The combined matrix H is transformed to $\hat{H}$ by using the FrFT with the fractional order α_3, which is expressed as

$$\hat{H} = F^{\alpha_3}(H) = F^{\alpha_3}\{[h_1\exp(j\psi_1)] * [h_2\exp(j\psi_2)]\}. \quad (18)$$

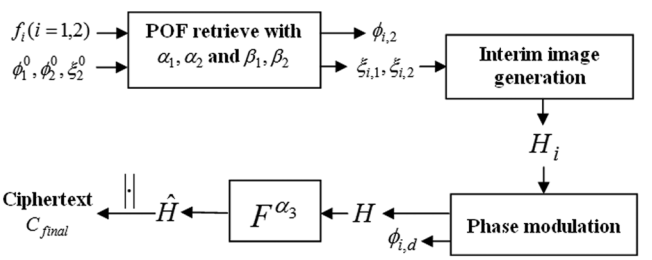


Fig. 2 Diagram of double-image encryption process.

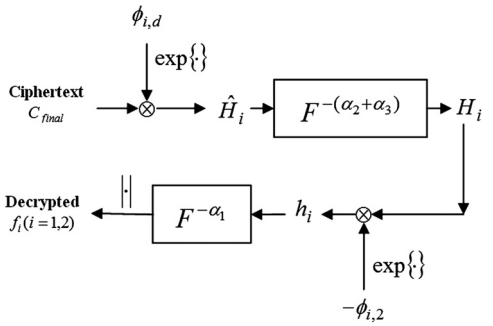


Fig. 3 Diagram of double-image decryption process.

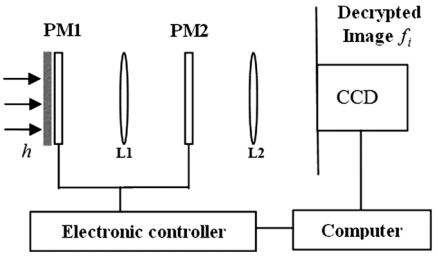


Fig. 4 Optical implementation of decryption process.

In the same time, the amplitude of $\hat{H}$ is extracted as the real-value ciphertext C_{final} by using following equation

$$C_{\text{final}} = |\hat{H}| = |F^{\alpha_3}\{[h_1 \exp(j\psi_1)] * [h_2 \exp(j\psi_2)]\}|. \quad (19)$$

Additionally, a decryption key $\phi_{i,d}$ is generated as following:

$$\phi_{i,d} = \arg\left[\exp(j \arg\{F^{\alpha_3}[h_i \exp(j\psi_i)]\}) \frac{|F^{\alpha_3}[h_i \exp(j\psi_i)]|}{|H|}\right], \quad (20)$$

where $|H|$ denotes the amplitude of the combined matrix.

The decryption process is depicted in Fig. 3, which is different from the encryption process and much simple. It should be paid attention to the following main steps

- When decrypting the plaintext image f_i, the complex matrix $\hat{H}_i$ is first generated by multiplying the ciphertext C_{final} with the phase function $\exp(j\phi_{i,d})$ produced with the corresponding decryption key $\phi_{i,d}$.
- The complex matrix $\hat{H}_i$ is transformed to H_i by using the inverse FrFT with the fractional order $-(\alpha_2+\alpha_3)$, and then h_i is generated by multiplying H_i with the phase matrix $\exp(-j\phi_{i,2})$ produced with another corresponding decryption key $\phi_{i,2}$.
- The complex matrix h_i is transformed to $\hat{h}_i$ by using the inverse FrFT with the fractional order $-\alpha_1$, and then the amplitude of the matrix $\hat{h}_i$ is extracted as the decrypted image f_i, which is expressed as

$$f_i = |F^{-\alpha_1}\{F^{-(\alpha_2+\alpha_3)}[C_{\text{final}} \exp(j\phi_{i,d})]\} \exp(-j\phi_{i,2})|. \quad (21)$$

From above description of the encryption and decryption processes, one can see that only three random phase functions denoted by ϕ_1^0, ϕ_2^0, and ξ_2^0 is used as the encryption keys, which have no relationship with decryption. Simultaneously, the phase functions $\phi_{i,2}$ and $\phi_{i,d}$ produced in the encryption process are used as the decryption keys according to each decrypted image f_i, which are directly related to the original plaintext images. Apparently, the keys for decryption are different from those for encryption, which means the entire cryptosystem is asymmetric. As we all know, some cryptosystems are vulnerable to the conventional attacks such as known plaintext attack and chosen plaintext attack because of the linearity and symmetry existed in these encryption schemes.[13–15] The proposed asymmetric double-image encryption scheme can break the linearity of the cryptosystem and has high resistance against to these conventional attacks. In addition, the decryption keys $\phi_{i,2}$ and $\phi_{i,d}$ can be assigned to different valid users in order to enhance the security, in which each original plaintext image f_i can be decrypted if all two phase masks $\exp(j\phi_{i,d})$ and $\exp(-j\phi_{i,2})$ are correctly placed in the verification system.

The proposed asymmetric double-image encryption scheme can be implemented with an electro-optical hybrid setup. It is worth noting that although the encryption process and the formation of decryption keys are complicated and can be realized digitally with the help of computer, the decryption process is much simple and can be implemented with some optoelectronic devices. A simple optical setup is depicted in Fig. 4, which is based on the $4f$ imaging system similar to DRPE. When decrypting the image f_i, the phase masks PM1 and PM2 are only placed with the phase masks $\exp(j\phi_{i,d})$ and $\exp(-j\phi_{i,2})$, respectively. Obviously, the decryption process is convenient and efficient.

3 Numerical Simulation and Security Analysis

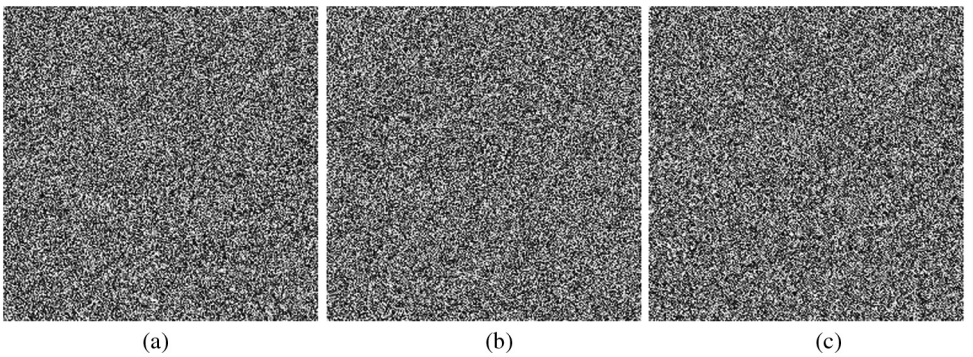
Numerical simulations have been performed to verify the feasibility and effectiveness of the proposed asymmetric double-image encryption scheme. Two grayscale images "Zelda" and "Baboon" with 256×256 pixels and 256 Gy levels, which are shown in Figs. 5(a) and 5(b), are used for encryption. The related fractional orders are set as $\alpha_1 = 0.2$, $\alpha_2 = \alpha_1 + 0.4$, $\beta_1 = \alpha_1 + 0.3$, $\beta_2 = \alpha_2 + 0.1$, and $\alpha_3 = \alpha_1 + 0.1$. The ciphertext image encrypted by using three random phase functions as encryption keys is shown in Fig. 5(c), which looks like white noise. The decryption keys generated in the encryption process and used for the correct decrypted image "Zelda" are shown in Figs. 6(a) and 6(b), whereas the keys for image "Peppers" are shown in Figs. 6(c) and 6(d). The corresponding decrypted images with the correct decryption keys are shown in Figs. 6(e) and 6(f).

3.1 *Brute-Force Attack Analysis*

The robustness against the brute-force attack is tested, in which an invalid user attempts to retrieve the original images with two possible ways, namely decode plaintext with (1) no keys, (2) two arbitrarily selected phase functions from the encryption keys. Figures 7(a) and 7(b) display the decrypted results by using no keys and arbitrarily selected phase functions, from which an invalid user cannot obtain any useful information. So, the proposed asymmetric has powerful ability to resist the brute-force attack.

(a) (b) (c)

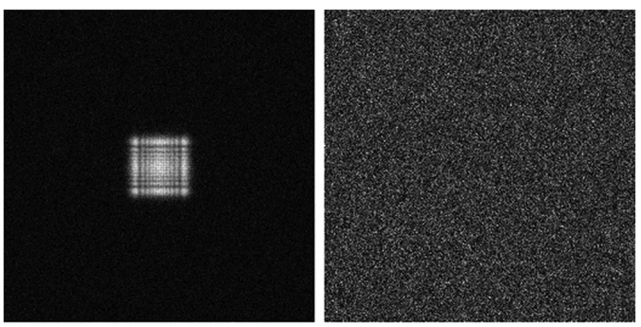
Fig. 5 (a) Image "Zelda," (b) image "Peppers," and (c) ciphertext.



(a) (b) (c)

(d) (e) (f)

Fig. 6 (a) Decryption key $\phi_{i,2}$ for image "Zelda," (b) decryption key $\phi_{i,d}$ for image "Zelda," (c) decryption key $\phi_{i,2}$ for image "Peppers," (d) decryption key $\phi_{i,d}$ for image "Peppers," (e) decrypted image "Zelda," and (f) decrypted image "Peppers."



(a) (b)

Fig. 7 Decrypted results using (a) no keys and (b) two arbitrarily selected phase functions.

3.2 *Potential Attack Analysis*

Usually, there are four conventional potential attacks, such as cipher-only attack, known plaintext attack, chosen plaintext attack, and chosen ciphertext attack, in which chosen plaintext attack is the most powerful attack. If a cryptosystem can resist chosen plaintext attack, it can resist other attacks. According to the proposed asymmetric double-image encryption, an illegal user can use the same encryption keys ϕ_1^0, ϕ_2^0, and ξ_2^0 to encrypt two fake plaintext images and obtain the phase functions $\phi_{i,2}$, $\phi_{i,d}$ to decrypt the original ciphertext in order to retrieve the corresponding plaintext f_i. Supposing images "Lena" and "Baboon" shown in Figs. 8(a) and 8(b) are chosen as fake plaintext images, the phase functions $\phi_{i,2}$ and $\phi_{i,d}$ are obtained in the encryption process and used to decrypt the original ciphertext of "Zelda"

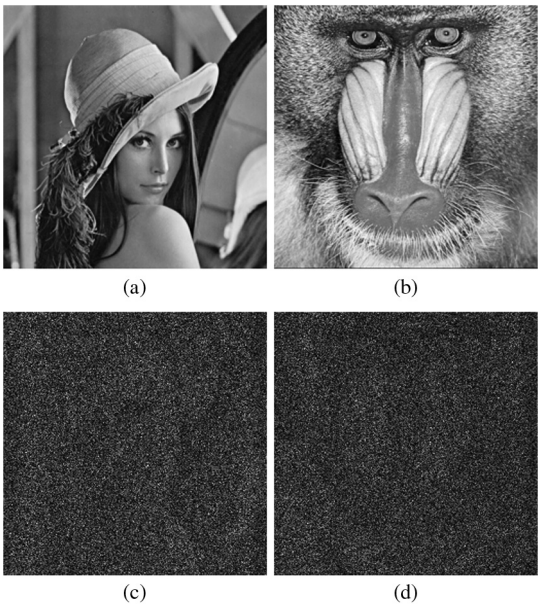


Fig. 8 Two fake plaintext images (a) "Lena," (b) "Baboon," (c) decrypted "Zelda," and (d) decrypted "Peppers."

and "Peppers". Figures 8(c) and 8(d) display the decrypted images of "Zelda" and "Peppers," respectively. As it is seen from Figs. 8(c) and 8(d), the retrieved images provide no valuable information on the content of "Zelda" and "Peppers" though the fake plaintexts themselves can be seen faintly.

Similar to the ciphertext-only attack proposed in Ref. 26, the phase-retrieval algorithm shown in Fig. 9 is introduced into the decryption process as a test. Supposing the invalid user has known the phase function $\phi_{i,d}$, he can recover the function $\phi_{i,2}$ by use of FrFT. Thus, the original images f_i can be decrypted by using Eq. (21). Initially, the phase function $\phi_{i,2}^0$ is generated randomly. The process is simulated with 300 iterations. The decryption results are displayed in Fig. 10. Figure 10(a) shows that the values of the MSE curves are large, which means the phase function $\phi_{i,2}$ cannot be retrieved. Figures 10(b) and 10(c) show the decrypted image "Zelda" and "Peppers," respectively, which are noise-like images. The results have demonstrated that the proposed encryption scheme has high security under the ciphertext-only attack.

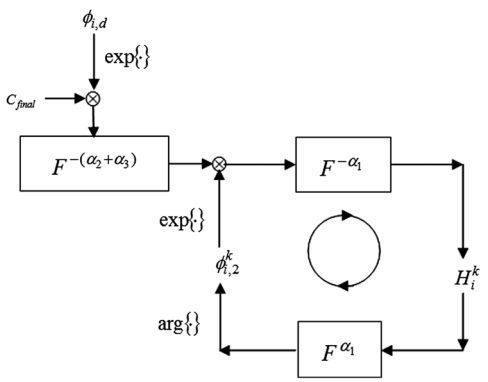


Fig. 9 The diagram of ciphertext-only attack by using the phase-retrieval algorithm.

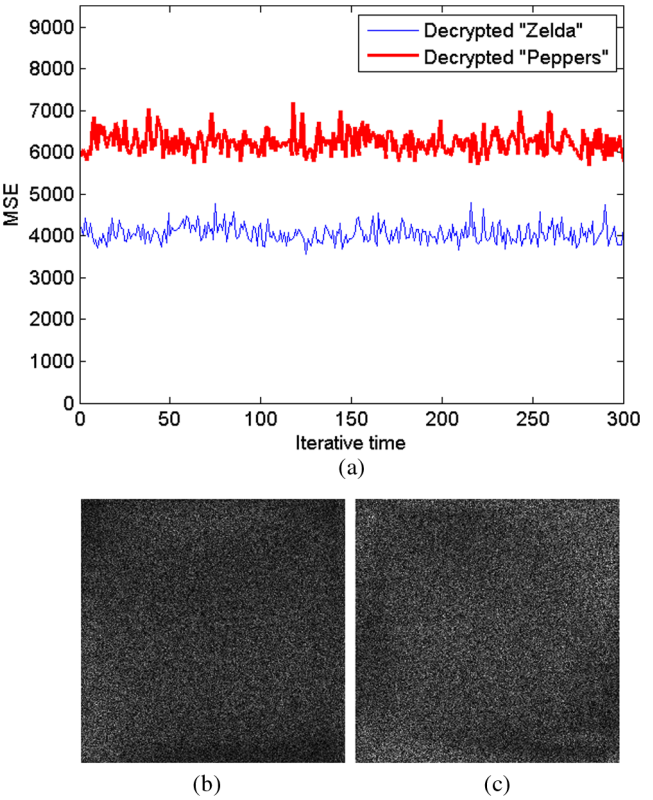


Fig. 10 The results of ciphertext-only attack: (a) mean square error (MSE) curves, (b) decrypted image "Zelda," and (c) decrypted image "Peppers."

3.3 *Occlusion Attack Analysis*

The robustness against occlusion attack is analyzed. When considering the robustness against occlusion, the decryption process should be performed on the ciphertext of "Zelda" and "Peppers" with all correct decryption keys, in which the ciphertext image is occluded partly. Figure 11(a) shows the occluded ciphertext whose pixel values at the left-top corner are replaced with 0 in simulation, namely the ciphertext is cropped by 50% in the left side. Figures 11(b) and 11(c) display the corresponding recovered images from Fig. 11(a). Figure 12(a) shows the occluded ciphertext whose left-side pixel values are replaced with 0, and Figs. 12(b) and 12(c) display the recovered. Apparently, the main information of the original images can be recognized visually from the decrypted ones. Similar results can be obtained when the ciphertext is cropped by 50% or 100% in the right side. So, the proposed asymmetric double-image encryption has high robustness against occlusion attack.

3.4 *Noise Attack Analysis*

When considering the robustness against noise, a Gaussian random noise is added to the ciphertext of "Zelda" and "Peppers," in which the noise interferes with the ciphertext image in the following way:

$$C' = C(1 + kG), \tag{22}$$

where C and C' are the original ciphertext and the noise-affected ciphertext image, respectively, k is a coefficient

(a) (b) (c)

Fig. 11 (a) Ciphertext with 50% occlusion in the left side, (b) decrypted image "Zelda," and (c) decrypted image "Peppers."

(a) (b) (c)

Fig. 12 (a) Ciphertext with 100% occlusion in the left side, (b) decrypted image "Zelda," and (c) decrypted image "Peppers."

which denotes the noise strength, and G is a Gaussian random noise with zero-mean and identity standard deviation. Figure 13 shows the decrypted images of "Zelda" when k is set to 0.2, 0.4, 0.6, 0.8, and 1.0. Similar results can be obtained for image "Peppers." From Fig. 13, it is obvious that the content of the decrypted images can be recognized despite of noise interference, and the proposed encryption scheme has high robustness against noise attack.

3.5 *Statistical Analysis*

The contribution of fractional orders on the security of the proposed double-image encryption is researched. Figure 14 shows the relationship between MSE and the deviation of the fractional order α_1. When α_1 is correct, the MSE value between the original image "Zelda" with its decrypted one approximates to zero. When α_1 slightly departs from the correct value, the MSE value sharply increases. Similar result is obtained according to image "Peppers." In practical, if the deviation of the order α_1 is larger than 0.006, the content of decryption images cannot be recognized totally. Figures 15(a) and 15(b) show the decrypted images "Zelda" and "Peppers," respectively, while the deviation of the order α_1 equals 0.006.

In order to test the correlations of adjacent pixels, the 2000 pairs of adjacent pixels are randomly selected in vertical, horizontal, and diagonal directions from the plaintext images "Zelda" and "Peppers" as well as from the ciphertext, and then the CCs of two adjacent pixels is calculated as follows:

$$\mathrm{Cor} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{[\sum_{i=1}^{N}(x_i - \bar{x})^2][\sum_{i=1}^{N}(y_i - \bar{y})^2]}}, \tag{23}$$

where $\bar{x} = 1/N\sum_{i=1}^{N} x_i$ and $\bar{y} = 1/N\sum_{i=1}^{N} y_i$. Table 1 shows the results of CCs of the plaintext images and ciphertext, which indicates that the correlations of two adjacent pixels of the plaintext image is significant while that of ciphertext are very low. So, illegal user also cannot obtain any valid information from this statistical data.

Figure 16 displays the histograms of the ciphertext of two groups of original images, namely "Zelda" and "Peppers" shown in Figs. 5(a) and 5(b), "Lena" and "Baboon" shown in Figs. 8(a) and 8(b). Obviously, it can be concluded that the different original images have consistent statistical properties because the distributions of the histograms are similar. Thus, the histograms of ciphertext cannot provide any useful information for the invalid user to perform this kind of statistical analysis attack.

Similar to the analysis process proposed in Ref. 34, the key spaces of the phase function $\phi_{i,2}$, $\phi_{i,d}$ as the decryption keys are analyzed, respectively. When decrypting the image "Zelda," the phase function $\phi_{1,d}$ is considered to fluctuate in certain range, namely there is a pseudo-key $\phi'_{1,d}$ satisfying the following relation:

$$\exp(j\phi'_{1,d}) = \exp(j\phi_{1,d}) + \exp(jd\Delta\phi), \tag{24}$$

where $\Delta\phi$ is a random phase function whose value is located in the range $(-\pi, \pi)$, and d is a coefficient whose value is

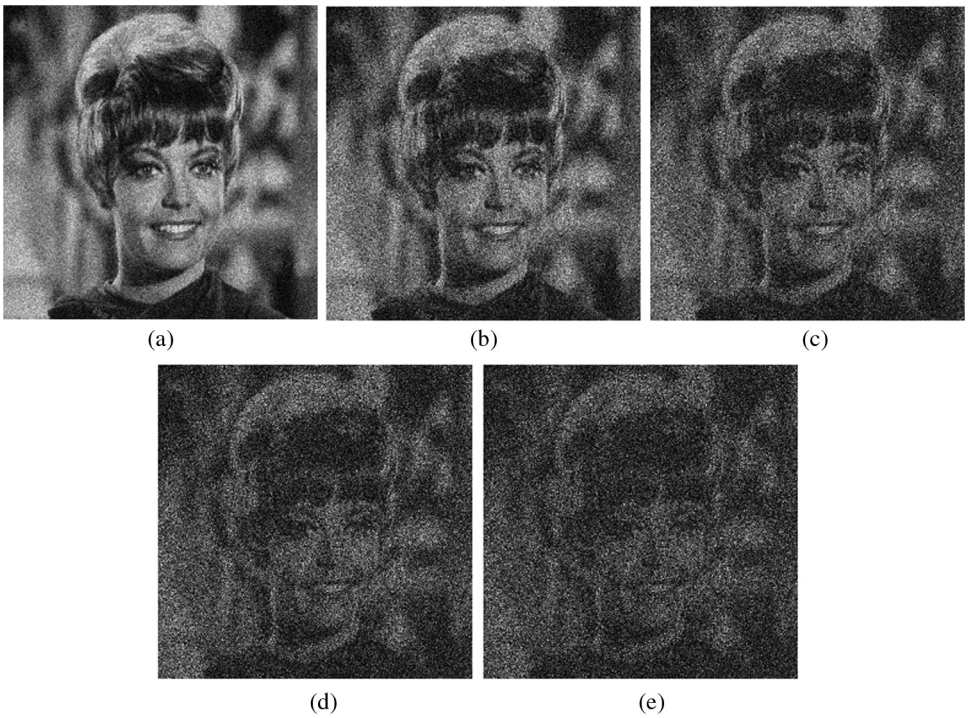


Fig. 13 Decrypted images with coefficient k: (a) $k = 0.2$, (b) $k = 0.4$, (c) $k = 0.6$, (d) $k = 0.8$, and (e) $k = 1.0$.

located in the range $(-1, 1)$. Then, the pseudo-key $\phi'_{1,d}$ is used to decrypt the ciphertext, and the normalized MSE curve versus to coefficient d is shown in Fig. 17(a). When the MSE is more than 50, any valid information cannot be obtained from the decrypted image in vision. From Fig. 10, it is obvious that the maximum value of Δd is 0.0538 while the normalized MSE is equal to 50, and the number of possible value for every pixel in the phase function is huge as $(2\pi/0.0538)^{256\times256}$. So, the key space of $\phi_{1,d}$ is estimated to be $S_1 \approx 116^{256\times256}$. Similarly, the normalized MSE curve of the phase function $\phi_{1,2}$ is shown in Fig. 17(b), and the corresponding key space is estimated $S_2 \approx 6^{256\times256}$. So, the entire key space of the cryptosystem almost equals $S_1 \times S_2$, which is enormous enough to resist brute-force attack.

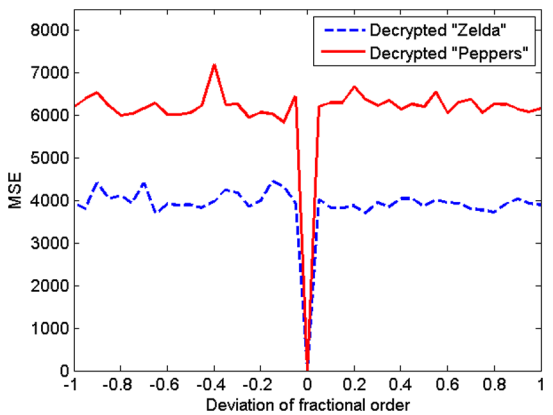


Fig. 14 The MSE versus the perturbation of the fractional order α_1.

3.6 *Specific Attack Analysis*

The proposed asymmetric double-image encryption scheme has inherent immunity to the specific attack proposed in Ref. 28. The encryption process of the asymmetric cryptosystem based on PTFT proposed in Ref. 16 is shown in Fig. 18, in which an image $f(x)$ is encrypted to the ciphertext $E_o(x)$ by using following equations:

$$g(u) = \mathrm{PT}\{\mathrm{FT}[f(x)R(x)]\}, \tag{25}$$

$$E_o(x) = \mathrm{PT}\{\mathrm{IFT}[g(u)R'(u)]\}, \tag{26}$$

where $R(x)$ and $R'(u)$ are two random phase functions as encryption keys. The decryption keys $P(u)$ and $P'(x)$ are generated in the encryption process by following equations:

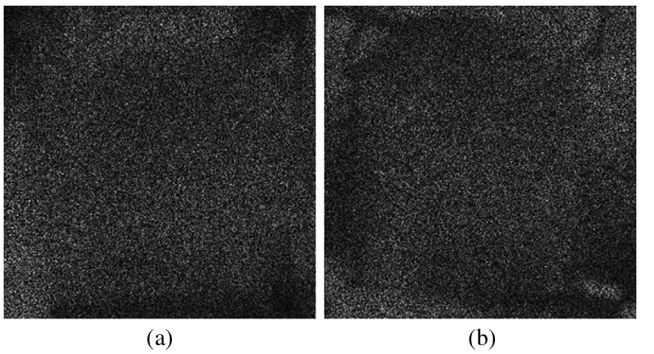


Fig. 15 (a) Decrypted image "Zelda" and (b) decrypted image "Peppers."

Table 1 Correlation results in the plaintext images and ciphertext.

Correlation coefficient	Plaintext image		Encrypted image
	Zelda	Peppers	Ciphertext
Horizontal direction	0.9689	0.9677	0.0228
Vertical direction	0.9842	0.9753	0.0211
Diagonal direction	0.9528	0.9453	0.0400

$$P(u) = \mathrm{PR}\{\mathrm{FT}[f(x)R(x)]\}, \tag{27}$$

$$P'(x) = \mathrm{PR}\{\mathrm{IFT}[g(u)R'(u)]\}, \tag{28}$$

where $\mathrm{PT}(\cdot)$ and $\mathrm{PR}(\cdot)$ denote the phase truncation and phase reservation operator, respectively. According to Fig. 18, the specific attack is divided into two steps.[28] The first step is used to retrieve estimations of $g(u)$ and decryption by $P'(x)$ using $R'(u)$ and $E_o(x)$ with an iteration process, which is expressed as

$$g_k(u) = \mathrm{PT}\{\mathrm{FT}[E_o(x)P'_k(x)]\}, \tag{29}$$

$$E_{k+1}(x) = \mathrm{PT}\{\mathrm{IFT}[g_k(u)R'(u)]\}, \tag{30}$$

$$P'_{k+1}(x) = \mathrm{PR}\{\mathrm{IFT}[g_k(u)R'(u)]\}, \tag{31}$$

where the phase function $P'_0(x)$ is arbitrarily chosen. The second step is to obtain the decrypted image $f(x)$ and decryption $P(u)$ by using the estimation of $g(u)$ and $R(x)$ with another iteration process, which is expressed as

$$f_k(u) = \mathrm{PT}\{\mathrm{IFT}[g_0(u)P_k(u)]\}, \tag{32}$$

$$g_{k+1}(u) = \mathrm{PT}\{\mathrm{FT}[f_k(x)R(x)]\}, \tag{33}$$

$$P_{k+1}(u) = \mathrm{PR}\{\mathrm{FT}[f_k(x)R(x)]\}, \tag{34}$$

where the initial phase function $g_0(u)$ is the estimation of $g(u)$ in first step.

From above description of the specific attack, the encryption keys $R'(u)$ and $R(x)$ is very important, which is used to retrieve the decryption keys $P'(x)$ and $P(u)$ in two steps, respectively. The encryption mechanism of the proposed asymmetric scheme is different from the PTFT-based cryptosystem, where three random encryption keys ϕ_1^0, ϕ_2^0, and ξ_2^0 are only used for the POF retrieve of the plain image f_i. In

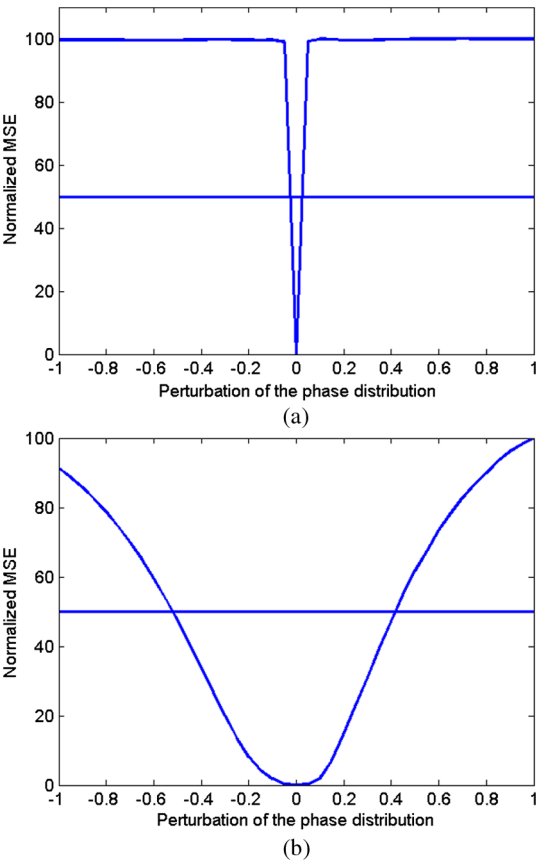


Fig. 17 (a) The normalized MSE versus the perturbation of the phase function $\phi_{1,d}$ and (b) the normalized MSE versus the perturbation of the phase function $\phi_{1,2}$.

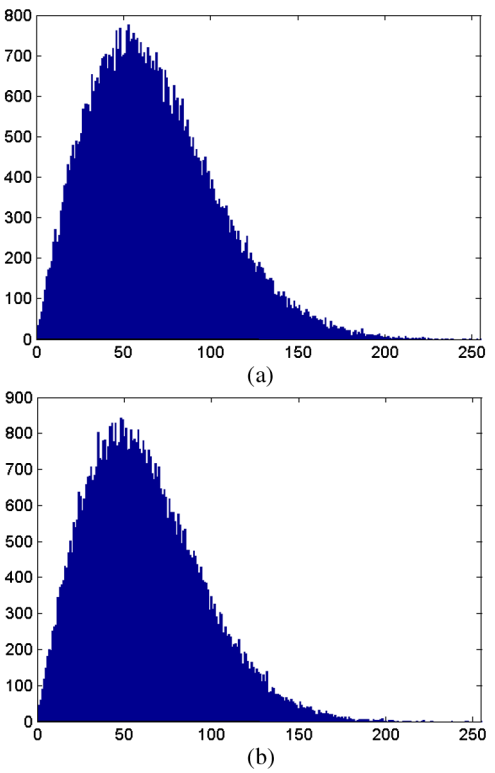


Fig. 16 (a) Histogram of the ciphertext of "Zelda" and "Peppers" (b) histogram of the ciphertext of "Lena" and "Baboon."

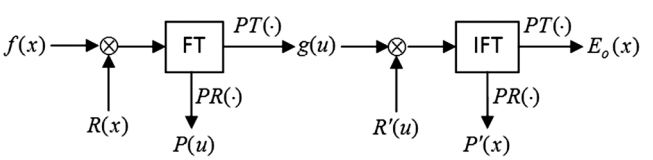


Fig. 18 Diagram of the encryption process proposed in Ref. 28.

addition, the generation of the decryption key $\phi_{i,d}$ has no relation to these encryption keys. So, the encryption keys cannot afford any information to recover the decryption keys and plaintext images.

4 Conclusion

In conclusion, a double-image encryption scheme based on asymmetric technique is proposed, in which the encryption and decryption processes are different and the decryption keys are not identical to the encryption ones. Three random phase functions are employed as encryption keys and used to retrieve the POFs of plain images based on the iterative phase retrieval process. Meanwhile, two interim-encrypted images generated with the corresponding phase functions are combined into a complex matrix, which is transformed to the real-value ciphertext with stationary white noise distribution. Owing to applications of the asymmetric technique, the fundamental drawbacks resulted from the linearity can be avoided and therefore high robustness against existing attacks can be achieved. A set of numerical simulations have illustrated the feasibility and effectiveness of the proposed encryption scheme.

Acknowledgments

This work was supported by Foundation of Shaanxi Education Department of Shaanxi Province under grant 11JK1032, Xi'an Science and Technology Bureau under grant CXY1120-1, the National Natural Science Foundation of China under grant number 61302135 and 61272284.

References

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**(7), 767–769 (1995).
2. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.* **25**(12), 887–889 (2000).
3. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* **28**(4), 269–271 (2003).
4. H. Li and Y. Wang, "Information security system based on iterative multiple-phase retrieval in gyrator domain," *Opt. Laser Technol.* **40**(7), 962–966 (2008).
5. S. Yuan et al., "Information hiding based on double random-phase encoding and public-key cryptography," *Opt. Express* **17**(5), 3270–3284 (2009).
6. M. He et al., "Security enhanced optical encryption system by random phase key and permutation key," *Opt. Express* **17**(25), 22462–22473 (2009).
7. W. Chen and X. Chen, "Space-based optical image encryption," *Opt. Express* **18**(26), 27095–27104 (2010).
8. N. Zhou, Y. Wang, and J. Wu, "Image encryption algorithm based on the multi-order discrete fractional Mellin transform," *Opt. Commun.* **284**(2), 5588–5597 (2011).
9. M. R. Abuturab, "Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding," *Opt. Lasers Eng.* **50**(9), 1209–1216 (2012).
10. M. R. Abuturab, "Securing color image using discrete cosine transforming gyrator transform domain structured-phase encoding," *Opt. Lasers Eng.* **50**(10), 1383–1390 (2012).
11. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain," *Opt. Express* **20**(4), 3853–3865 (2012).
12. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photonics* **1**(3), 589–636 (2009).
13. A. Carnicer et al., "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.* **30**(13), 1644–1646 (2005).
14. X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.* **31**(22), 3261–3263 (2006).
15. X. Peng et al., "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.* **31**(8), 1044–1046 (2006).
16. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.* **35**(2), 118–120 (2010).
17. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," *Opt. Lett.* **30**(11), 1306–1308 (2005).
18. A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," *Appl. Opt.* **48**(31), 5933–5947 (2009).
19. A. Alfalou et al., "Simultaneous fusion, compression, and encryption of multiple images," *Opt. Express* **19**(24), 24023–24029 (2011).
20. X. Wang and D. Zhao, "Fully phase multiple-image encryption based on superposition principle and the digital holographic technique," *Opt. Commun.* **285**(21–22), 4280–4284 (2012).
21. X. Deng and D. Zhao, "Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain," *Opt. Laser Technol.* **44**(2), 374–377 (2012).
22. H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxon algorithm and phase modulation in Fresnel-transform domain," *Opt. Lett.* **34**(24), 3917–3919 (2009).
23. H. T. Chang, H. E. Hwang, and C. L. Lee, "Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain," *Opt. Commun.* **284**(18), 4146–4151 (2011).
24. H. T. Chang et al., "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," *Appl. Opt.* **50**(5), 710–716 (2011).
25. H. Li and Y. Wang, "Double-image encryption based on iterative gyrator transform," *Opt. Commun.* **281**(23), 5745–5749 (2008).
26. Z. Liu et al., "Double image encryption by using iterative andom binary encoding in gyrator domains," *Opt. Express* **18**(11), 12033–12043 (2010).
27. X. Wang and D. Zhao, "Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval," *Opt. Commun.* **284**(19), 4441–4445 (2011).
28. X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Commun.* **285**(6), 1078–1081 (2012).
29. X. Wang and D. Zhao, "Double images encryption method with resistance against the specific attack based on asymmetric algorithm," *Opt. Express* **20**(11), 11994–12003 (2012).
30. H. Li and Y. Wang, "Double-image encryption based on discrete fractional random transform and chaotic maps," *Opt. Lasers Eng.* **49**(7), 753–757 (2011).
31. Y. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Opt. Lasers Eng.* **51**(4), 472–480 (2013).
32. L. Sui et al., "Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain," *Opt. Lasers Eng.* **51**(12), 1297–1309 (2013).
33. H. Li and Y. Wang, "Double-image encryption by iterative phase retrieval algorithm in fractional Fourier domain," *J. Mod. Opt.* **55**(21), 3601–3609 (2008).
34. N. Zhou et al., "Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform," *Opt. Commun.* **284**(12), 2789–2796 (2011).

Liansheng Sui received his PhD degree in 2003, and now he is an associate professor at the School of Computer Science and Engineering, Xi'an University of Technology, China. His research interests include optics communications, image analysis, and pattern recognition.

Haiwei Lu received her BS degree in 2012, and now she is an MS candidate at the School of Computer Science and Engineering, Xi'an University of Technology, China. Her research interests include optics communications and image processing.

Xiaojuan Ning received her PhD degree in 2011, and she currently works in Xi'an University of Technology. Meanwhile, she has cooperated with Institute of LIAMA and National Laboratory of Pattern Recognition at Institute of Automation, Chinese Academy of Sciences. Her current research interests include scene modeling and shape analysis.

Yinghui Wang received his BS, MS, and PhD degrees in 1989, 1999, and 2002, respectively, and now he is a professor at the School of Computer Science and Engineering, Xi'an University of Technology, China, and Institute of Computer Science, Shaanxi Normal University, China. His research interests include software evolution, image analysis, and pattern recognition.