Double-image sharing encryption based on associated fractional Fourier transform and gyrator transform

Jinpeng Ma (马金鹏)[1], Zhengjun Liu (刘正君)[2], Zhongyi Guo (郭忠义)[1], and Shutian Liu (刘树田)[1*]

[1] *Department of Physics, Harbin Institute of Technology, Harbin 150001, China*

[2] *Department of Automation Measurement and Control Engineering, Harbin Institute of Technology, Harbin 150001, China*

[*] *E-mail: stliu@hit.edu.cn*

Received June 22, 2009

We present a novel method for realizing double-image encryption algorithm by combining the images in different transform domains. Two original images are encrypted into two interim images by fractional Fourier transform and gyrator transform, respectively. The two encrypted images can be obtained by means of the addition and subtraction of the two interim images. This is defined as a double-image sharing scheme, in which the original images are encrypted into two parts. The original images cannot be recovered only with any one of the two interim images. Numerical simulation experiments demonstrate the validity of the algorithm.

OCIS codes: 100.0100, 200.3050, 100.2000.

doi: 10.3788/COL20100803.0290.

Optical information security is becoming an important subject in communication science. During the past decade, a number of image encryption algorithms have been proposed[1−5]. A classical one is the random phase encoding scheme in Fourier domain[1], moreover, in the fractional Fourier transform (FrFT) domain[2] and Fresnel diffraction domain[3]. This algorithm has been proved that the security is attractive in defence[6,7]. Owing to the advantage of fractional order and wide range of applications in optics, the FrFT is frequently used for image encryption. Recently, the gyrator transform (GT) has also attracted lots of attention in the field of image processing[8,9]. GT is related closely to the FrFT and is also an image encryption and decryption tool.

Multi-image encryption is a new concept in the field of information security. Several multi-image encryption algorithms have been proposed[10−16]. The algorithms proposed in Refs. [10, 11] encode two original images into the amplitude and phase in the input and combine them into one image. However, these methods have the drawbacks in optical implementations since the decrypted phase image cannot be easily manipulated. Situ *et al*. proposed the algorithm by using wavelength multiplexing[12] and position multiplexing methods[13], but the decrypted images are not perfect due to the cross-talk effects between images. Moreover, double-image encryption based on FrFT by using Gerechberg-Saton (G-S) phase retrieval algorithm[14], fractional spectrum cutting[15], and random phase encoding[16] have been proposed, respectively.

In Ref. [5], an image encryption scheme has been proposed, in which the original image is encrypted into two encrypted images by means of commutation and anti-commutation rules with one-dimensional (1D) FrFT. In this letter, we generalize this image encryption scheme to the double-image sharing encryption. Two original images are firstly encoded by FrFT and GT with random phases respectively. Then the two interim encoded images are combined together with addition and subtraction to yield two encrypted sharing parts. The original information can only be retrieved with both encrypted images.

As the same as the FrFT, gyrator operation also belongs to linear canonical transform, which produces a rotation in twisted position-spatial frequency planes on the phase space. Both FrFT and GT are written as the form of integral transform. The FrFT and GT with the order α of a two-dimensional (2D) function $f_{\rm i}(x_{\rm i}, y_{\rm i})$ are expressed as

$$f_{\rm o}\left(x_{\rm o}, y_{\rm o}\right) = \iint f_{\rm i}\left(x_{\rm i}, y_{\rm i}\right) K_{\alpha}\left(x_{\rm i}, y_{\rm i}; x_{\rm o}, y_{\rm o}\right) {\rm d}x_{\rm i}{\rm d}y_{\rm i}. \tag{1}$$

The kernel of GT is defined as

$$K_{\alpha}\left(x_{\rm i}, y_{\rm i}; x_{\rm o}, y_{\rm o}\right) = \frac{1}{|\sin\phi_{\alpha}|} \exp\left[2{\rm i}\pi \frac{\left(x_{\rm o}y_{\rm o} + x_{\rm i}y_{\rm i}\right)\cos\phi_{\alpha} - \left(x_{\rm i}y_{\rm o} + x_{\rm o}y_{\rm i}\right)}{\sin\phi_{\alpha}}\right], \tag{2}$$

and the kernel of 2D FrFT is given as

$$K_{\alpha}\left(x_{\rm i}, y_{\rm i}; x_{\rm o}, y_{\rm o}\right) = \left(1 - {\rm i}\cot\phi_{\alpha}\right) \exp\left[{\rm i}\pi \frac{\left(x_{\rm i}^2 + y_{\rm i}^2\right)\cos\phi_{\alpha} - 2\left(x_{\rm i}x_{\rm o} + y_{\rm i}y_{\rm o}\right) + \left(x_{\rm o}^2 + y_{\rm o}^2\right)\cos\phi_{\alpha}}{\sin\phi_{\alpha}}\right], \tag{3}$$

where $(x_{\rm i}, y_{\rm i})$ and $(x_{\rm o}, y_{\rm o})$ indicate the input and output coordinates, respectively, and $\phi_\alpha = \alpha\pi/2$ is the transform angle. From the kernel functions, the difference between GT and FrFT is apparent that the kernel function of the GT is a product of hyperbolic and plane waves, however, the kernel function of the FrFT is a product of spherical and plane waves.

We propose the method for the double-image sharing encryption. Both of the two original images are encoded by FrFT and GT respectively. Then the two results of the transformation are combined together to obtain two encrypted images by a specific mathematical method. The random phase is used to encode the original images into white noise in the mathematic process, however, unlike double-random-phase encoding, the random phase is not required in the process of image decryption.

Let $I_1(x,y)$ and $I_2(x,y)$ denote the original images respectively. The double-image encryption algorithm is expressed as

$$P_1(x_{\rm o}, y_{\rm o}) = \mathcal{G}^{\alpha_1}\{I_1(x,y) R_1(x,y)\} + \mathcal{F}^{\alpha_2}\{I_2(x,y) R_2(x,y)\}, \quad (4)$$

$$P_2(x_{\rm o}, y_{\rm o}) = \mathcal{G}^{\alpha_1}\{I_1(x,y) R_1(x,y)\} - \mathcal{F}^{\alpha_2}\{I_2(x,y) R_2(x,y)\}, \quad (5)$$

where $R_i(x,y)$ $(i = 1,2)$ are random phase functions. Without losing the generality, we use one random phase function (i.e., $R(x,y) = R_1(x,y) = R_2(x,y)$) in our numerical simulations. The symbols $\mathcal{G}^\alpha\{\cdots\}$ and $\mathcal{F}^\alpha\{\cdots\}$ denote the GT and FrFT with order α, respectively, which also can be regarded as extra keys in the encrypting system, in which the original images were encrypted into two encoding interim images. By combining the two encoding interim images in a given way of addition and subtraction mathematically, we get the final encrypted images. In cryptography, the scheme is a secret sharing with two participants. However, the difference is that the double-images are encrypted instead of a single one in our scheme. The encryption process requires both of the two participants together. It is obvious that there are no unique solutions for two variables only with Eq. (4) or (5), hence the original images cannot be mathematically reconstructed with knowing only one of P_1 and P_2.

An experimental setup to implement the proposed double-image encryption algorithm in optics based on Mach-Zehnder interferometer is shown in Fig. 1. The FrFT is implemented in optics by one lens as we all know.

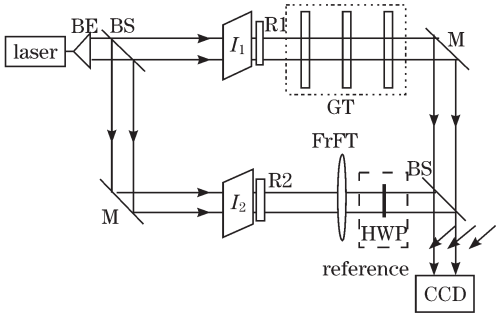

Fig. 1. Experimental setup of the double-image encryption. BE: beam expander; BS: beam splitter; R: random phase mask; M: mirror.

The GT can be performed by an optical system which is constructed from three generalized lenses and two fixed free space intervals, and every generalized lens is a combination of two convergent cylindrical lenses of the same power. The transformation parameter α of GT could be changed by rotating the cylindrical lenses.

In this encrypted system, the original images and random phase masks are placed in two different arms, respectively. The upper arm implements GT, whereas the lens in the lower arm performs FrFT. The half wave plate (HWP) in lower arm to control the relative phase between two beams could change the addition or subtraction between the two secret images. The operations are corresponding to Eqs. (4) and (5). The encrypted images as the superposition of two beams can be recorded by a charge-coupled device (CCD) with the on-line digital holography.

The decrypted process is the inverse of the encryption. It is performed by addition and subtraction of the encrypted images with the corresponding GT and FrFT of orders $-\alpha_1$ and $-\alpha_2$, respectively. The decrypted process is implemented easily either digitally or optically. The same as the encrypted algorithm, it is expressed as

$$\mathcal{G}^{-\alpha_1}\{P_1 + P_2\} = 2I_1', \quad (6)$$

$$\mathcal{F}^{-\alpha_2}\{P_1 - P_2\} = 2I_2', \quad (7)$$

where $I_i' = I_i(x,y) R_i(x,y)$, $(i$=1,2) represent the recovered images. If only the intensities are required, the random phase cannot be used in the decrypted process.

A series of numerical simulation experiments were performed to demonstrate the effectiveness of the proposed method. The original images are cameraman and Lean both with 256×256 pixels, as shown in Figs. 2(a) and (b), respectively. The interim encoding images are obtained by GT of original image multiplied by random phase with order of 0.6 in Fig. 2(a) and the FrFT with order of 1.1 in Fig. 2(b) multiplied by random phase. The random phase function was uniformly randomly distributed in the

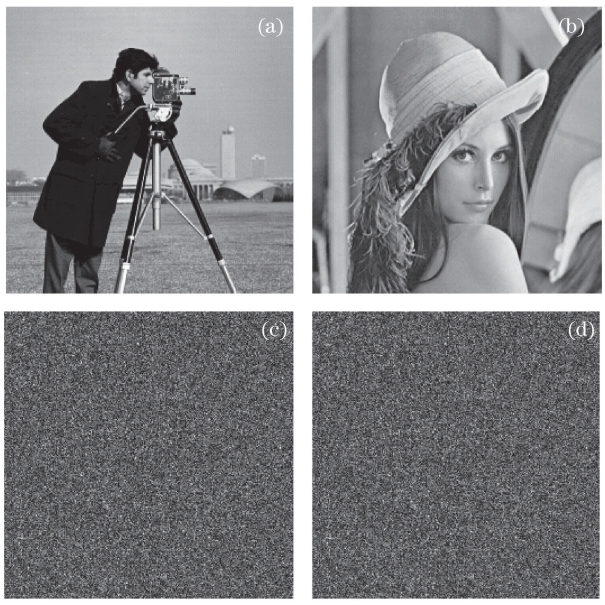

Fig. 2. Two orignal images of (a) cameraman and (b) Lena. The encrypted images of (c) P_1 and (d) P_2.

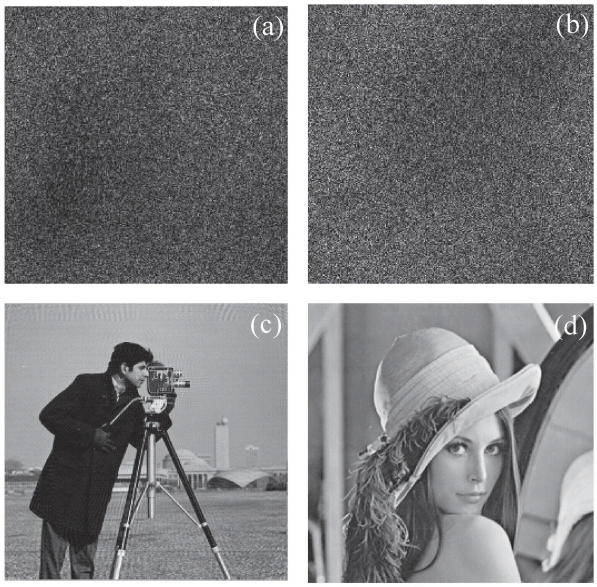

Fig. 3. Decrypted images from only one of the encrypted images with correct orders of (a) GT and (b) FrFT, respectively. Correct decrypted results of (c) cameraman and (d) Lena.

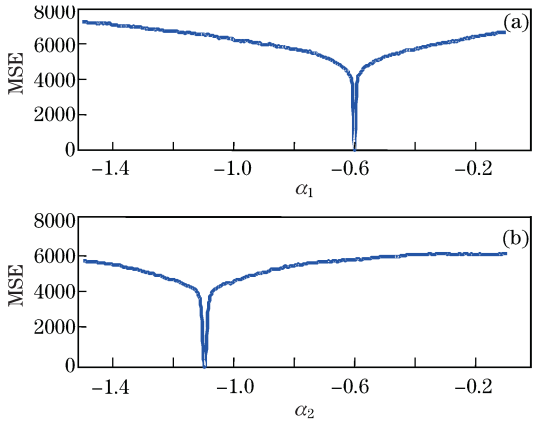

Fig. 4. MSE curves between the decrypted images obtained by (a) GT and (b) FrFT with different orders and original images.

range of $[0, 2\pi]$. The encrypted images depicted in Figs. 2(c) and (d) are obtained by combining two interim encoding images according to Eq. (2). If only one of the encrypted images is obtained by unauthorized people, it is impossible to recover the original images even other parameters (such as the transformation order) are taken too. The direct decrypted results from one of the encryption image (Fig. 2(c)) by GT and FrFT with correct orders are given in Figs. 3(a) and 2(b) respectively. The results are completely white noise images. Any information about the initial images cannot be found from these results. The reconstructed results with both encrypted images and correct orders are displayed in Figs. 3(c) and (d), respectively. The results were retrieved with high fidelity to the original images.

To evaluate the reliability of this encryption method, the mean square error (MSE) is introduced as

$$\mathrm{MSE} = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}|X'_{m,n} - X_{m,n}|^2}{M \times N}, \qquad (8)$$

where X' and X denote the amplitudes of the retrieved image and original image, and M and N are the pixel numbers of the images. The dependence of MSE on the changes of orders of GT and FrFT are shown in Figs. 4(a) and (b), respectively. From these curves, it proves that the MSE has the minimum value for a very narrow range of orders of GT and FrFT. It means that the orders are also the key ingredients to provide a good security for our algorithm. The corresponding MSE values of Figs. 3(c) and (d) between the original images are 3.66×10^{-27} and 3.48×10^{-27}, respectively. It means that the original images have been retrieved nearly completely. The simulation results show that this double-image encryption algorithm is effective.

In conclusion, a novel method for double-image encryption is proposed based on combination of FrFT and GT. In this algorithm, the original double-images are encrypted into two different transform domains simultaneously, and then shared into another two images. The obtained sharing parts are associated, with only one of them we cannot decrypt the original images. Numerical simulation results demonstrate the effectiveness of this algorithm. By using two different transforms, the orders of GT and FrFT can be regarded as the extra keys, hence the security of this algorithm is promoted. Furthermore, this algorithm can be implemented by two FrFTs with different orders.

This work was supported by the National Natural Science Foundation of China under Grant Nos. 10674038 and 10974039.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20,** 767 (1995).
2. G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25,** 887 (2000).
3. G. Situ and J. Zhang, Opt. Lett. **29,** 1548 (2004).
4. Y. Wang, Y. Wang, and Y. Yang, Chinese J. Lasers (in Chinese) **33,** 1360 (2006).
5. Z. Liu, M.-A. Ahmad, and S. Liu, Opt. Commun. **279,** 285 (2007).
6. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, Appl. Opt. **46,** 6641 (2007).
7. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, Opt. Express **15,** 10253 (2007).
8. J. A. Rodrigo, T. Alieva, and M. L. Calvo, Opt. Express **15,** 2190 (2007).
9. J. A. Rodrigo, T. Alieva, and M. L. Calvo, J. Opt. Soc. Am. A **24**, 3135 (2007).
10. X. Meng, L. Cai, M. He, G. Y. Dong, and X. X. Shen, J. Opt. A: Pure Appl. Opt. **7,** 624 (2005).
11. M. He, L. Cai, Q. Liu, X. Wang, and X. Meng, Opt. Commun. **247,** 29 (2005).
12. G. Situ and J. Zhang, Opt. Lett. **30,** 1306 (2005).
13. G. Situ and J. Zhang, J. Opt. A: Pure Appl. Opt. **8,** 391 (2006).
14. Z. Liu and S. Liu, Opt. Commun. **275,** 324 (2007).
15. Z. Liu, Q. Li, J. Dai, X. Sun, S. Liu, and M. A. Ahmad, Opt. Commun. **282,** 1536 (2009).
16. R. Tao, Y. Xin, and Y. Wang, Opt. Express **15,** 16067 (2007).