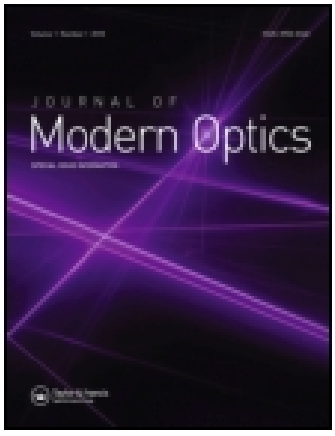

Journal of Modern Optics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tmop20

Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique

Lihua Gong [a] , Xingbin Liu [a] , Fen Zheng [a] & Nanrun Zhou [a b c]

[a] Department of Electronic Information Engineering , Nanchang University , Nanchang 330031 , China

[b] Information Security Center , Beijing University of Posts and Telecommunications , Beijing 100876 , China

[c] Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition , Nanchang Hangkong University , Nanchang 330063 , China

Published online: 13 Sep 2013.

To cite this article: Lihua Gong , Xingbin Liu , Fen Zheng & Nanrun Zhou (2013) Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique, Journal of Modern Optics, 60:13, 1074-1082, DOI: 10.1080/09500340.2013.831139

To link to this article: http://dx.doi.org/10.1080/09500340.2013.831139

Journal of Modern Optics, 2013
Vol. 60, No. 13, 1074–1082, http://dx.doi.org/10.1080/09500340.2013.831139

Taylor & Francis
Taylor & Francis Group

Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique

Lihua Gong[a], Xingbin Liu[a], Fen Zheng[a] and Nanrun Zhou[a,b,c]*

[a]*Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China;* [b]*Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;* [c]*Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, Nanchang 330063, China*

(*Received 1 July 2013; accepted 29 July 2013*)

We present a novel multiple-image encryption algorithm by combining log-polar transform with double random phase encoding in the fractional Fourier domain. In this algorithm, the original images are transformed to annular domains by inverse log-polar transform and then the annular domains are merged into one image. The composite image is encrypted by the classical double random phase encoding method. The proposed multiple-image encryption algorithm takes advantage of the data compression characteristic of log-polar transform to obtain high encryption efficiency and avoids cross-talk in the meantime. Optical implementation of the proposed algorithm is demonstrated and numerical simulation results verify the feasibility and the validity of the proposed algorithm.

Keywords: log-polar transform; fractional Fourier transform; multiple-image encryption

1. Introduction

Over the past few decades, information security has played an important role in social activities and has attracted more and more attention. As one of the hottest research topics, image encryption has been further developed by many scholars. In recent years, optical information processing technology has demonstrated its advantages in the field of image encryption due to its high processing speed and more degrees of freedom. Various optical techniques have been reported for image encryption [1–24]. Among them, the double random phase encoding (DRPE) algorithm [1] is the most commonly used method, where two independent random phase masks are located at the input plane and the transform plane, respectively, and the plaintext can be encoded into stationary white noise. Subsequently, Unnikrishnan et al. extended this classical algorithm from the Fourier domain to fractional Fourier domain [3], which enhanced the security of encryption systems. Some transforms with new features have been applied to the field of image encryption to achieve better system performance, such as the gyrator transform [16], fractional Mellin transform [17–19], fractional cosine transform [20], and so on.

In recent years, optical image encryption has been extended to multiple-image encryption (MIE) to raise the efficiency of encryption. Plenty of approaches have been exploited in this promising field, such as interference and grating modulation [25], wavelength multiplexing [26], position multiplexing [27], random phase matching [28], and key rotation multiplexing [29], etc. It is obvious that all these techniques mentioned above cannot avoid cross-talk effects. However, there are some techniques used in image encryption that also avoid cross-talk to some extent. For example, Liu et al. proposed an optical multiple-image encryption algorithm based on frequency shift [30]. Deng et al. proposed a multiple-image encryption scheme using a phase retrieval algorithm and intermodulation in the Fourier domain [31]. The number of images to be encrypted in some multiple-image encryption schemes is fixed. In practice, the speed and efficiency of image encryption algorithms are limited for a fixed number of encrypted images.

In this paper, we propose a flexible multiple-image encryption algorithm by utilizing data compression characteristics of log-polar transform (LPT). The images to be encrypted are transformed by inverse log-polar transform (ILPT) into annular domains, and several annular domain images are superimposed together to yield a single image by choosing proper radii. Then the composite image will be encrypted by DRPE in the fractional Fourier domain, which can be implemented with an opto-electronic hybrid setup. The proposed algorithm avoids cross-talk and the number of images to be encrypted is

*Corresponding author. Email: nrzhou@ncu.edu.cn

variable. In the proposed algorithm, different numbers of images can be encrypted by choosing different radii parameters. Owing to the images to be encrypted being transformed by ILPT into annular domains, if the number of images is increased, the information contained in the annular domain will be decreased. Therefore, the capacity of encryption algorithm can be increased at the cost of the quality of the decrypted images. The rest of this paper is organized as follows: a brief introduction of the basic theory is given in Section 2, the multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique is proposed in Section 3, simulation results are given in Section 4 to demonstrate the effectiveness and the robustness of the proposed algorithm, and some concluding remarks are summarized in the final section.

2. Basic theory

2.1. Fractional Fourier transform

Fractional Fourier transform (FrFT) is a powerful tool for signal and optical information processing. FrFT can be exactly implemented in optics with single lens by changing the distances of the lens performing the Fourier transform. Conventionally, the α order FrFT [32,33] can be expressed as

$$F^{\alpha}\{f(x)\}(u) = \int_{-\infty}^{+\infty} K_{\alpha}(x,u) f(x)\mathrm{d}x, \tag{1}$$

where $f(x)$ indicates the input function and $K_{\alpha}(x,u)$ is the transform kernel function, i.e.

$$K_{\alpha}(x,u) = \begin{cases} A\exp[\mathrm{i}\pi(x^2\cot\varphi - 2xu\csc\varphi + u^2\cot\varphi)], & \alpha \neq n\pi, \\ \delta(x-u), & \alpha = 2n\pi, \\ \delta(x+u)\ , & \alpha = (2n+1)\pi. \end{cases} \tag{2}$$

and

$$A = \frac{\exp[-\mathrm{i}(\pi\mathrm{sgn}(\varphi)/4 - \varphi/2)]}{\sqrt{|\sin\varphi|}}, \tag{3}$$

where $\varphi = \alpha\pi/2$ is the transformation angle corresponding to the transform order. When $\alpha = 1$, the FrFT reduces to the ordinary Fourier transform. The two-dimensional FrFT is

$$F^{\alpha_1,\alpha_2}\{f(x,y)\}(u,v) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} K_{\alpha_1,\alpha_2}(x,y;u,v) f(x,y)\mathrm{d}x\mathrm{d}y, \tag{4}$$

with the transform kernel

$$K_{\alpha_1,\alpha_2}(x,y;u,v) = K_{\alpha_1}(x,u)K_{\alpha_2}(y,v). \tag{5}$$

2.2. The log-polar transform

The log-polar transform is a conformal mapping from the points in the Cartesian coordinates plane (x,y) to the points in the log-polar plane (u,v). A detailed introduction to the log-polar transform can be found in [34]. For a digital image, as shown in Figure 1, the log-polar transform maps pixel circular rings centered with central point to columns of log-polar coordinates. Suppose one pixel of original image on the Cartesian coordinates denotes as (x,y) and the corresponding pixel on the log-polar plane denotes as (u,v), the vector from the pixel (x,y) to the central point $(0,0)$ denotes as $\mathbf{p}$, the mapping relation between the original image and the transformed image can be described as

$$\begin{cases} \rho = \ln\sqrt{x^2+y^2} \\ \theta = \arctan\dfrac{y}{x} \end{cases}, \tag{6}$$

$$\begin{cases} u = [m\cdot\rho] \\ v = [n\cdot\theta] \end{cases}, \tag{7}$$

where ρ denotes the module of vector $\mathbf{p}$, and θ denotes the angle between vector $\mathbf{p}$ and x-axis positive direction. m and n are constants to adjust the results and the square brackets are used to indicate the integer part.

In the realization process of log-polar transform, some parameters should be set in advance. These parameters include the center position, the radii of the innermost and the outermost rings, the numbers of discrete sampling points along distance axis, and the angle axis. The size of the transformed image is determined by the number of discrete sampling points along distance axis and the angle axis. Meanwhile, there exists no one-to-one correspondence relationship between Cartesian coordinate and log-polar coordinate owing to the log-polar transform being a nonlinear transform. In addition, the log-polar transform has properties of angle invariability and distance invariability, i.e. angle rotation in Cartesian

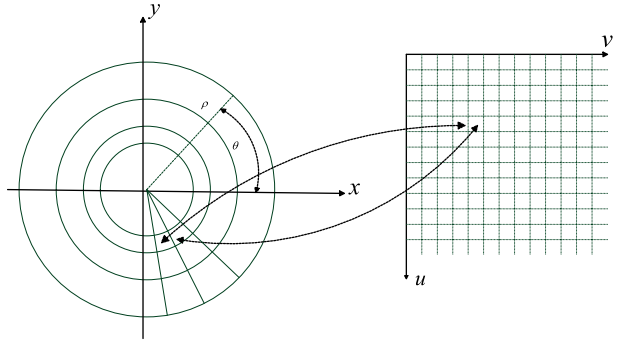

Figure 1. Log-polar mapping. (The colour version of this figure is included in the online version of the journal.)

coordinate causes left and right movements in the log-polar plane, scale variation in Cartesian coordinate would lead to upper and lower movements in the log-polar plane.

3. Multiple-image encryption and decryption algorithm

To encrypt many images, we consider transforming each image into an annular domain with ILPT, and different annular domain images can be merged into one image, then the multiple-image encryption algorithm can be realized by encrypting the composite image. Based on this idea, a multiple-image encryption scheme is proposed, as shown in Figure 2. RPM1 and RPM2 represent two independent random phase masks. CRPM1 and CRPM2 represent the conjugate phase masks corresponding to RPM1 and RPM2, respectively. C denotes the ciphertext.

Suppose the images to be encrypted are $I_k(x,y), k = 1,2,\ldots,N$, with the size of $M \times M$ pixels. ILPT is introduced for transforming the original images to annular domains and the parameters of transform are radii of the innermost and the outermost rings, denoted by r_{in} and r_{out}, respectively.

The images to be encrypted are transformed by ILPT; each annular image should not overlap with another by choosing proper transform parameters, and this process can be expressed as

$$g_k(x,y) = \text{ILPT}\{I_k(x,y)\}, \qquad k = 1,2,\ldots,N. \tag{8}$$

Then the transformed images can be merged into one image $g(x,y)$

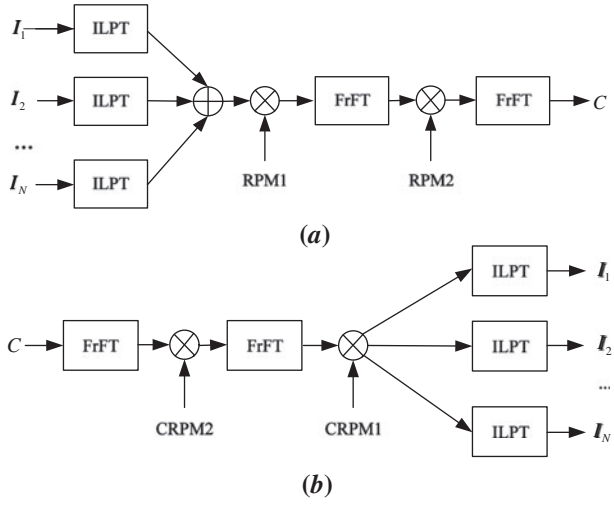

Figure 2. The flowcharts of (*a*) the encryption process and (*b*) the decryption process.

$$g(x,y) = \sum_{k=1}^{N} g_k(x,y), \qquad k = 1,2,\ldots,N, \tag{9}$$

where $g(x,y)$ denotes the composite image of N annular domains.

Next, the composite image $g(x,y)$ is encrypted by the double random phase encoding technique in the fractional Fourier transform domain and the final encrypted image $C(u,v)$ can be obtained as

$$C(u,v) = F^{\alpha_2}\{F^{\alpha_1}\{(g(x,y)\exp[\mathrm{i}\varphi(x,y)])\}\exp[\mathrm{i}\xi(u,v)]\}, \tag{10}$$

where $F^{\alpha}\{\cdot\}$ denotes fractional Fourier transform of α order, and the orders of two times fractional Fourier transform are α_1 and α_2, respectively. $\varphi(x,y)$ and $\xi(u,v)$ are two independent random phase masks with the value distributed in the interval $[0,2\pi]$ in the space domain and the frequency domain, respectively. In the whole encryption process, the encryption keys include the orders of FrFT and two random phase masks, while the radii of annular domains can serve as secondary keys.

The image decryption, as shown in Figure 2(*b*), is the inverse process of the encryption. With correct order keys α_1 and α_2, phase masks $\varphi(x,y)$ and $\xi(u,v)$, composite image $g(x,y)$ can be recovered by using double random phase decryption as

$$g(x,y) = F^{-\alpha_1}\{\{F^{-\alpha_2}[C(u,v)]\}\exp[-\mathrm{i}\xi(u,v)]\} \times \exp[-\mathrm{i}\varphi(x,y)], \tag{11}$$

where $F^{-\alpha}\{\cdot\}$ denotes an inverse fractional Fourier transform of order α. With the correct radii parameters used in the encryption, the center position is the center point of image, the discrete sampling points along distance axis and along angle axis are equal to the size of original images, thus the decrypted image can be obtained as

$$I_k(x,y) = \text{LPT}\{g_{r_{k,\text{in}},r_{k,\text{out}}}(x,y)\}, \quad k = 1,2,\ldots,N \tag{12}$$

where $r_{k,\text{in}}$ and $r_{k,\text{out}}$ denote the radii of the innermost and the outermost rings of the kth image. The quality of recovered images is determined by the scale of annular domains. The original images can be recovered well when the number of encrypted images is small.

The MIE algorithm can be implemented with an optoelectronic hybrid setup, which is depicted in Figure 3. At the beginning, some parameters of transformation are set in advance, and then the input images are transformed with ILPT in the computer successively and they are compressed into annular domains. Then the obtained annular domains are merged into one image (denoted as $g(x,y)$). Then the composite image $g(x,y)$

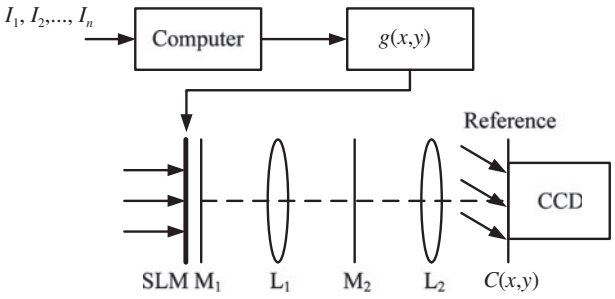

Figure 3. Optoelectronic hybrid setup.

modulated by spatial light modulator (SLM) is encrypted by the DRPE system. In the DRPE system, the composite image is multiplied by random phase masks M1 and M2 in space domain and fractional Fourier domain, respectively. Finally, the obtained ciphertext $C(x,y)$ can be directly captured by CCD.

4. Numerical simulation and discussion

To demonstrate the effectiveness and the reliability of the proposed image encryption algorithm, some experiments were conducted. The three images shown in Figures 4(*a–c*) with 512×512 pixels were chosen to be encrypted. The radii $(r_{\text{in}}, r_{\text{out}})$ of ILPT for the three original images are $(30, 126)$, $(127, 195)$, $(196, 255)$, respectively. Thus the radii of three obtained annular domains are different to each other and the three annular domains can be merged into one image without loss of useful information.

The composite image is shown in Figure 5(*a*), which has 511×511 pixels. In the DRPE process, the orders of FrFT are $\alpha_1 = 0.5$, $\alpha_2 = 0.3$, respectively. Two random phase masks M_1, M_2 are generated by random functions and distributed in the interval $[0, 2\pi]$. Figure 5(*b*) is the final encrypted image.

The decrypted images, which can be obtained with the correct decryption keys, are shown in Figures 6(*a–c*). The discrete sampling points along the distance axis and along the angle axis are equal to 512, and the size of the decrypted images is equal to that of the original images. Though the edges of the decrypted images have a little distortion, they are acceptable visually.

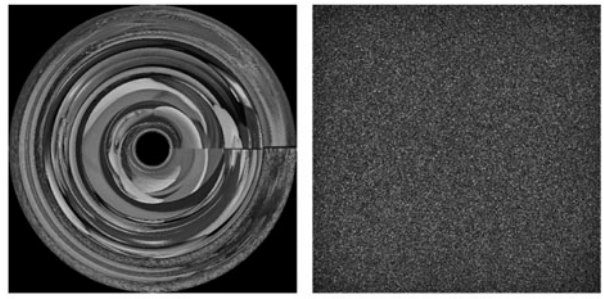

Figure 5. (*a*) Composite image, (*b*) encrypted image.

To evaluate the quality of a decrypted image, a mean square error (MSE) algorithm is introduced,

$$\text{MSE} = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} |I_o(x,y) - I_o'(x,y)|^2}{M \times N} \qquad (13)$$

where $I_o(x,y)$ and $I_o'(x,y)$ denote the pixel values of the original image and retrieved image, respectively. For the three decrypted images shown in Figures 6(*a–c*), the corresponding values of MSE are 813.0, 1180.4, and 1119.5, respectively. The values of MSE are within the acceptable range.

4.1. Statistical analysis

In image analysis, an image histogram is used to demonstrate the distribution of image pixels. Figures 7(*a–d*) show the histograms of the original images and ciphertext, respectively. The histogram of ciphertext is quite different from the histograms of original images; therefore, the attackers cannot obtain any useful information on the original images with statistical analysis.

The correlation coefficient used to express the correlation of image pixels is defined as:

Figure 4. Original images: (*a*) Lena, (*b*) peppers, (*c*) baboon.

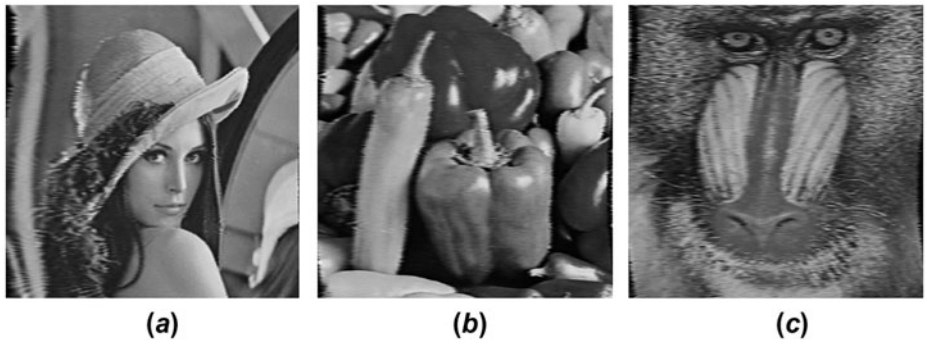

Figure 6. Decryption results with correct keys.

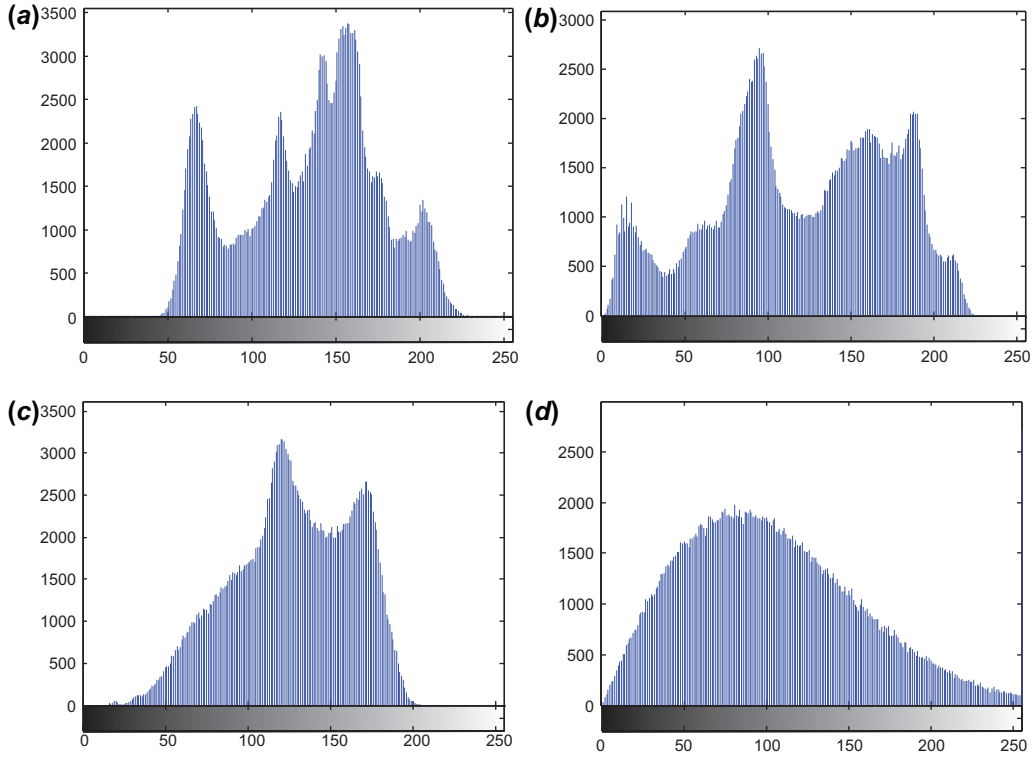

Figure 7. The histograms of original images and encrypted image: (*a*) histogram of Lena; (*b*) histogram of peppers; (*c*) histogram of baboon; (*d*) histogram of ciphertext. (The colour version of this figure is included in the online version of the journal.)

$$C = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}}, \qquad (14)$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$, $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. In order to test the correlation of original images and ciphertext, 2000 pairs of adjacent pixels were randomly selected in three directions, respectively. The correlation coefficients of original images and ciphertext are given in Table 1. The pixels of original images are highly correlated in horizontal, vertical, and diagonal directions. The correlation coefficients of the ciphertext are very small, which indicates the adjacent pixels of the encrypted image are irrelevant.

From the statistical analysis, it can be seen that the proposed algorithm can resist statistical attacks.

4.2. Key sensitivity analysis

The security of the proposed scheme is ensured by DRPE in the FrFT domain; the keys include the orders of FrFT and two random phase masks. If one of the orders of FrFT is not correct, the decrypted image cannot be recognized. Figure 8 shows the MSE curves with FrFT orders for three images. Generally, when the value of MSE is larger than 3.5×10^3, any useful information on the original image cannot be obtained from the

Table 1. Correlation coefficients of adjacent pixels.

Correlation coefficient	Horizontal	Vertical	Diagonal
Lena	0.9773	0.9596	0.9345
Peppers	0.9768	0.9594	0.9495
Baboon	0.7107	0.8212	0.6887
Ciphertext	0.0474	0.0236	0.0262

decrypted image. The value of MSE is high when the deviation of FrFT order is small. From the MSE curves, one can see the system is sensitive to the orders of FrFT.

The two random phase masks used in the encryption process are the main keys of the proposed scheme. When the random phase masks M_1 and M_2 are not correct, the decrypted images will be noise-like images, as shown in Figures 9(*a*–*c*).

4.3. Robustness analysis

In the process of recording, transmission, and storage, due to equipment reasons the ciphertext image may partially lost or be blended with noise, which may lead to the images not being decrypted correctly. Therefore, the robustness of this algorithm was examined by testing occlusion and noise attacks. The encrypted image cut by 25% is shown in Figure 10(*a*), and the corresponding decrypted images are shown in Figures 10(*b*–*d*), respectively. The decrypted images can also undoubtedly be recognized.

Noise can be added to the encrypted image C as follows:

$$C' = C(1 + sG_n), \tag{15}$$

where G_n represents white Gaussian noise with zero-mean and unit variance, s is the coefficient indicating the strength of noise. Figure 11(*a*) shows the encrypted image distorted by noise with $s = 0.1$. The decrypted images with correct keys are listed in Figure 11(*b*–*d*), showing that the major information of the original images can still be obtained. As a result, this method is robust enough against occlusion and noise attacks.

4.4. Encryption capacity

We then tried to encrypt more images by using this algorithm. Five original test images, shown in Figures 12(*a*–*e*), were chosen for encryption. The parameters (r_{in}, r_{out}) of ILPT corresponding to the images in Figures 12(*a*–*e*) were

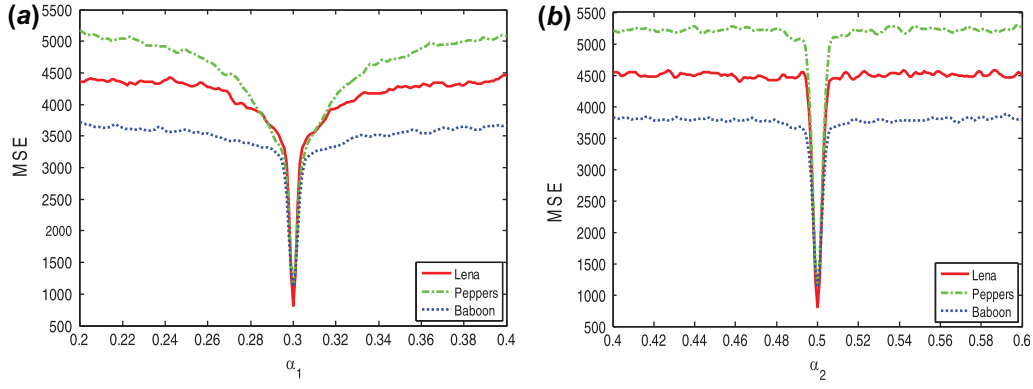

Figure 8. MSE curves versus deviation of FrFT orders. (The colour version of this figure is included in the online version of the journal.)

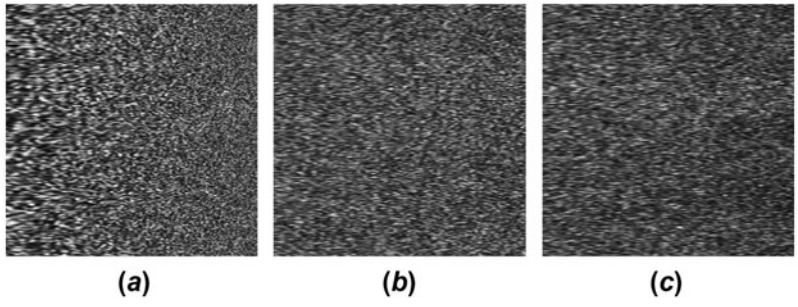

Figure 9. Decrypted images with incorrect phase keys.

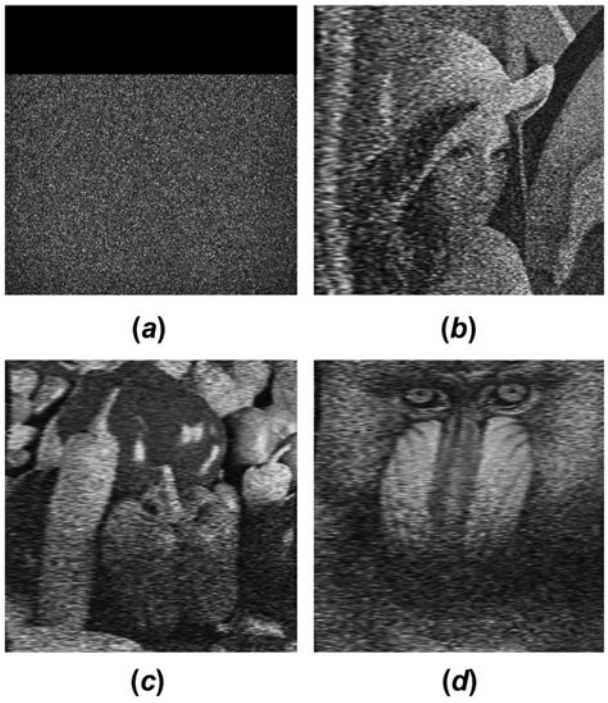

Figure 10. Decrypted results against occlusion attack of cutting upper data: (*a*) attacked image, (*b–d*) corresponding decrypted images.

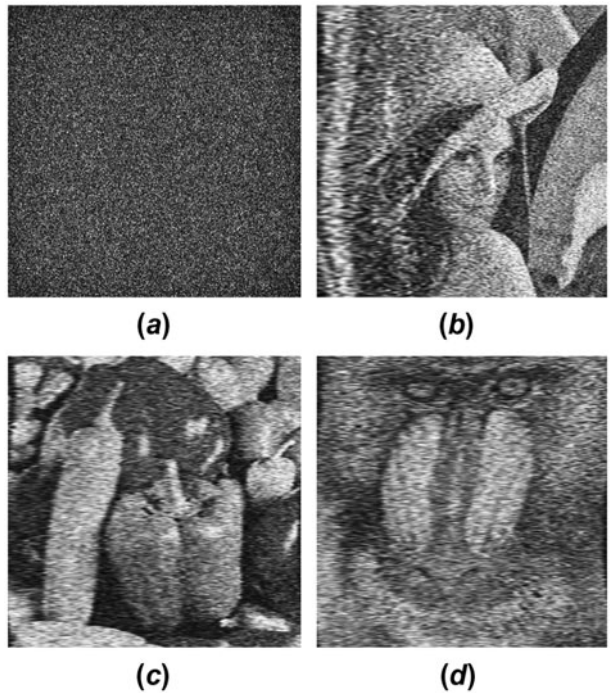

Figure 11. Decrypted results against noise attack with $s = 0.5$: (*a*) attacked image, (*b–d*) corresponding decrypted images.

chosen as $(30, 86)$, $(87, 145)$, $(146, 175)$, $(176, 210)$, and $(211, 255)$, respectively. The decrypted images with correct keys are shown in Figures 12(*f–j*).

To further test the effectiveness and the encryption capacity of the proposed algorithm, eight original test images, shown in Figures 13(*a–h*), were encrypted and decrypted. The parameters (r_{in}, r_{out}) for encrypting eight

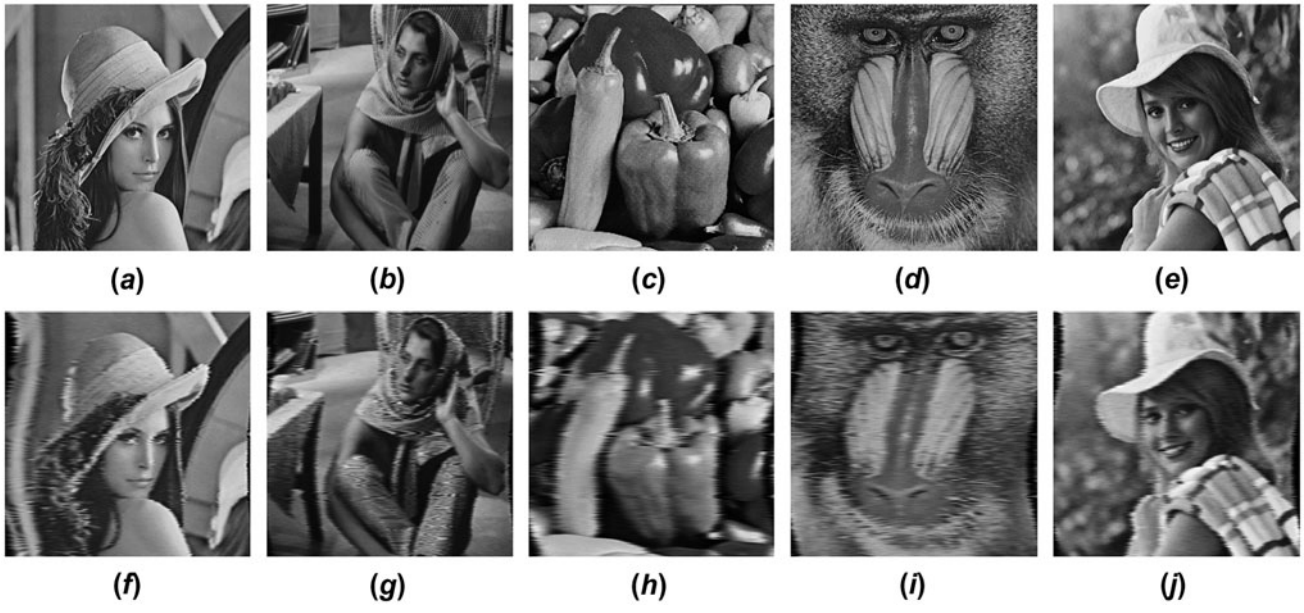

Figure 12. The simulation results: (*a–e*) five original images for encryption; (*f–j*) decrypted images corresponding to the original images.

Figure 13. The simulation results: (*a–h*) eight original images for encryption; (*i–p*) decrypted images corresponding to the original images.

original images were $(15, 50)$, $(51, 80)$, $(81, 110)$, $(111, 140)$, $(141, 170)$, $(171, 200)$, $(201, 230)$, and $(231, 255)$, respectively. The correctly decrypted images are shown in Figures 13(*i–p*). The main information of the original test images can be easily obtained from the decrypted images. It can be seen from the simulation results that the proposed algorithm is flexible on the number of images to be encrypted. The decrypted image has a little distortion since, in the process of LPT, there is no one-to-one correspondence between the pixel values of the original image and the transformed image. The encryption process and the decryption process are fast as the algorithm can be realized by an optoelectronic hybrid setup. Therefore, the proposed algorithm suits the requirements of high-speed transmission with moderate decrypted image quality.

5. Conclusion

We have proposed a new algorithm of multiple-image encryption by introducing LPT into the field of image encryption, which provides a new method for designing multiple-image encryption schemes. In the encryption process, we take full advantage of the LPT to compress

original images into annular domains and merged these annular domains into one image. Then the composite image is encrypted by the DRPE technique. All plaintexts can be extracted from the ciphertext without any cross-talk. This algorithm can be realized with a simple optoelectronic hybrid setup, which improves the efficiency of encryption and decryption. A series of numerical simulations have been shown to demonstrate the effectiveness and the security of the proposed method, and the capacity of the proposed algorithm has also been examined. The simulations verify that the proposed algorithm is flexible in encrypting multiple images, and does not increase the difficulty of optical implementation.

Funding

This work was supported by the National Natural Science Foundation of China [grant number 61262084], [grant number 61141007]; the Foundation for Young Scientists of Jiangxi Province (Jinggang Star), the Natural Science Foundation of Jiangxi Province [grant number 20114BAB201018], [grant number 2009GQS0080]; the Opening Project of Key Laboratory of Image Processing and Pattern Recognition (Nanchang Hangkong University), Jiangxi Province [grant number TX201204002].

References

[1] Refregier, P.; Javidi, B. *Opt. Lett.* **1995,** *20,* 767–769.
[2] Zhang, S.Q.; Karim, M.A. *Microwave Opt. Technol. Lett.* **1999,** *21,* 318–323.
[3] Unnikrishnan, G.; Joseph, J.; Singh, K. *Opt. Lett.* **2000,** *25,* 887–889.
[4] Mogensenn, P.C.; Gluckstad, J. *Opt. Lett.* **2000,** *25,* 566–568.
[5] Li, Y.Z.; Kreske, K.; Rosen, J. *Appl. Opt.* **2000,** *39,* 5295–5301.
[6] Peng, X.; Cui, Z.Y.; Tan, T.N. *Opt. Commun.* **2002,** *212,* 235–245.
[7] Seo, D.H.; Kim, S.J. *Opt. Lett.* **2003,** *28,* 304–306.
[8] Situ, G.H.; Zhang, J.J. *Opt. Lett.* **2004,** *29,* 1584–1586.
[9] Zhao, J.L.; Lu, H.Q.; Song, X.S.; Li, J.F.; Ma, Y.H. *Opt. Commun.* **2005,** *249,* 493–499.
[10] Hwang, H.E.; Han, P.J. *Opt. Soc. Am. A* **2006,** *23,* 1870–1874.
[11] Chen, L.F.; Zhao, D.M. *Opt. Express* **2006,** *14,* 8552–8560.
[12] Singh, M.; Kumar, A.; Singh, K. *Opt. Lasers Eng.* **2008,** *46,* 763–768.
[13] Liu, Z.J.; Chen, H.; Liu, T.; Li, P.F.; Dai, J.M.; Sun, X.G.; Liu, S.T. *J. Opt. (Bristol, U.K.)* **2010**, *12*, 035407.
[14] Nishchal, N.K.; Naughton, T.J. *Opt. Commun.* **2011,** *284,* 735–739.
[15] Qin, W.; Peng, X. *Opt. Lett.* **2010,** *35,* 118–120.
[16] Singh, N.; Sinha, A. *Opt. Lasers Eng.* **2009,** *47,* 539–546.
[17] Zhou, N.R.; Wang, Y.X.; Gong, L.H. *Opt. Commun.* **2011,** *284,* 3234–3242.
[18] Zhou, N.R.; Wang, Y.X.; Gong, L.H.; Chen, X.B.; Yang, Y.X. *Opt. Laser Technol.* **2012,** *44,* 2270–2281.
[19] Zhou, N.R.; Wang, Y.X.; Wu, J.H. *Opt. Commun.* **2011,** *284,* 5588–5597.
[20] Wu, J.H.; Zhang, L.; Zhou, N.R. *Opt. Commun.* **2010,** *283,* 1720–1725.
[21] Tao, R.; Xin, Y.; Wang, Y. *Opt. Express* **2007,** *15,* 16067–16079.
[22] Takeda, M.; Nakano, K.; Suzuki, H.; Yamaguchi, M. *J. Opt. (Bristol, U.K.)* **2012**, *14*, 094003.
[23] Chen, W.; Chen, X.D.; Sheppard, C.J.R. *J. Opt. (Bristol, U.K.)* **2012**, *14*, 075402.
[24] Sui, L.S.; Gao, B. *Opt. Laser Technol.* **2013,** *48,* 117–127.
[25] He, W.Q.; Peng, X.; Meng, X.F. *J. Opt. (Bristol, U.K.)* **2012**, *14*, 075401.
[26] Situ, G.H.; Zhang, J.J. *Opt. Lett.* **2005,** *30,* 1306–1308.
[27] Situ, G.H.; Zhang, J.J. *J. Opt. A: Pure Appl. Opt.* **2006,** *8,* 391–397.
[28] He, M.Z.; Cai, L.Z.; Liu, Q.; Wang, X.C.; Meng, X.F. *Opt. Commun.* **2005,** *247,* 29–37.
[29] Xiao, Y.L.; Su, X.Y.; Li, S.K.; Liu, X.Q.; Zeng, S.G. *Opt. Laser Technol.* **2011,** *43,* 889–894.
[30] Liu, Z.J.; Zhang, Y.; Zhao, H.F.; Ahmad, M.A.; Liu, S.T. *Optik (Munich, Ger.)* **2011**, *122*, 1010–1013.
[31] Deng, X.P.; Zhao, D.M. *Opt. Laser Technol.* **2012,** *44,* 374–377.
[32] Sahin, A.; Ozaktas, H.M.; Mendlovic, D. *Opt. Commun.* **1995,** *120,* 134–138.
[33] Garcia, J.; Mas, D.; Dorsch, R.G. *Appl. Opt.* **1996,** *35,* 7013–7018.
[34] Li, Y.J.; Zhang, K. *Vision Bionics Image Guidance Technique and Application*; National Defense Industry Press: Beijing, 2006.