High Security Multiple-image Encryption using Discrete Cosine Transform and Discrete Multiple-Parameter Fractional Fourier Transform

Guanghui Ren[1], Jianan Han[1], Haihui Zhu[1], Jiahui Fu[1], and Mingguang Shan[2]
[1] School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, 150001, P.R. China
[2] College of Information and Communication Engineering, Harbin Engineering University, Harbin, 150001, P.R. China
Email: {rgh, hanjianan, fjh}@hit.edu.cn; hit_zhuhaihui@163.com; smgsir@gmail.com

Abstract —A multiple-image encryption scheme is proposed by using discrete cosine transform and discrete multiple-parameter fractional Fourier transform (DMPFRFT). Each image is performed by discrete cosine transform and filtering procedure and then multiplexed into a complex signal. After operated by a pixel scrambling, the complex signal is multiplied by random phase mask, and then encrypted into one image in DMPFRFT domain. The original images can be retrieved by using such correct keys as pixel scrambling operation, random phase mask and the parameters of DMPFRFT. Numerical simulations have been done to verify the feasibility and security of the proposed method

Index Terms—Image encryption, Discrete cosine transform, Discrete multiple-parameter fractional Fourier transform

I. INTRODUCTION

Recently, a large body of work has been reported on image encryption, but most of them are dealing with one or two images [1]-[9]. There is some trouble in decryption and transmission for highly correlated and large volume data and images, which are encrypted and transmitted, separately. To solve this problem, more and more efforts have been focused on multiple image encryption which has a high application value in multiuser authentication and content distribution and in improving the efficiency of secret information transmission [10]-[13]. A multiple image encryption scheme in a prior work with wavelength multiplexing and position multiplexing was proposed by Situ and Zhang [11]-[12], however, the qualities of decrypted images are not perfect due to the cross-talk effects between images. To avoid the cross-talk encountered with the Fourier Transform (FT), A. Alfalou *et al*. have investigated compression and encryption simultaneously [13], which is shown to be applicable to multiples images. They relied on image fusion in the spectral domain and usage of the Discrete Cosine Transform (DCT) instead of the Fourier transform. As we all know, complex operations are more complex than real operations, but most of general problems can be solved within the scope of real numbers. Therefore, in many cases, discrete cosine transform can replace discrete Fourier transform to solve the same problem, which just performed by real operation to improve the efficiency. The last level of their encryption algorithm is based on double random phase encryption (DRP) using the Fourier transform. However, it is well established that the standard double random phase encryption (DRP) has a low key space and exhibits vulnerability to various attacks. Then as a generalization of the traditional Fourier transform, the fractional Fourier transform (FRFT) has attracted more attention [2]-[5], [10]. In the past decades, the FRFT has been extended to Discrete Multiple-Parameter Fractional Fourier Transform (DMPFRFT). The DMPFRFT gives us more choices to represent signals in the fractional Fourier domain with extra freedom provided by vector parameters, and shows improved performance and security in image encryption. So it has been widely applied in image encryption [6]-[9]. In this paper, we propose a novel multiple-image encryption scheme based on DCT and DMPFRFT, which can convert multiple images into one encrypted image. The results of simulations, statistical analysis and key sensitivity tests show that the proposed image encryption scheme is an efficient and secure way for multiple image encryption.

The remaining sections of this paper are organized as follows: Section II introduces the proposed multiple-image encryption method, Section III presents the numerical simulation results to demonstrate the performance of the method, and Section IV states the conclusions.

II. PRINCIPLE

A. DMPFRFT

The DMPFRFT is a generalization of the FRFT, which has a transform kernel with multiple-parameter, so it can give us more choices to represent signals with extra degrees of freedom. The DMPFRFT with order (α_L, α_R), periodicity (M_L, M_R) and vector parameter ($\mathbf{m}_L$,$\mathbf{n}_L$; $\mathbf{m}_R$,$\mathbf{n}_R$) for a 2D signal $\mathbf{X}=(x_{n,m})_{NL\times NR}$ is straightforward as two 1D DMPFRFT in the row and column, respectively, and can be defined as

Manuscript received October 30, 2015; revised May 10, 2016
Corresponding author email: hanjianan@hit.edu.cn.
doi:10.12720/jcm.11.5.491-497

$$\mathbf{X}_{(M_L,M_R)}^{(\alpha_L,\alpha_R)}\left(\mathbf{m}_L,\mathbf{n}_L;\mathbf{m}_R,\mathbf{n}_R\right)=F_{(M_L,M_R)}^{(\alpha_L,\alpha_R)}\left(\mathbf{n}_L^{'},\mathbf{n}_R^{'}\right)\mathbf{X}=F_{(M_L)}^{(\alpha_L)}\left(\mathbf{n}_L^{'}\right)\cdot\mathbf{X}\cdot F_{(M_R)}^{(\alpha_R)}\left(\mathbf{n}_R^{'}\right) \tag{1}$$

where **n**' is

$$u_k=\left(km_k+Mm_kn_k+n_k\right)\qquad k=0,1,2,\cdots,(M-1)$$

The decomposition structure of DMPFRFT is given by:

$$F_M^{\alpha}\left(\mathbf{n}^{'}\right)=VD^{\alpha}V^T=\begin{cases}\sum_{k=0}^{N-1}\exp\left\{(-2\pi i/M)\left[\alpha\left(\bmod(k,M)+n_{\bmod(k,M)}^{'}M\right)\right]\right\}v_kv_k^T & \text{for } N \text{ odd}\\ \sum_{k=0}^{N-2}\exp\left\{(-2\pi i/M)\left[\alpha\left(\bmod(k,M)+n_{\bmod(k,M)}^{'}M\right)\right]\right\}v_kv_k^T & \\ \quad+\exp\left\{(-2\pi i/M)\left[\alpha\left(\bmod(N,M)+n_{\bmod(N,M)}^{'}M\right)\right]\right\}v_{N-1}v_{N-1}^T & \text{for } N \text{ even}\end{cases}$$

where T is the matrix transpose, **V** is a matrix with the eigenvectors as column vectors, i.e. $\mathbf{V}=[\mathbf{v}_0|\mathbf{v}_1|\ldots|\mathbf{v}_{N-2}|\mathbf{v}_{N-1}]$ for N odd and $\mathbf{V}=[\mathbf{v}_0|\mathbf{v}_1|\ldots|\mathbf{v}_{N-2}|\mathbf{v}_N]$ for N even, **D** is a diagonal matrix with its diagonal entries corresponding to the eigenvalues for each column eigenvectors $\mathbf{v}_k$ in **V** [14]-[18].

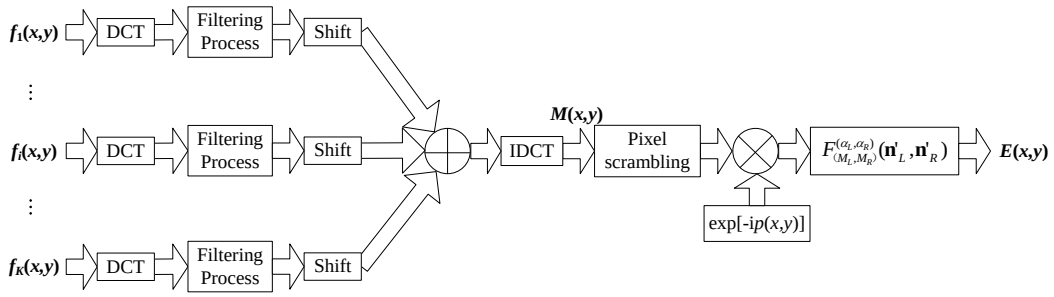


Fig. 1. Schematic of encryption

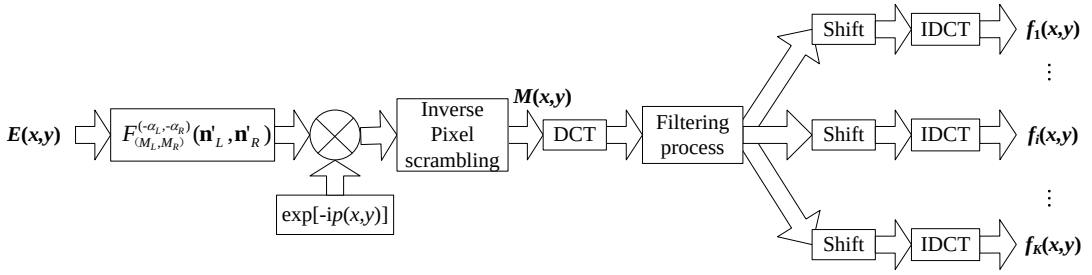


Fig. 2. Schematic of decryption

B. Multiple-Image Encryption Algorithm

The proposed encryption process is shown in Fig. 1. We consider K target images of size (N,N) pixels, and let $f_i(x,y)$ represent the ith target image. Firstly, we apply Discrete Cosine Transform (DCT) separately to every of these images. Secondly, every spectrum is multiplied by a low-pass filter, of size set to (N',N') pixels, positioned in its upper left corner. In this way, a block containing the relevant information for reconstructing every target image is obtained. We denote the proposed filtering method by **F**(•). The compression rate T_c_pixel (expressed in pixels) is evaluated as follows [13]

$$\begin{aligned}T_c\_\text{pixel}&=1-\frac{\text{size of multiplexed DCT spectral plane}}{\text{size of K input images}}\\&=1-\frac{N^2}{K\times N^2}=1-\frac{1}{K}\end{aligned} \tag{2}$$

Then the inverse Discrete Cosine Transform (IDCT) is used after all of these blocks are grouped together [13]. To avoid information overlap these blocks are shifted. It should be noted that the capability of multiplexing can be increased by appropriately selecting the filter size. The smaller the filter size is, the more images can be multiplexed, but the qualities of recovered images may be worse. Once this procedure is accomplished, a synthesized signal $M(x,y)$ can be obtained, which can be expressed as

$$M(x,y)=\text{IDCT}\left[\sum_{i=1}^{K}\text{F}\left[\text{DCT}\left[f_i(x,y)\right]\right]\right] \tag{3}$$

For encryption, the pixel scrambling operation [2], [19] **J**[·] is first done on the synthesized signal $M(x,y)$, and the scrambled result $\mathbf{J}[M(x,y)]$ is then multiplied by RPM function $\exp[ip(x_a)]$, where $p(x_a)$ is statistically white sequence uniformly distributed in $[0,2\pi]$. By using a

further DMPFRFT operation with parameters of (M_L,M_R; α_L, α_R; $\mathbf{m}_L$,$\mathbf{n}_{L;}$ $\mathbf{m}_R$,$\mathbf{n}_R$), the final distribution $E(x,y)$ of the output encrypted image, which also has a stationary white distribution in the output domain, can be obtained in (4).

The proposed decryption process is shown in Fig. 2 which is the reverse process of the encryption. It consists of decrypting and demultiplexing steps. For decrypting step, $E(x,y)$ is applied by the inverse of 2D DMPFRFT, the conjugate of RPM, and the inverse pixel scrambling $\mathbf{J}^{-1}[\cdot]$ to obtain the decrypted complex signal $M(x,y)$, as given in (5),

$$\begin{aligned} E(x,y) &= F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(\mathbf{n}_L',\mathbf{n}_R')\left\{\mathrm{J}\left[M(x,y)\right]\exp\left[ip(x,y)\right]\right\} \\ &= F^{(\alpha_L,\alpha_R)}_{(M_L,M_R)}(x,y)\left\{\mathrm{J}\left[\mathrm{IDCT}\left[\sum_{i=1}^{K}\mathrm{F}\left[\mathrm{DCT}\left[f_i(x,y)\right]\right]\right]\right]\exp\left[ip(x,y)\right]\right\} \end{aligned} \tag{4}$$

$$M(x,y) = \mathrm{J}^{-1}\left\{F^{(-\alpha_L,-\alpha_R)}_{(M_L,M_R)}\left[E(x,y)\right]\exp\left[-ip(x,y)\right]\right\} \tag{5}$$

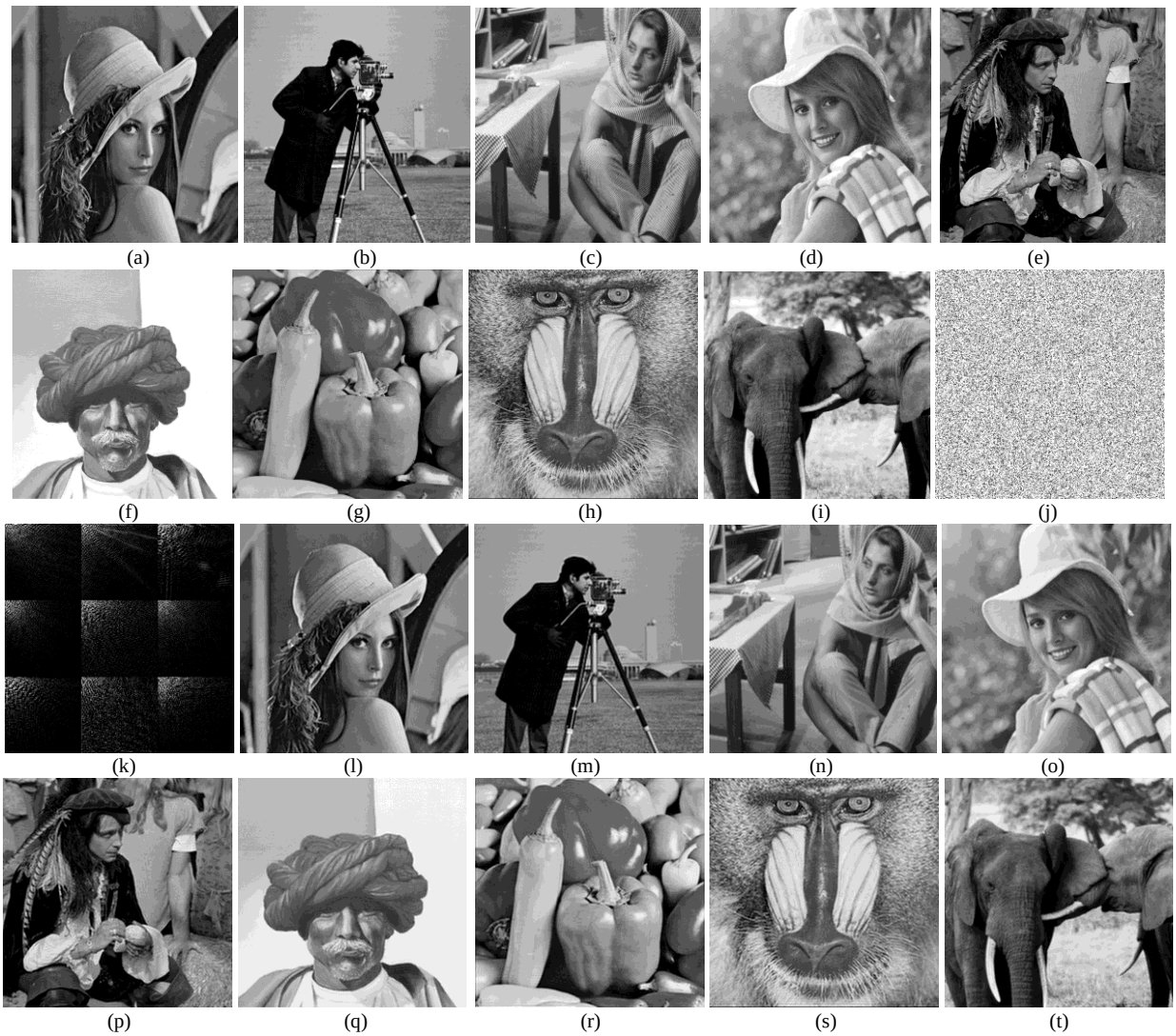


Fig. 3. (a-i) Target images, (j) encrypted image, (k)the spectrum of decrypted complex signal, (l-t) decrypted images.

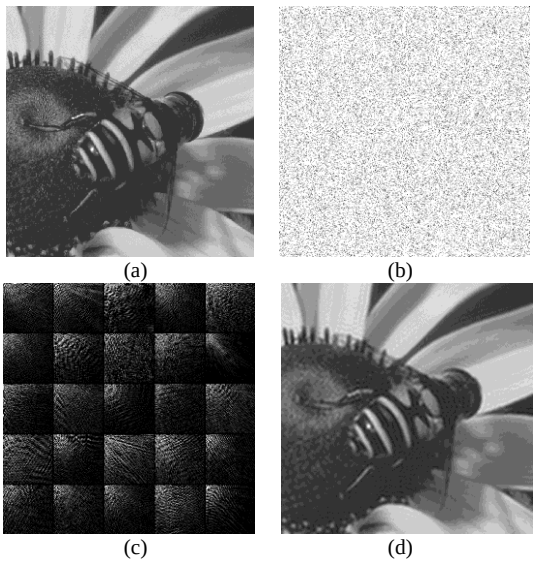
For demultiplexing step, we can see all blocks belonged to every images in the spectral plane by utilizing Discrete Cosine Transform (DCT) to $M(x,y)$. Every image can be obtained by taking the inverse Discrete Cosine Transform (IDCT) after properly filtering out and shifting every block.

It can be seen from the presents above that to retrieve the images, both the pixel scrambling operation, RPM and the parameters of DMPFRFT such as the periodicities (M_L,M_R), transform orders (α_L,α_R) and vector parameters ($\mathbf{m}_L$,$\mathbf{n}_{L;}$ $\mathbf{m}_R$,$\mathbf{n}_R$) are required. They serve as the keys of this algorithm, and play important roles in the encryption process.

III. Simulation Results and Performance Analysis

Numerical simulation experiments have been carried out to verify the proposed encryption method using

Matlab R2012a on a PC with dual-core CPU of 2.6GHz and memory of 2GB. In our experiment, we first take 9 images with 512×512 pixels and 256 gray levels as the target images to be encrypted, as shown in Fig. 3(a-i), respectively. T_c_pixel is 0.89. The size of low-pass filter is (170,170) pixels. Pixel scrambling operation breaks the image up into 65,536 subsections of 2×2 pixels. The random phase mask is generated by random function on Matlab platform. The system parameters are (M_L, M_R; α_L, α_R)=(15,20;0.34,0.73). The vector parameters ($\mathbf{m}_L$,$\mathbf{n}_L$) and ($\mathbf{m}_R$,$\mathbf{n}_R$) are 1×15 and 1×20 random vectors whose values are independent integer values, respectively. Fig. 3(j) is the encrypted image with stationary white noise. After the correct keys are utilized to decrypt, the resulting function is then transformed by the Discrete Cosine Transform to obtain the spectrum of the decrypted complex signal which is shown as Fig. 3(k). We can see that there are 9 blocks belonged to every image respectively. By properly designing the filters, the image can be then reproduced as shown in Fig. 3(*l*-*t*). The computational time for the whole scheme to encrypt and decrypt the 9 images is about 11.66s. It can be seen that the decrypted images are the same as the original images. It can be also noted that there is no cross-talk between the 9 decrypted images.

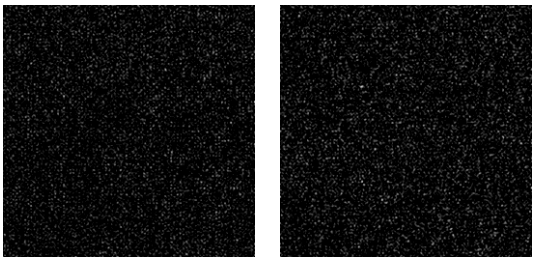


(a) (b) (c) (d)

Fig. 4.(a) Target images (Media 1), (b) encrypted image, (c)the spectrum of decrypted complex signal, (d) decrypted images (Media 2).

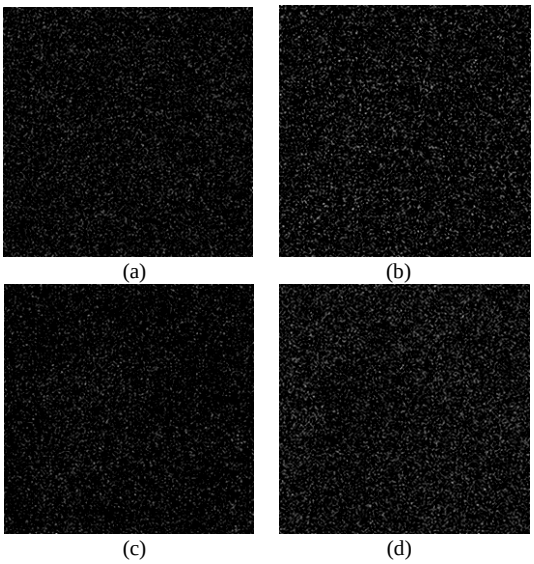
We also take 25 images with 512×512 pixels and 256 gray levels as the target images, for convenience, we put those images into a movie as shown in Fig. 4(a) (Media 1). T_c_pixel is 0.96. The size of low-pass filter is (100,100) pixels. The pixel scrambling operation, RPM and the parameters of DMPFRFT is same as the former experiment. Then the encrypted image with stationary white noise can be obtained as shown Fig. 4(b). After applying correct key to the encrypted image and transforming DCT, the spectrum of the decrypted complex signal can be obtained as shown in Fig. 4(c). It can be seen that there are 25 blocks belonged to every image respectively. By properly designing the filters, the images can be then reproduced as shown in Fig. 4(d) (Media 2). We can see that although the decrypted images have lost some higher frequency detail, they can be recognized easily. The computational time for the whole scheme to encrypt and decrypt the 25 images is about 18.41s. It should be noted the computational time increases as the number of images increase. Our future work is to further reduce the computational time, and improve the quality and quantity of the encrypted images.

In the following analysis, the influence of the deviation of difference keys on the decrypted images is considered. We take 9 images for experiment, they also be put into a movie. Fig. 5(a) (Media 3) shows the decrypted images obtained by wrong RPM. Fig. 5(b) (Media 4) shows the decrypted images obtained without correct inverse pixel scrambling operation. Fig. 6 show the decrypted images obtained by wrong parameters of DMPFRFT. It can be seen from Fig. 5 and Fig. 6 that when the RPM, inverse pixel scrambling operation and/or DMPFRFT parameters are not correct, the images can hardly be recognized in vision even the other keys are correct. This would lead to a high security hierarchy in applications.



(a) (b)

Fig. 5. (a) Decrypted images with wrong RPM (Media 3), (b) decrypted images without correct inverse pixel scrambling operation (Media 4).



(a) (b) (c) (d)

Fig. 6 Decrypted images with different incorrect keys: (a) {(14,19); (-0.34,-0.73); ($\mathbf{m}_L$,$\mathbf{n}_L$); ($\mathbf{m}_R$,$\mathbf{n}_R$)} (Media 5), (b){(15,20); (-0.34+10^{-7},-0.73+10^{-7}); ($\mathbf{m}_L$,$\mathbf{n}_L$); ($\mathbf{m}_R$,$\mathbf{n}_R$)} (Media 6), (c){(15,20); (-0.34,-0.73); ($\mathbf{m}_L$+2,$\mathbf{n}_L$+1); ($\mathbf{m}_R$,$\mathbf{n}_R$)} (Media 7), (d) { (15,20); (-0.34,-0.73); ($\mathbf{m}_L$,$\mathbf{n}_L$); ($\mathbf{m}_R$+1,$\mathbf{n}_R$+1)} (Media 8).

In order to further quantitatively evaluate the performance of this method, the normalized mean square

error (NMSE) between the original image and the decrypted image is defined as

$$\mathrm{NMSE} = \sum_{j=1}^{N}\sum_{i=1}^{M}\left[I_D(i,j) - I_E(i,j)\right]^2 \Big/ \sum_{j=1}^{N}\sum_{i=1}^{M}\left[I_E(i,j)\right]^2 \quad (6)$$

where $M \times N$ are the size of the image, $I_D(i,j)$ and $I_E(i,j)$ are the values of the decrypted image and the original image at the pixel (i,j), respectively.

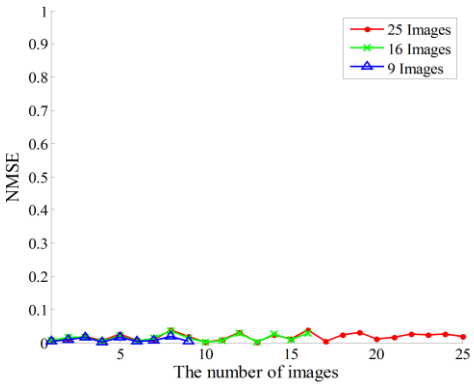
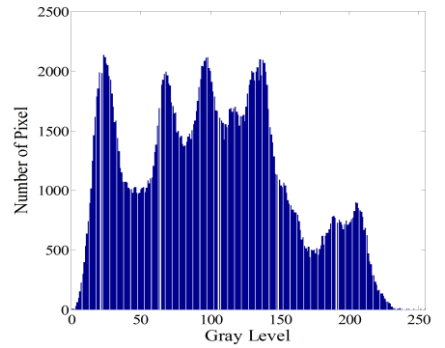
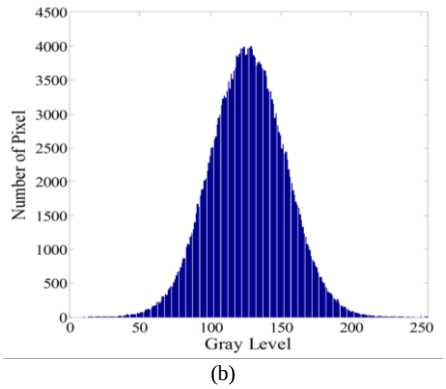


Fig. 7. Normalized mean square error (NMSE) for all images.

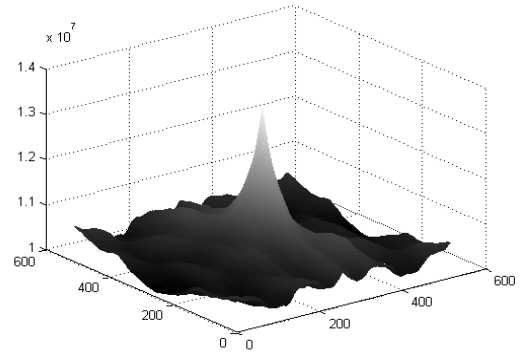
The NMSE curves of different decrypted image with total number of 9, 16 and 25 are shown in Fig.7. It can be seen from Fig. 7 that this method has a uniform quality for every image, and NMSE is inversely proportional to the number of images. We also calculated the NMSE between the synthesized signal $M(x,y)$ and decrypted complex signal, the value is 4.5799e-30+3.8690e-31i. We can know that the pixel scrambling and DMPFRFT operation almost have no distortion, our future work is improving the performance of the multiplexing and the demultiplexing steps.



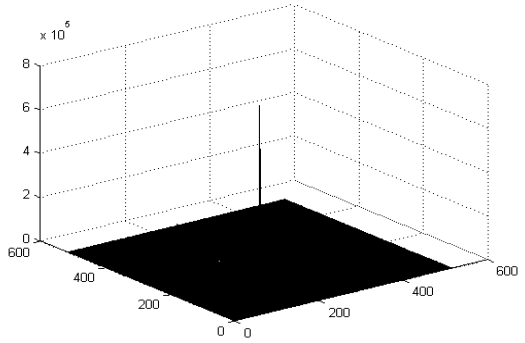
(a)



(b)



(c)



(d)

Fig. 8. (a) Histogram of the first image; (b) histogram of encrypted image; (c) self-correlation of the first image; (d) self-correlation of encrypted image.

Image histograms and self-correlation performances are tested to show the statistical properties of the encryption algorithm. Fig. 8 (a) and (b) are the image histograms of the first image and the encrypted image, respectively. There are significant differences between (b) and (a), so useful information cannot be obtained by attackers according to the statistical properties. Fig. 8(c) and (d) are the self-correlation images of the first image and the encrypted image, respectively. It can be seen that the correlation of the encrypted image is much weaker than that of the first image. It further proves that the algorithm has a strong capability of decorrelation to resist attacks from statistical analysis.

The robustness of this method is also tested against occlusion. Fig. 9 (b) shows the corresponding retrieved images with all the correct keys from Fig. 9(a) of encrypted image cut by 25%. It can be seen that the retrieved images can be recognized with no doubt, and it proves this method has certain robustness against attacks.

There exist four potential types of attacks: cipher only attack, known plaintext attack, chosen plaintext attack and chosen ciphertext attack. Generally speaking, chosen plaintext attack is the most powerful attack. If a algorithm can resist this attack, it can resist other types of attack [20]-[21]. The chosen plaintext attack is assumed that the attackers have the ability to trick a legitimate user of the system into encrypting particular images [20]. But no matter which particular image may be choose, the pixel scrambling operation could transform it to another randomly [19]. Therefore the proposed image encryption scheme can resist these classical types of attacks.

(a) (b)

Fig. 9 Robustness against occlusion: (a) encrypted image with 25% occlusion; (b) the decrypted images from (a) (Media 9).

IV. Conclusion

In this paper, a novel algorithm based on the discrete cosine transform and the discrete multiple-parameter fractional Fourier transform is proposed to encrypt multiple images into one image with stationary white distribution. The original image is performed by discrete cosine transform and filtering procedure, respectively, and then multiplexed into a synthesized image. After being scrambled and multiplied by RPM, the image is encrypted into random white noise by utilizing DMPFRFT. This method enhances the key space of the system, improves spectrum efficiency, and further provides a much higher security level. And we only need one image to decrypt multiple images, the transmission could be easier, the efficiency could be raised greatly. Numerical simulation results indicate that the algorithm is sensitive to the keys, could resist attacks from statistical analysis, occlusion, chosen plaintext and known plaintext, and provide considerable robustness to blind decryption, which further prove the validity of the method. It's no doubt that for a novel method, there are still much work required to do, such as computation time which is important for visualizing the coding performance, color images and/or general images encryption. This will be our next work.

References

[1] Z. J. Liu, S. Li, W. Liu, Y. H. Wang, and S. T. Liu, "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 51, pp. 8-14, Jan. 2013.

[2] Z. Zhong, J. Chang, M. G. Shan, and B. G. Hao, "Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption," *Optics Communications*, vol. 285, pp. 18-23, Jan. 2012.

[3] Z. Zhong, J. Chang, M. G. Shan, and B. G. Hao, "Double image encryption using double pixel scrambling and random phase encoding," *Optics Communications*, vol. 285, pp. 584-8, Mar. 2012.

[4] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express*, vol. 15, pp. 16067-16079, Nov. 2007.

[5] Z. J. Liu and S. T. Liu, "Double image encryption based on iterative fractional Fourier transform," *Optics Communications*, vol. 275, pp. 324-329, July 2007.

[6] M. G. Shan, J. Chang, Z. Zhong, and B. G. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," *Optics Communications*, vol. 285, pp. 4227-4234, Oct. 2012.

[7] R. Tao, J. Lang, and Y. Wang, "Optical image encryption based on the multiple-parameter fractional Fourier transform," *Optics Letters*, vol. 33, pp. 581-583, Mar. 2008.

[8] J. Lang, R. Tao, and Y. Wang, "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function," *Optics Communications*, vol. 283, pp. 2092-2096, May 2010.

[9] B. H. Zhu, S. T. Liu, and Q. W. Ran, "Optical image encryption based on multifractional Fourier transforms," *Optics Letters*, vol. 25, pp. 1159-1161, Aug. 2000.

[10] Z. J. Liu, J. M. Dai, X. G. Sun, and S. T. Liu, "Triple image encryption scheme in fractional Fourier transform domains," *Optics Communications*, vol. 282, pp. 518-522, Feb. 2009.

[11] G. Situ and J. J. Zhang, "Position multiplexing for multiple-image encryption," *Journal of Optics A-Pure and Applied Optics*, vol. 8, pp. 391-397, May 2006.

[12] G. H. Situ and J. J. Zhang, "Multiple-Image encryption by wavelength multiplexing," *Optics Letters*, vol. 30, pp. 1306-1308, June 2005.

[13] A. Alfalou, C. Bresseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," *Optics Express*, vol. 21, pp. 8025-8043, Apr. 2013.

[14] D. Z. Kon, X. J. Shen, Q. Z. Xu, W. Xin, and H. Q. Guo, "Multiple-Image encryption scheme based on cascaded fractional Fourier transform," *Applied Optics*, vol. 52, pp. 2619-2625, Apr. 2013.

[15] S. C. Pei, M. H. Yeh, and C. C. Tseng, "Discrete fractional fourier transform based on orthogonal projections," *IEEE Transactions on Signal Processing*, vol. 47, no. 5, pp. 1335-1348, May 1999.

[16] Z. J. Liu, H. F. Zhao, and S. T. Liu, "A discrete fractional random transform," *Optics Communications*, vol. 255, pp. 357-365, Nov. 2005.

[17] G. Cariolaro, T. Erseghe, P. Kranianskas, and N. Laurrent, "Multiplicity of fractional Fourier transforms and their relationships," *IEEE Transactions on Signal Processing*, vol. 48, pp. 227-241, Jan. 2000.

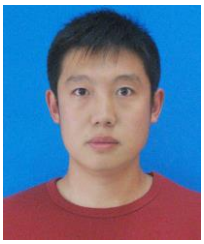
[18] J. Lang, R. Tao, Q. W. Ran, and Y. Wang, "The multiple-parameter fractional Fourier transform," *Science in China Series F-information Sciences*, vol. 51, pp. 1010-1024, Aug. 2008.

[19] J. L. Zhao, H. Q. Lu, X. S. Song, J. F. Liu, and Y. H. Ma, "Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique," *Optics Communications*, vol. 249, pp. 493-499, May 2005.

[20] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption

against various attacks," *Optics Express*, vol. 15, pp. 10253-10265, Aug. 2007.
[21] H. Liu and H. Nan, "Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform," *Optics and Laser Technology*, vol. 50, pp. 1-7, Sep. 2013.

Guanghui Ren is a professor in the School of Electronics and Information Engineering at Harbin Institute of Technology (HIT). He received the B.S. degree in electronic instrument and measurement technology in 1984 and M.E. degree in signal and information processing in 2003 from HIT. His research interests include wireless communication, interference alignment, image processing, automatic test systems, and parallel computing.



Jianan Han received the B.S. degree in computer science in 2006 from HIT. He received the M.E. degree in signal and information processing in 2011 from HIT. He is currently working toward the Ph.D. degree in information and communication at HIT. His research interests include digital image processing and wireless communication.

Haihui Zhu was born in Jiangxi, China in 1993. He received the B.Sc. (in 2015) degree in Electronics and Information Engineering from the School of Electrical and Information Engineering at Harbin Institute of Technology (HIT), China. He is a postgraduate student in School of Information and Communication Engineering at Harbin Institute of Technology. His research interests is image processing and signal processing.

Jiahui Fu is an associate professor in the School of Electronics and Information Engineering at HIT. He received the B.S. degree in electronic and information technology in 1995, M.E. degree in microwave technology in 2003, and Ph.D. degree in electronics science and technology in 2005 from HIT. His research interests include wireless communication, image processing, microwave circuit, and electromagnetic compatibility

Mingguang Shan is a associate professor in College of Information and Communication. Engineering, Harbin Engineering University. He obtained his BS, MS, and PHD degrees in 2002, 2005, and 2008, respectively, in instrumentation science and technology from the Department of Automatic Measurement and Control Engineering of Harbin Institute of Technology, China. His current research interest focuses on interferometry, digital holography, fiber sensor and image processing.