Optica Applicata, Vol. XLVII, No. 1, 2017
DOI: 10.5277/oa170112

A known-plaintext attack on iterative random phase encoding in fractional Fourier domains

FUCHENG YIN[1], QI HE[2], ZHENGJUN LIU[2*]

[1]Data Recovery Key Laboratory of Sichuan Province, Neijiang Normal University, Neijiang 641100, Sichuan, P.R. China

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

[*]Corresponding author: zjliuv@gmail.com, zjliu@hit.edu.cn

Known-plaintext attack is considered for decrypting the image generated by iterative random phase encoding in fractional Fourier transform domains. The double random phase encoding in Fourier domains is introduced to design the known-plaintext attack procedure. The decryption test is explored without both fractional order and these random phase masks. Some numerical simulations are made to demonstrate the validity of the known-plaintext attack.

Keywords: image encryption, phase encoding, known-plaintext attack.

1. Introduction

Optical image encryption (or hiding) technology has been considered for protecting 2-D information in transmission after the double random phase encoding (DRPE) [1] in Fourier domains was reported. The DRPE has been expanded into other transformation domains [2, 3] and employed for encrypting one or more original images [4, 5]. The interference method has been introduced into the research on the image encryption algorithms [6, 7]. Some encryption schemes have been reported by use of Hartley transform, random transforms and commutation rules [8–13]. The pixel scrambling operation has been considered for constructing the encryption algorithms [14–18] as well. Multiple-encryption is a new information hiding format. Two kinds of multiple-image encryption methods have been proposed by using wavelength multiplexing [19] and position multiplexing [20]. As a kind of special case of multiple-encryption, several double-image encryption algorithms have been represented by combining amplitude encoding and phase encoding [21–26]. Moreover, color image encryption algorithm can be used for hiding three original gray-level images [27–32] as a potential method.

In recent years, the security of image encryption algorithm has become a concern for various potential attacks. The key-space of DRPE technique has been evaluated and analyzed in [33]. The collision phenomenon in DRPE has been presented and eval-

uated for the validity of key in the applications of watermarking and authentication [34]. Several attacks on DRPE [35, 36], such as known-plaintext attack (KPA) and brute force attacks, have been researched.

The KPA on DRPE in fractional Fourier domains has been reported in [37], in which the decryption can be achieved by an incorrect fractional order. Moreover, the two kinds of KPA [35, 36] are formed by referring the encryption process. In this article, the KPA on iterative random phase encoding in fractional Fourier transform (FrFT) domains is researched. The model of the KPA is designed by the DRPE in Fourier domains without the fractional order and the random phase masks are used in iterative random phase encoding. The Gerchberg–Saxton phase retrieval algorithm [38] is employed for retrieving unknown phase masks in the KPA. Some numerical simulations are conducted to demonstrate the performance of the attack.

The rest of this paper is organized in the following sequence. In Section 2, the scheme of KPA on iterative random phase encoding is introduced in detail. In Section 3, numerical simulation is achieved to test the validity of the attack scheme. Concluding remarks are summarized in the final section.

2. Known-plaintext attack scheme

Before the KPA is represented, we recall the iterative random phase encoding in FrFT domains briefly.

Figure 1 gives the flowchart of the iterative random phase encoding in fractional Fourier domains, which was reported in [39]. The encryption process can be expressed as

$$C_k = I_k \exp(iR_k) \tag{1a}$$

$$I_{k+1} = \mathcal{F}^{\alpha_{k+1}}[C_k] \tag{1b}$$

where $k = 0, 1, ..., N-1$, and the real function I_0 and complex function I_N represent the original image and final encrypted data, respectively. Multiple random phase masks

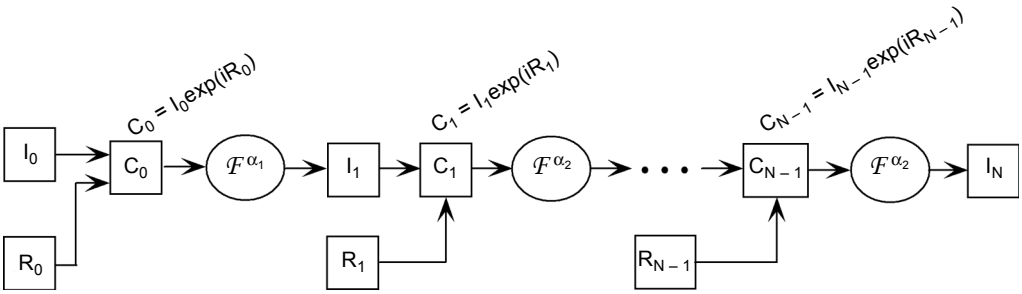

Fig. 1. The flowchart of iterative random phase encoding algorithm.

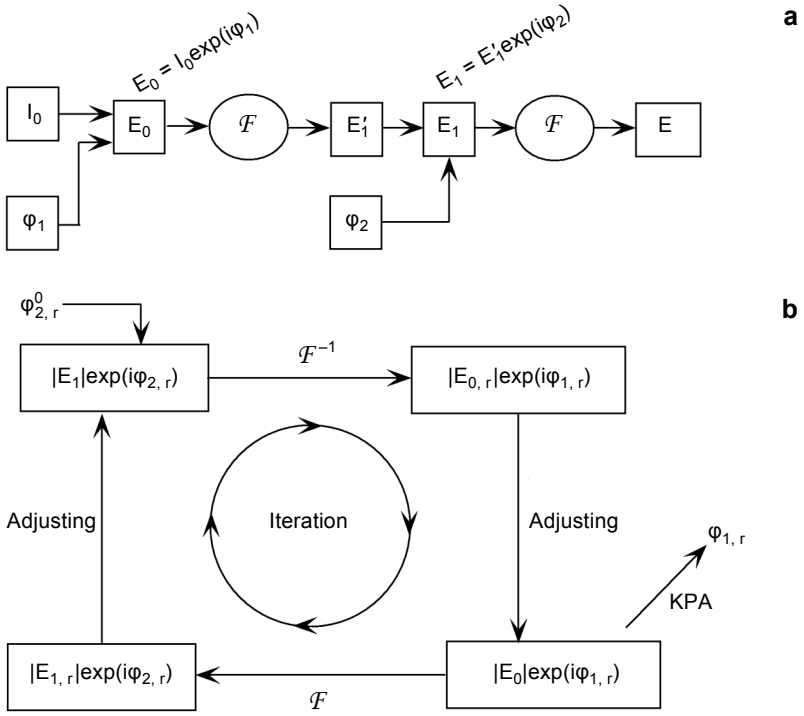

Fig. 2. DRPE in Fourier domain (**a**), and iterative Gerchberg–Saxton phase retrieval algorithm (**b**).

$(R_1, R_2, ..., R_{N-1})$ and fractional orders $(\alpha_1, \alpha_2, ..., \alpha_{N-1})$ are applied for enhancing the security of the encryption scheme. When total iteration number N is taken as 2, this encryption scheme reduces to the DRPE in FrFT domains [3].

The KPA will be constructed from a DRPE in Fourier domain. The original image I_0 is again encrypted according to the flowchart shown in Fig. 2**a**. The functions φ_1 and φ_2 are random phases. The symbol E denotes the obtained secret data. In this paper, we suppose that the two encrypted images are the same, namely $E = I_N$. The two random phase functions will be obtained by using the Gerchberg–Saxton phase retrieval algorithm with the secret data I_N, which is published or known before decrypting secret. The modulo of the complex function $|E_1|$ can be calculated as

$$|E_1| = |E_1'| = |\mathcal{F}^{-1}[E]| = |\mathcal{F}^{-1}[I_N]| \tag{2}$$

From the definition of the KPA [35, 37], the original image I_0 and the image I_N are known during searching the key used in image encryption. By using the two amplitude functions I_0 and $|E_1|$, the phase retrieval algorithm displayed in Fig. 2**b** can solve the random phase function $\varphi_{1,r}$, which is the recovered value of the phase φ_1. Here the function $\varphi_{2,r}^0$ is random and is regarded as the initial value of the phase $\varphi_{2,r}$. After the

phase $\varphi_{1,r}$ is obtained by iterative calculation, the recovered value of the second random phase $\varphi_{2,r}$ can be expressed as

$$\varphi_{2,r} = \arg\left\{\frac{\mathcal{F}[I_0 \exp(i\varphi_{1,r})]}{\mathcal{F}^{-1}[I_N]}\right\} \tag{3}$$

where the function "arg" is to compute the angle of a complex number. The secret image will be decrypted by use of the phase $\varphi_{2,r}$, which is represented as

$$I_{0,r} = \left|\mathcal{F}^{-1}\left\{\mathcal{F}^{-1}[I_N]\exp(i\varphi_{2,r})\right\}\right| \tag{4}$$

where the output $I_{0,r}$ is the recovered image by using KPA.

The fractional order in iterative algorithm [39] is an additional parameter for enhancing the security of information hiding technology. When the value of the order is changed, the algorithm will generate a different output pattern. In Fig. 3, a virtual re-

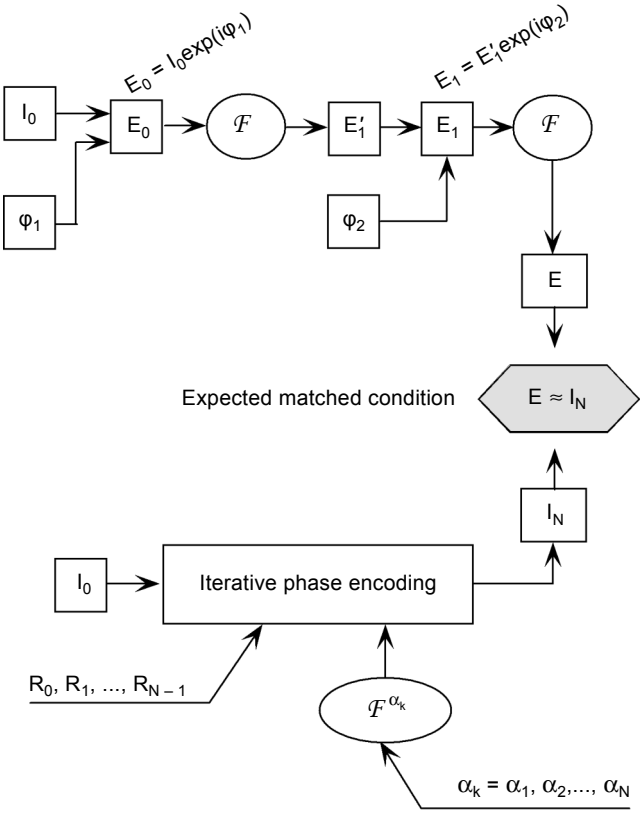

Fig. 3. The virtual relation between DRPE in Fourier domain and iterative phase encoding in FrFT.

lation between DRPE and iterative phase encoding is designed for obtaining an expected matched condition $E \approx I_N$. Therefore the KPA on DRPE in Fourier transform domains can be applied to decrypt iterative random phase encoding algorithm under the assumption in Fig. 3. The corresponding experimental result will be given in next section.

3. Numerical simulation

To test the effectiveness of the KPA on iterative random phase encoding, three groups of different encryption process are considered in this paper. The corresponding parameters employed in numerical simulation are written as follows:

$$g_1: \quad N = 2, \quad \alpha_1 = \alpha_2 = 0.7 \tag{5}$$

$$g_2: \quad N = 6, \quad \alpha_1 = \alpha_2 = ... = \alpha_6 = 0.8 \tag{6}$$

$$g_3: \quad N = 10, \quad \alpha_k = 0.2 + 0.7\sin(k\pi/20), \quad k = 1, 2, ..., 10 \tag{7}$$

In every unit of the iterative random phase encoding, the phase function R_k is fixed at different value. A gray-level image having 256 × 256 pixels is regarded as original secret image in the iterative random phase encoding and is shown in Fig. 4**a**. By using iterative random phase encoding procedure with the parameters defined in Eqs. (5)–(7), three encrypted images are computed and illustrated in Figs. 4**b**–4**d**, respectively. There they are random patterns and will be decrypted by KPA described in Section 2. The relative mean square error (RMSE) function is employed for weighting the difference of two images and are defined as

$$\mathrm{RMSE} = \mathrm{rmse}(I_\mathrm{s}, I_\mathrm{t}) = 10\log\left\{\frac{\sum_{\forall m,\, n}\left[I_\mathrm{s}(m, n) - I_\mathrm{t}(m, n)\right]^2}{\sum_{\forall m,\, n} I_\mathrm{s}^2(m, n)}\right\} \tag{8}$$

where I_s and I_t are the standard image and compared image, respectively. The RMSE value will be utilized for determining the quality of decrypted images.

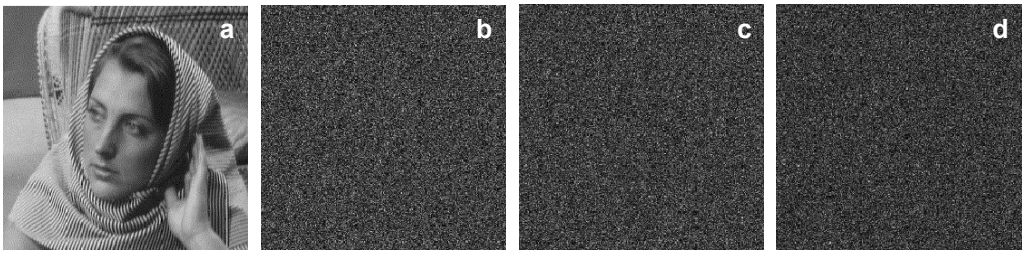

Fig. 4. An original image (**a**) and three encrypted images (**b**–**d**) calculated with Eqs. (5)–(7).

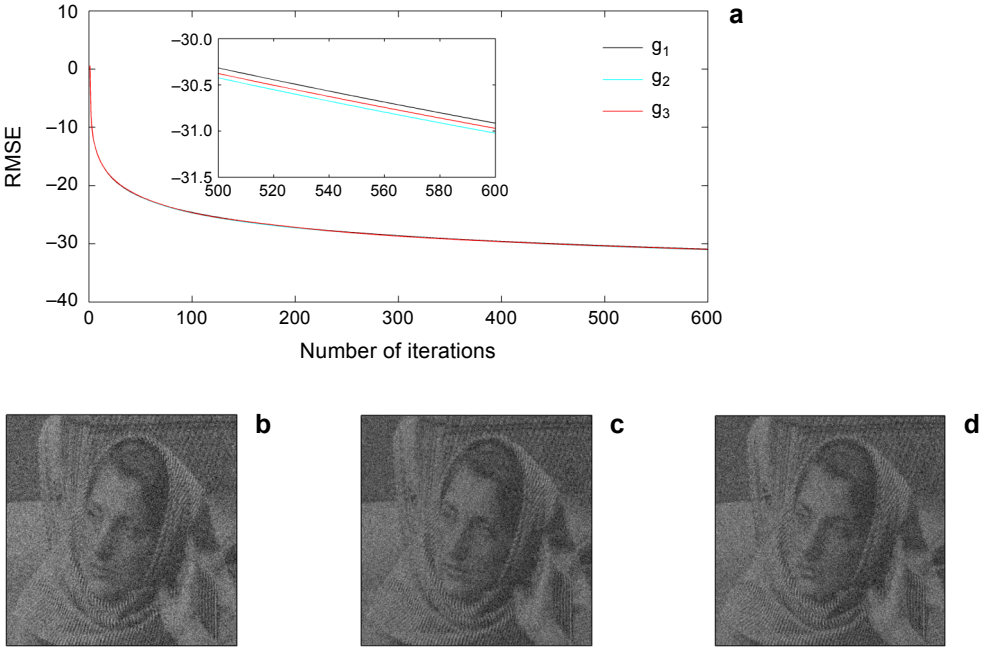

Fig. 5. Convergence of the phase retrieval algorithm (**a**) and the decrypted images (**b**–**d**) generated from the encrypted images in Figs. 4**b**–4**d**. The values of NMSE are equal to 8.10×10^{-4} (**b**), 7.90×10^{-4} (**c**) and 8.00×10^{-4} (**d**).

The decrypted results of the KPA are calculated and shown in Fig. 5. The convergence of the Gerchberg–Saxton phase retrieval algorithm is shown in Fig. 5**a**, where RMSE represents the error of the original image and recovered image quantitatively. After iterations the quality of retrieved image is almost stable. The three RMSE curves from the three tests have a similar trend. The decrypted images drawn in Figs. 5**b**–5**d** are obtained by the retrieved phase $\varphi_{2,r}$ to attack the encrypted images. The main outline of the original image can be recognized from these images. However the detail of secret image is polluted by random noise. The attack has no ideal output, which is close to original image, by using the Gerchberg–Saxton algorithm directly. The result has shown that the iterative random phase encoding is vulnerable under the decryption of KPA as well. Here an effective approximate phase encoding model of DRPE can be evaluated from the KPA.

For the group g_2, we change the value of order as $\alpha'_1 = \alpha'_2 = \ldots = \alpha'_6 = 0.6$ and $\alpha''_1 = \alpha''_2 = \ldots = \alpha''_6 = 0.7$. Here different values of order α_k are employed for testing the virtual relation in Fig. 3. The iterative phase retrieval calculation is performed 500 times. The retrieved phases and decrypted images are displayed in Fig. 6. From Figs. 5 and 6, different values of fractional orders α_k can be recovered by using KPA in Fourier transform domain. The obtained phases have obvious difference and are

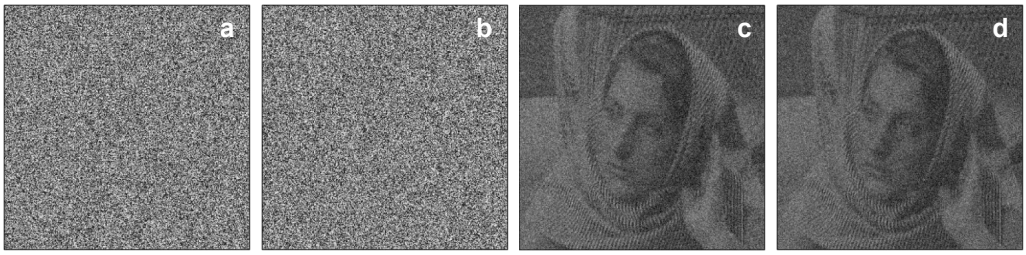

Fig. 6. The decryption result: retrieved phase φ_2 (**a**, **b**), recovered image with NMSE = 7.83×10^{-4} (**c**), and with NMSE = 7.73×10^{-4} (**d**). Here (**a**, **c**) are obtained, where all orders are 0.6 in iterative encoding and (**b**, **d**) are from the condition that all orders are 0.7.

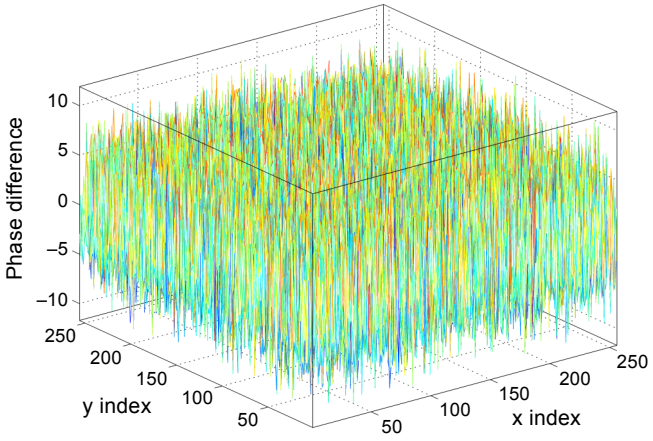

Fig. 7. The phase difference of two phase distributions in Figs. 5**a** and 5**b**.

shown in Fig. 7. The key phase φ_k will depend on the values of orders α_k. The quality of retrieved images in Figs. 5**b**–5**d** and 6**c**–6**d** have main information of original secret image.

4. Conclusion

To summarize, the paper has researched a KPA on iterative random phase encoding in fractional Fourier domains. The attacked object is the secret image obtained from iterative random phase encoding. A precondition designing the KPA is that two different encryption systems (DRPE and iterative random phase encoding) are equivalent to generate the same encrypted image. Thereby the KPA can be made from a DRPE in Fourier domains. The Gerchberg–Saxton phase retrieval algorithm is introduced for retrieving the two random phase functions in the DRPE. Some numerical simulations have demonstrated that this KPA can decrypt the images formed by iterative random

phase encoding. Furthermore the KPA defined in this paper can be considered for decrypting other optical encryption systems.

Acknowledgements – This work was supported by the National Natural Science Foundation of China (No. 61575053), the Program for New Century Excellent Talents in University (No. NCET-12-0148), the China Postdoctoral Science Foundation (Nos. 2013M540278 and 2015T80340), the Fundamental Research Funds for the Central Universities (No. HIT.BRETIII.201406), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry, China.

References

[1] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769.
[2] GUOHAI SITU, JINGJUAN ZHANG, *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586.
[3] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000, pp. 887–889.
[4] YUAN SHENG, ZHOU XIN, MOHAMMAD S.A., LU XI, LI XIAO-FENG, *Information hiding based on double random-phase encoding and public-key cryptography*, Optics Express **17**(5), 2009, pp. 3270–3284.
[5] ALFALOU A., MANSOUR A., *Double random phase encryption scheme to multiplex and simultaneous encode multiple images*, Applied Optics **48**(31), 2009, pp. 5933–5947.
[6] MENG X.F., CAI L.Z., XU X.F., YANG X.L., SHEN X.X., DONG G.Y., WANG Y.R., *Two-step phase -shifting interferometry and its application in image encryption*, Optics Letters **31**(10), 2006, pp. 1414–1416.
[7] YAN ZHANG, BO WANG, *Optical image encryption based on interference*, Optics Letters **33**(21), 2008, pp. 2443–2445.
[8] LINFEI CHEN, DAOMU ZHAO, *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006, pp. 3438–3440.
[9] ZHENGJUN LIU, HAIFA ZHAO, SHUTIAN LIU, *A discrete fractional random transform*, Optics Communications **255**(4–6), 2005, pp. 357–365.
[10] ZHENGJUN LIU, SHUTIAN LIU, *Randomization of the Fourier transform*, Optics Letters **32**(5), 2007, pp. 478–480.
[11] ZHENGJUN LIU, SHUTIAN LIU, *Random fractional Fourier transform*, Optics Letters **32**(15), 2007, pp. 2088–2090.
[12] HANG CHEN, XIAOPING DU, ZHENGJUN LIU, CHENGWEI YANG, *Color image encryption based on the affine transform and gyrator transform*, Optics and Lasers in Engineering **51**(6), 2013, pp. 768–775.
[13] ZHENGJUN LIU, AHMAD M.A., SHUTIAN LIU, *Image encryption scheme based on the commutation and anti-commutation rules*, Optics Communications **279**(2), 2007, pp. 285–290.
[14] ZHENGJUN LIU, QIUMING LI, JINGMIN DAI, XIAOYI ZHAO, XIAOGANG SUN, SHUTIAN LIU, AHMAD M.A., *Image encryption based on random scrambling of the amplitude and phase in the frequency domain*, Optical Engineering **48**(8), 2009, article ID 087005.
[15] ZHENGJUN LIU, YAN ZHANG, HAIFA ZHAO, AHMAD M.A., SHUTIAN LIU, *Optical multi-image encryption based on frequency shift*, Optik – International Journal for Light and Electron Optics **122**(11), 2011, pp. 1010–1013.
[16] HENNELLY B.M., SHERIDAN J.T., *Random phase and jigsaw encryption in the Fresnel domain*, Optical Engineering **43**(10), 2004, pp. 2239–2249.
[17] SINHA A., SINGH K., *Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes*, Optical Engineering **44**(5), 2005, article ID 057001.
[18] JOSHI M., SHAKHER C., SINGH K., *Fractional Fourier plane image encryption technique using radial hilbert-, and jigsaw transform*, Optics and Lasers in Engineering **48**(7–8), 2010, pp. 754–759.

[19] Guohai Situ, Jingjuan Zhang, *Multiple-image encryption by wavelength multiplexing*, Optics Letters **30**(11), 2005, pp. 1306–1308.
[20] Guohai Situ, Jingjuan Zhang, *Position multiplexing for multiple-image encryption*, Journal of Optics A: Pure and Applied Optics **8**(5), 2006, pp. 391–397.
[21] Ran Tao, Yi Xin, Yue Wang, *Double image encryption based on random phase encoding in the fractional Fourier domain*, Optics Express **15**(24), 2007, pp. 16067–16079.
[22] Zhengjun Liu, Jingmin Dai, Xiaogang Sun, Shutian Liu, *Triple image encryption scheme in fractional Fourier transform domains*, Optics Communications **282**(4), 2009, pp. 518–522.
[23] Zhengjun Liu, Shutian Liu, *Double image encryption based on iterative fractional Fourier transform*, Optics Communications **275**(2), 2007, pp. 324–329.
[24] Huijuan Li, Yurong Wang, *Double-image encryption based on iterative gyrator transform*, Optics Communications **281**(23), 2008, pp. 5745–5749.
[25] Zhengjun Liu, Qiuming Li, Jingmin Dai, Xiaogang Sun, Shutian Liu, Ahmad M.A., *A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains*, Optics Communications **282**(8), 2009, pp. 1536–1540.
[26] Zhengjun Liu, Qing Guo, Lie Xu, Ahmad M.A., Shutian Liu, *Double image encryption by using iterative random binary encoding in gyrator domains*, Optics Express **18**(11), 2010, pp. 12033–12043.
[27] Chen W., Quan C., Tay C.J., *Optical color image encryption based on Arnold transform and interference method*, Optics Communications **282**(18), 2009, pp. 3680–3685.
[28] Yamamoto H., Hayasaki Y., Nishida N., *Secure information display with limited viewing zone by use of multi-color visual cryptography*, Optics Express **12**(7), 2004, pp. 1258–1270.
[29] Joshi M., Chandrashakher, Singh K., *Color image encryption and decryption for twin images in fractional Fourier domain*, Optics Communications **281**(23), 2008, pp. 5713–5720.
[30] Linfei Chen, Daomu Zhao, *Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography*, Optics Express **15**(24), 2007, pp. 16080–16089.
[31] Zhengjun Liu, Jingmin Dai, Xiaogang Sun, Shutian Liu, *Color image encryption by using the rotation of color vector in Hartley transform domains*, Optics and Lasers in Engineering **48**(7–8), 2010, pp. 800–805.
[32] Zhengjun Liu, Lie Xu, Ting Liu, Hang Chen, Pengfei Li, Chuang Lin, Shutian Liu, *Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains*, Optics Communications **284**(1), 2011, pp. 123–128.
[33] Monaghan D.S., Gopinathan U., Naughton T.J., Sheridan J.T., *Key-space analysis of double random phase encryption technique*, Applied Optics **46**(26), 2007, pp. 6641–6647.
[34] Situ G., Monaghan D.S., Naughton T.J., Sheridan J.T., Pedrini G., Osten W., *Collision in double random phase encoding*, Optics Communications **281**(20), 2008, pp. 5122–5125.
[35] Xiang Peng, Peng Zhang, Hengzheng Wei, Bin Yu, *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006, pp. 1044–1046.
[36] Frauel Y., Castro A., Naughton T.J., Javidi B., *Resistance of the double random phase encryption against various attacks*, Optics Express **15**(16), 2007, pp. 10253–10265.
[37] Qin W., Peng X., *Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys*, Journal of Optics A: Pure and Applied Optics **11**(7), 2009, article ID 075402.
[38] Gerchberg R.W., Saxton W.O., *A practical algorithm for the determination of phase from image and diffraction plane pictures*, Optik (Jena) **35**(2), 1972, pp. 237–246.
[39] Yan Zhang, Cheng-Han Zheng, Tanno N., *Optical encryption based on iterative fractional Fourier transform*, Optics Communications **202**(4–6), 2002, pp. 277–285.

Received May 26, 2016
in revised form July 12, 2016