Optical encryption scheme based on ghost imaging with disordered speckles*

Yu-dong Zhang(张玉东)[1] and Sheng-mei Zhao(赵生妹)[1,2,†]

[1] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing* 210003, *China*

(Received 11 September 2016; revised manuscript received 7 January 2017; published online 30 March 2017)

An optical encryption scheme based on a ghost imaging system with disordered speckles is proposed to obtain a higher security with a small key. In the scheme, Alice produces the random speckle patterns and obtains the detection results with the help of a computational ghost imaging (CGI) system. Then Alice permutes the order of the random speckle patterns and shares the permutation sequence as a secure key to the authorized users. With the secure key, Bob could recover the object with the principle of the CGI system, whereas, the unauthorized users could not obtain any information of the object. The numerical simulations and experimental results show that the proposed scheme is feasible with a small key, simultaneously, it has a higher security. When the eavesdropping ratio (ER) is less than 40%, the eavesdropper cannot acquire any useful information. Meanwhile, the authorized users could recover completely with the secure key.

Keywords: optical encryption, computational ghost imaging, small key, disordered speckles

PACS: 42.30.–d, 42.50.Ar, 42.30.Wb, 42.30.Va **DOI:** 10.1088/1674-1056/26/5/054205

1. Introduction

Since it was experimentally demonstrated with an entangled source in 1995 by Pittman *et al.*,[1] ghost imaging (GI) has attracted a lot of attention. Its successful realization with thermal light in 2002[2] made GI become a promising field to obtain higher resolution images. Especially, a new configuration of the GI system, called computational ghost imaging (CGI),[3] opened up some new perspectives with the GI system. The key principle of GI is the correlation between the two signals obtained from two separated detectors in a GI system, where one signal is recorded by a bucket detector in the signal beam to collect all the illumination passing through an object, and the other is the intensity signal collected in the reference beam with a high spatial resolution detector, such as a charge coupled device (CCD). The image is retrieved at the reference beam after the correlation between the signals from both beams.[4–17] The past has witnessed the rapid developments of the GI technique. For example, Ferri *et al.* presented the differential ghost imaging (DGI) to enhance the signal-to-noise ratio of recovering images.[12] Bromberg *et al.* experimentally demonstrated a GI technique using only a single detector.[14] Cao *et al.* discussed the geometrical optics of a GI system,[15] and achieved color GI with pseudo-white-thermal light.[16]

Recently, GI has found its novel application in optical encryption.[18–26] For example, in 2010, Clemente *et al.* proposed an optical encryption scheme based on computational GI to encrypt and securely transmit information to a remote party.[23] Successively, Tanha *et al.* proposed a gray and color optical encryption scheme to improve the security and developed the application in 2012.[24] Kong *et al.* proposed an approach to encrypt ghost images by flexibly manipulating the position correlation of a pair of 'signal' and 'idler' beams.[25] We presented a QR-coded compressive ghost imaging optical encryption, where the computational GI technique, QR code, and compressive sensing technique are adopted in the scheme.[27] Additionally, Li *et al.* proposed a new protocol of high-speed secure key distribution over an optical network based on computational correlation imaging.[21]

It is shown that the optical encryption schemes based on CGI have noticeably reduced the number of the bits required to transmit an image because the encryption of the object image is not a complex valued matrix but simply an intensity vector. However, the series random speckle patterns to produce the detection results in the signal beam are commonly selected as a secure key in most existing optical encryption schemes, and they have to be transmitted to the authorized users in a private channel. Hence, the corresponding key distribution is a severe task in the realizations of the existing optical encryption schemes based on the CGI system. A secure and only with a little key distribution scheme is a promising direction.

In this paper, we propose a secure optical encryption scheme based on CGI with a small key. Here, a permutation sequence of the random speckle patterns, instead of the random speckle patterns themselves, is used as the secure key. In the proposed scheme, Alice produces the random speckle patterns and obtains the detection results with the help of a CGI

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61475075 and 61271238) and the Open Research Fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, China (Grant No. NYKL2015011).

†Corresponding author. E-mail: zhaosm@njupt.edu.cn

© 2017 Chinese Physical Society and IOP Publishing Ltd

system. Then Alice permutes the order of the random speckle patterns and keeps the permutation sequence as a secure key. Later, Alice transmits the disordered speckle patterns and the detection results to Bob by a public channel, and sends the permutation sequence to Bob by a private channel. The unauthorized users cannot reconstruct the object because the correlations between the detection results and the speckle patterns are destroyed. On the contrary, the legitimate users could reorder the random speckle patterns by the received key, and recover the object with the theory of CGI.

This paper is organized as follows. In Section 2, we propose a secure optical encryption based on CGI with a small key, and give the theoretical analysis of the proposed scheme. In Section 3, we present the experimental and numerical simulations results to testify the proposed scheme. Finally, we draw our conclusion in Section 4.

2. Optical encryption scheme based on GI with disordered speckles

Figure 1 shows the schematic diagram of the proposed optical encryption scheme, where $\{I_i(x,y)\}_{i=1}^{M}$ are M speckle patterns with random intensities. They could be produced by projecting light on to a special digital light device, such as a spatial light modulator (SLM) or digital micro-mirror device (DMD). $\{I_j(x,y)\}_{j=1}^{M}$ are the disordered random intensity patterns produced by $\{I_i(x,y)\}_{i=1}^{M}$ with a permutation P, which is taken as the secure key in this paper. Alice uses the random speckle patterns $\{I_i(x,y)\}_{i=1}^{M}$ in a CGI system to generate a series of detection results $\{B_i\}_{i=1}^{M}$, and transmits both of the detection results $\{B_i\}_{i=1}^{M}$ and the disordered random intensity patterns $\{I_j(x,y)\}_{j=1}^{M}$ to receivers by a public channel. Simultaneously, she shares the secure key, the permutation P, with the authorized users by a private channel. Because the correlations between the detection results and the disorderly random speckle patterns are destroyed, eavesdroppers who have no secure key cannot reconstruct the imaging of the object even though they have the detection results. On the other hand, the legitimate users first reorder the disordered random intensity patterns $\{I_j(x,y)\}_{j=1}^{M}$ by the same permutation operation with the secure key, then reconstruct the imaging with the help of the GI principle. In the proposed scheme, the secret key with M bits is very small in comparison with the random speckle patterns in most existing encryption schemes based on CGI.

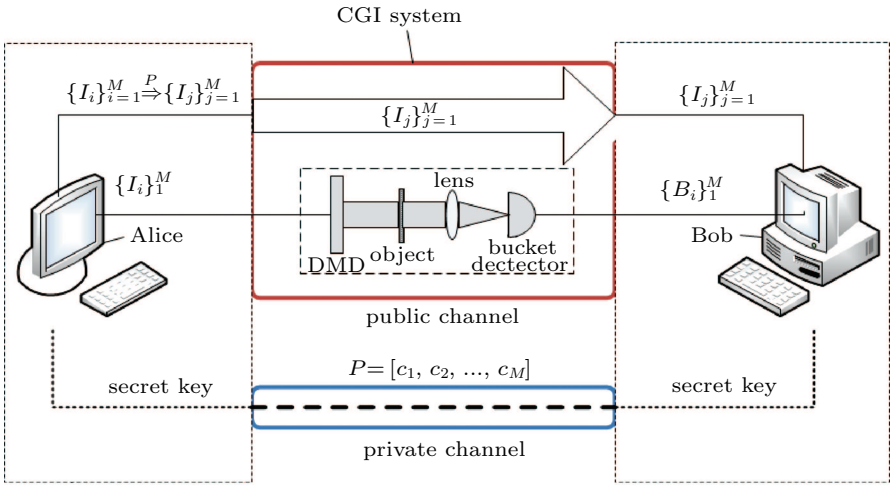


Fig. 1. (color online) Schematic diagram of the proposed encryption scheme with CGI system. The detection results from the object and the disorderly speckle patterns are transmitted to users by a public channel, meanwhile, the secret key, the permutation P for the disorderly speckle patterns, is transmitted to the authorized users by a private channel.

The detection result B_i in Fig. 1 represents the whole of the intensities passing through an object and is detected by a bucket detector in the CGI system

$$B_i = \int I_i(x,y)T(x,y)\mathrm{d}x\mathrm{d}y, \tag{1}$$

where $T(x,y)$ is the transmission function of the object, and $I_i(x,y)$ is the intensity distribution of the i-th speckle pattern. With M detections, the detection results $\{B_i\}_{i=1}^{M}$ are achieved with the M different random speckle patterns $\{I_i(x,y)\}_{i=1}^{M}$. Alice permutes the speckle patterns $\{I_i(x,y)\}_{i=1}^{M}$ to the disordered speckle patterns $\{I_j(x,y)\}_{j=1}^{M}$,

$$\{I_j(x,y)\}_{j=1}^{M} = P\{I_i(x,y)\}_{i=1}^{M}, \tag{2}$$

where P is the permutation operation with only M data. Because P is a permutation operation, it is known that $P^2 = I$, which indicates that the order of the speckle patterns can be recovered when the permutation is operated twice. With the key and the transmitted information, the authorized users (Bob) could recover the object with GI theory. He first reorders the received intensity patterns $\{I_j^{\mathrm{r}}(x,y)\}_{j=1}^{M}$,

$$\{I_j^{\mathrm{r}}(x,y)\}_{j=1}^{M} = P\{I_j^{\mathrm{t}}(x,y)\}_{j=1}^{M} = P^2\{I_i(x,y)\}_{i=1}^{M}$$

$$= I\{I_i(x,y)\}_{i=1}^{M} = \{I_i(x,y)\}_{i=1}^{M}. \quad (3)$$

Then, the imaging of the object can be reconstructed with the second-order correlation

$$O(x,y) = \frac{1}{M}\sum_{i=1}^{M}[B_i - \langle B\rangle]I_i^{\mathrm{r}}(x,y) = \frac{1}{M}\sum_{i=1}^{M}[B_i - \langle B\rangle]I_i^{\mathrm{r}}(x,y). \quad (4)$$

On the other hand, the unauthorized users cannot recover the imaging $O'(x,y)$, because $\{B_i\}_{i=1}^{M}$ have no correlation with $I_j(x,y)_{j=1}^{M}$

$$O'(x,y) = \frac{1}{M}\sum_{i=1}^{M}[B_i - \langle B\rangle]I_j^{\mathrm{r}}(x,y) = \frac{1}{M}\sum_{i=1}^{M}[B_i - \langle B\rangle]I_j^{\mathrm{r}}(x,y), \quad (5)$$

where $O'(x,y)$ is random data. No useful information can be obtained from the random data $O'(x,y)$.

3. Experiment and simulation results

In this section, we testify the proposed optical encryption scheme by experiment and numerical simulations. In addition, we discuss the vulnerability of the proposed scheme to eavesdropping.

Figure 2 is the schematic setup of the experiment. A digital micromirror device (DMD TIDLPC350) controlled by a computer is used as a source to generate the random speckle patterns. After, the beam with the random speckle patterns $\{I_i(x,y)\}_{i=1}^{M}$ (64×64 pixels) expands with a projecting lens and illuminates object 'NUPT' which is printed on a piece of transparent plastic thin sheet. The distance between the object and the DMD is 787.5 mm. The light through the object is focused by a lens with focal length 250 mm, and is received by a detector (Thorlabs power meter S120C and P-M100USB), where S120C is an optical power meter and PM100USB is a USB power and energy meter interface: they work together to play the role of the bucket detector. This signal is recorded as the detection result B_i. Alice sends both disordered random speckle patterns $\{I_j(x,y)\}_{j=1}^{M}$ and detection results $\{B_i\}_{i=1}^{M}$ to remote users in a public channel. Meanwhile, the secure key is sent to the legitimate user, Bob, in a private channel. The intensities of the random speckle patterns are produced by a computer. Each random speckle pattern has a Gaussian distribution with size 64×64 pixels.

In order to qualify the reconstructed image objectively, the mean square error (MSE) and peak signal-to-noise ratio (PSNR) are used as evaluations, which are defined as[27]

$$\mathrm{MSE} = \frac{1}{N}\sum_{x,y}(T'(x,y) - T(x,y))^2, \quad (6)$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{maxVal}^2}{\mathrm{MSE}}\right), \quad (7)$$

where $T(x,y)$ and $T'(x,y)$ denote the intensities of the original and the reconstructed images, respectively, N is number of pixels of the image, and maxVal is the maximum possible pixel value of the image.

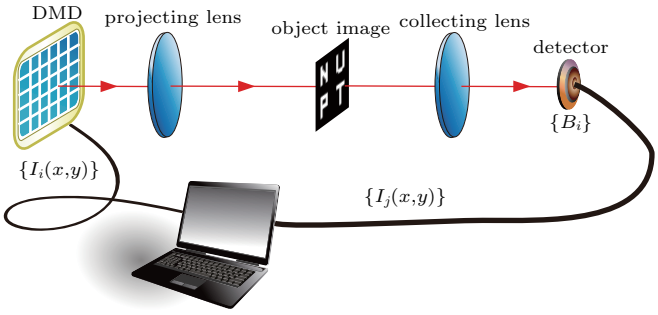


Fig. 2. (color online) Schematic setup of the experiment to testify the proposed scheme.

We first demonstrate the feasibility of the proposed encryption scheme in Fig. 3, where 'Lena' and 'NUPT' (64×64 pixels) are selected as the objects in the simulation, and only 'NUPT' is used for the experiment. Both compressive sensing and second-order correlation recovery methods are used. The measurement times are 4096 for the simulations and 5000 for the experimental results. With the proposed optical encryption scheme, the recovered images with the key have the complete information of the original ones; whereas, the recovery images without the key have no useful information of the original object images. For the object 'NUPT', the results in Fig. 3 show that PSNR = Inf, MSE = 0 for the legitimate users, PSNR = 5.22, MSE = 0.28 for the unauthorized users using the compressed sensing recovery method, while PSNR = 8.13, MSE = 0.15 for the legitimate users, PSNR = 5.21, MSE = 0.30 for the unauthorized users using the second-order correlation recovery method. The results with the compressed sensing technique are much better than those with the second-order correlation method. The experimental results have also demonstrated that for the recovered 'NUPT', PSNR is 7.15, MSE is 0.18 with the key, while PSNR is 5.13, MSE is 0.29 without the key using the second-order correlation recovery method. Due to the impact of environment and equipment noise, the recovered image from the experiment has a little lower quality. All the results indicate that the proposed scheme is feasible.

We then test the security of the proposed encryption scheme with the object 'NUPT' and compare with the results of the encryption scheme in Ref. [23]. Assume that a potential eavesdropper, who knows the proper reconstruction mechanism, has unauthorized access to a fraction (eavesdropping ratio, ER) of the secure key and uses the corresponding correct speckle patterns to reconstruct the image. The value of ER is set from 0 to 50%.

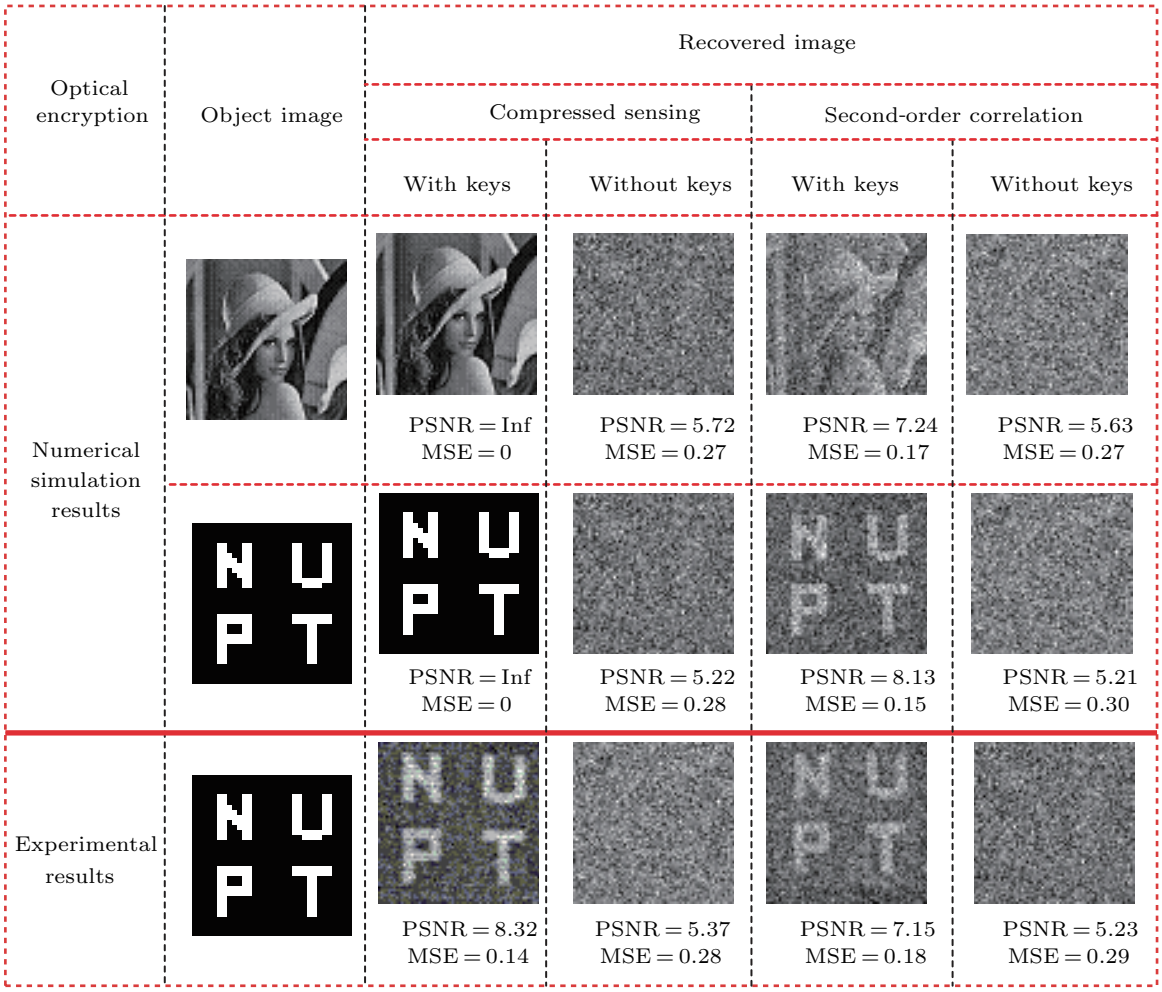


Fig. 3. (color online) The numerical simulation and experimental results with the proposed optical encryption scheme.

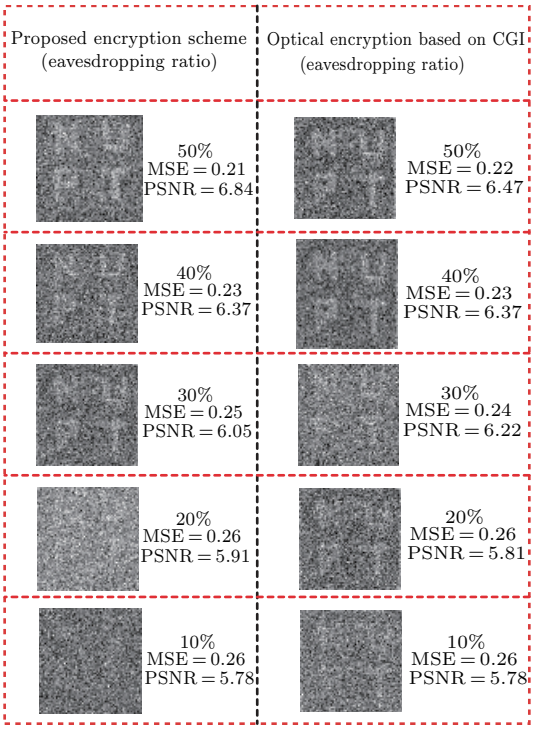


Fig. 4. (color online) The experimental results with the proposed scheme under different eavesdropping ratios.

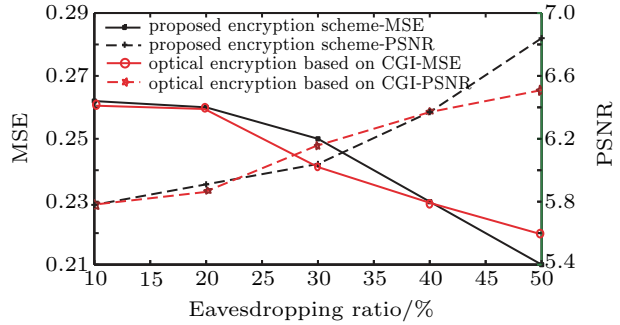


Fig. 5. (color online) The PSNR and MSE of the recovered images against the eavesdropping ratio.

Figures 4 and 5 show the experimental results using the proposed scheme under different ER. The measurement time is setup to 5000. All the results are reconstructed using the second-order correlation method. Figure 4 shows the reconstructed objects with the disordered speckles encryption scheme and the CGI encryption scheme[23] under different ER. Figure 5 shows that the PSNR and MSE of the reconstructed images against ER. The results indicate that the proposed scheme has similar results to the encryption scheme in Ref. [23], however, it has a much smaller key. With the proposed scheme, the amount of the secret key is bout 6.5×10^4

bits, while it is about 2.048×10^7 bits with the scheme in Ref. [23]. The ratio of the secret key is 3.17×10^{-3}. The results also show that the encrypted information cannot be retrieved when ER is less than 40%. The proposed scheme has high security.

4. Conclusion

We have proposed an optical encryption scheme based on the CGI system with disordered speckles. Alice produces the random speckle patterns and obtains the detection results with these random speckle patterns by the CGI technique. Later, she permutes the order of the random speckle patterns and shares the permutation sequence as a secret key to the authorized users. With the secret key, the legitimated user could recover the object, whereas the unauthorized user could not obtain any information of the object. It has similar results to the encryption scheme in Ref. [23], however, it has a much smaller key. The simulation and experiment results show the feasibility and the security of the proposed scheme. When the ER is less than 40%, the eavesdropper cannot acquire any useful information of the encrypted image. Meanwhile, the authorized users could recover completely the encrypted information with the secret key. The proposed optical encryption scheme has a samller key distribution in the private channel with a higher security. It has provided a practical method to complement optical encryption with the CGI system.

References

[1] Pittman T B, Shih Y H, Strekalov D V and Sergienko A V 1995 *Phys. Rev. A* **52** 3429

[2] Bennink R S, Bentley S J and Boyd R W 2002 *Phys. Rev. Lett.* **89** 113601

[3] Shapiro J H 2008 *Phys. Rev. A* **78** 061802

[4] Gatti A, Brambilla E, Bache M and Lugiato L A 2004 *Phys. Rev. Lett.* **93** 093602

[5] Ferri F, Magatti D, Gatti A, Bache M, Brambilla E and Lugiato L A 2005 *Phys. Rev. Lett.* **94** 183602

[6] Zhang D, Zhai Y H, Wu L A and Chen X H 2005 *Opt. Lett.* **30** 2354

[7] Erkmen B I and Shapiro J H 2006 *Phys. Rev. A* **74** 041601

[8] Meyers R, Deacon K S and Shih Y 2008 *Phys. Rev. A* **77** 041801

[9] Erkmen B I and Shapiro J H 2008 *Phys. Rev. A* **77** 043809

[10] Erkmen B I and Shapiro J H 2010 *Adv. Opt. Pho.* **2** 405

[11] Li C, Wang T, Pu J, Zhu W and Rao R 2010 *Appl. Phys. B* **99** 599

[12] Ferri F, Magatti D, Lugiato L and Gatti A 2010 *Phys. Rev. Lett.* **104** 253603

[13] Li M F, Zhang Y R, Luo K H, Wu L A and Fan H 2013 *Phys. Rev. A* **87** 033813

[14] Bromberg Y, Katz O and Silberberg Y 2009 *Phys. Rev. A* **79** 053840

[15] Cao D Z, Xiong J and Wang K G 2005 *Phys. Rev. A* **71** 013801

[16] Cao D Z, Xu B L, Zhang S H and Wand K G 2015 *Chin. Phys. Lett.* **32** 114208

[17] Zhao S M and Zhuang P 2014 *Chin. Phys. B* **23** 054203

[18] Wang L, Zhao S M, Cheng W W, Gong L Y, and Chen H W 2016 *Opt. Commun.* **366** 314

[19] Liu Q, Luo K H, Chen X H and Wu L A 2010 *Chin. Phys. B* **19** 094211

[20] Zafari M, Kheradmand M and Ahmadi-Kandjani S 2014 *J. Opt.* **16** 105405

[21] Li S, Yao X R, Yu W K, Wu L A and Zhai G J 2013 *Opt. Lett.* **38** 2144

[22] Tanha M, Kheradmand R and Ahmadi-Kandjani S 2013 *Phys.Scr.* **2013** 014059

[23] Clemente P, Durán V, Torrescompany V, Tajahuerce E and Lancis J 2010 *Opt.Lett.* **35** 2391

[24] Tanha M, Kheradmand R and Ahmadi-Kandjani S 2012 *Appl. Phys. Lett.* **101** 101108

[25] Kong L J, Li Y N, Qian S X, Li S M, Tu C H and Wang H T 2013 *Phys. Rev. A* **88** 013852

[26] Chen W and Chen X D 2013 *Appl. Phys. Lett.* **103** 221106

[27] Zhao S M, Wang L, Liang W Q, Cheng W W and Gong L Y 2015 *Opt. Commun.* **353** 90