Journal of the Optical Society of Korea
Vol. 20, No. 4, August 2016, pp. 476-480

ISSN: 1226-4776(Print) / ISSN: 2093-6885(Online)
DOI: http://dx.doi.org/10.3807/JOSK.2016.20.4.476

Optical Encryption Scheme with Multiple Users Based on Computational Ghost Imaging and Orthogonal Modulation

Sheng Yuan[1]*, Xuemei Liu[1], Xin Zhou[2], and Zhongyang Li[1]

[1]*Department of Information and Engineering, North China University of Water Resources and Electric Power, Zhengzhou 450011, China*
[2]*Department of Opto-electronics Science and Technology, Sichuan University, Chengdu 610065, China*

(Received March 4, 2016 : revised June 13, 2016 : accepted June 14, 2016)

For the application of multiusers, the arrangement and distribution of the keys is a much concerning problem in a cryptosystem. In this paper, we propose an optical encryption scheme with multiple users based on computational ghost imaging (CGI) and orthogonal modulation. The CGI encrypts the secret image into an intensity vector rather than a complex-valued matrix. This will bring convenience for post-processing and transmission of the ciphertext. The orthogonal vectors are taken as the address codes to distinguish users and avoid cross-talk. Only the decryption key and the address code owned by an authorized user are matched, the secret image belonging to him/her could be extracted from the ciphertext. Therefore, there are two security levels in the encryption scheme. The feasibility and property are verified by numerical simulations.

Keywords : Optical encryption, Computational ghost imaging, Orthogonal modulation
OCIS codes : (070.4560) Data processing by optical means; (110.1758) Computational imaging; (110.3010) Image reconstruction techniques

I. INTRODUCTION

In recent years, optical information processing techniques have been widely applied in the field of information security, as they can offer the advantages of high-speed parallel processing and multiple degrees of freedom (such as amplitude, phase, wavelength, and polarization). Especially since the double random-phase encryption method [1] was proposed, all kinds of random-phase encoding (RPE) schemes based on diffraction or interference principles have been booming [2-13]. As the accompanying complementary opposites, the corresponding security analyses have also been carried out and have promoted the further development of optical encryption techniques [14-18].

In practice, the distribution, transmission and storage of the ciphertext and key are important problems that need to be solved especially in the application of multiple users. Since ghost imaging (GI) experiments based on quantum entangled photon pairs [19] and a classical light source [20] were performed, GI, as an intriguing optical technique, has been receiving considerable current attention [21-25]. Recently as a development of GI, the computational ghost imaging (CGI) is successfully applied in the field of optical cryptography [26], which noticeably reduces the number of bits required to transmit and store, because the ciphertext is not a complex-valued matrix but simply an intensity vector. Subsequently, many methods were proposed to improve the security and develop its application [27-32]. In addition, several secret sharing schemes were proposed based on combination theory [33-35], in which a secret image is encrypted into multiple parts and transmitted separately to multiple users, and the secret can only be decrypted by the qualified set of users. This technique is a verification scheme for multiple users and brings security in many practical applications.

In some other applications of multiusers, the sender needs

*Corresponding author: shn.yuan@sohu.com
Color versions of one or more of the figures in this paper are available online.

to transmit different secret images to different authorized users. If the ciphertext of the multiple secret images is shared for all authorized users but anyone of them can only extract his/her own secret image with his/her own key, the burden of transmitting huge amounts of secret data borne by the channel will be reduced. In recent years, the orthogonal codes are utilized to design the keys for different authorized users to avoid the secret images being extracted mutually [36-38]. In this paper, we combine the CGI and the orthogonal modulation to achieve a secure and convenient scheme for multiuser application. In this scheme, all the secret images are firstly encrypted by CGI technique, and then modulated by an orthogonal matrix to obtain the ciphertext. The random-phase masks in CGI are taken as the encryption key and each vector in the orthogonal matrix is an address code for each user. Only the encryption key and address code are matched, the secret image could be retrieved from the ciphertext. There are two security levels in the encryption scheme to ensure the security of the secret images.

II. ENCRYPTION SCHEME WITH MULTIPLE USERS

2.1. Encryption

The schematic and flow chart of the encryption process are shown in Fig. 1. A spatially coherent laser is split into N light beams by the beam splitter (BS), and then passes through individual spatial light modulators (SLMs), which can be controlled by computer to introduce a series of random-phase masks $\{P_n^r\}$ as the encryption keys with phase values uniformly distributed over the interval $[0, 2\pi]$. Here, the subscripts $n = 1, 2, \cdots, N$ and $r = 1,2,\cdots, M$, N and M, respectively, are the number of the images to be encrypted and of measurements.

Each modified beam illuminates a secret image T_n, and each of the transmitted lights is converged into its own bucket detector (BD) to obtain the measurements D_n^r. Here, the bucket detector is utilized to capture the intensity of the convergent light and can be achieved by a photodiode [19], which is a single-pixel detector without spatial resolution (so-called bucket).

According to the principle of CGI, the process illustrated above is repeated M times for different random-phase masks P_n^r in each beam to obtain the intensity sequence $\left|D_n^r\right\rangle$,

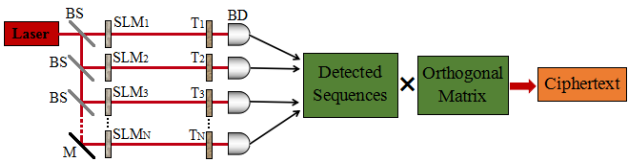

FIG. 1. Schematic and flow chart of encryption; BS: beam splitter, M: mirror, SLM: spatial light modulator, T_n: secret image, BD: bucket detector.

$$\left|D_n^r\right\rangle = \left|D_n^1, D_n^2, \cdots, D_n^M\right\rangle, \tag{1}$$

and

$$D_n^r = \int I_n^r(x,y) T_n(x,y) dxdy, \tag{2}$$

where $I_n^r(x, y)$ is the intensity of the Fresnel diffraction field of P_n^r, i.e.,

$$I_n^r(x,y) = \left|P_n^r(x,y) * h(x,y,z)\right|^2, \tag{3}$$

* denotes the 2D convolution operation. $h(x, y, z)$ is the point pulse function of the Fresnel transform described by

$$h(x,y,z) = \frac{\exp(j2\pi z/\lambda)}{j\lambda z} \exp\left[\frac{j\pi}{\lambda z}\left(x^2 + y^2\right)\right], \tag{4}$$

where $j = \sqrt{-1}$, z is the Fresnel propagation distance between the phase mask and the secret image in each beam, λ denotes wavelength of the laser. The intensity patterns $I_n^r(x, y)$ can be calculated by Eq. (3) and do not need to be detected by a real intensity detector such as a charge-coupled device (CCD), which is the main advantage of CGI [21].

Thus, N users corresponding to N sequences of $\left|D_n^r\right\rangle$ form a matrix D with $M \times N$ elements,

$$D = \left\langle \left|D_1^r\right\rangle, \left|D_2^r\right\rangle, \cdots, \left|D_N^r\right\rangle \right|. \tag{5}$$

Subsequently, the matrix D composed by the detected sequences is modulated by an orthogonal matrix O with $M \times N$ elements to form the ciphertext C, i.e.,

$$C(i,j) = \sum_{n=1}^{N} D(i,n) O(n,j), \tag{6}$$

In summary, all the secret images are firstly encrypted by random-phase masks $\{P_n^r\}$ in the system of CGI, and then modulated by an orthogonal matrix O to obtain the ciphertext. The random-phase masks are taken as the encryption key and each vector in the orthogonal matrix is an address code for each user. There are two security levels in the encryption scheme to ensure the security of the secret images.

2.2. Decryption

We know that the orthogonal code satisfies

$$\sum_{n=1}^{N} O(i,n) O^T(n,j) = \delta_{ij}, \tag{7}$$

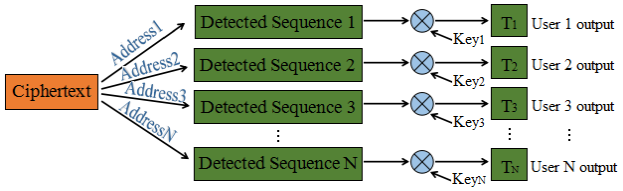

FIG. 2. Schematic and flow chart of decryption.

where O^T is the transpose of O, δ_{ij} is the Dirac delta function. Then in the decryption process (shown in Fig. 2), the kth column of the orthogonal matrix O^T is applied to the ciphertext C in order to extract the detected sequence $|D_k^r\rangle$ corresponding to the kth secret image:

$$D_k^r = \sum_{j=1}^{N}\left[\sum_{n=1}^{N} D(i,n)O(n,j)\right]O^T(j,k) = D(i,k)\big|_{i=r}. \quad (8)$$

Therefore, each column of the orthogonal matrix O^T corresponds to a detected sequence of one secret image, and all the column vectors can be regarded as the address codes of all the secret images for multiple users.

In the following step, the secret image can be retrieved by the principle of CGI according to the extracted sequence $|D_n^r\rangle$ and the calculated decryption key $I_n^r(x, y)$ by Eq. (3), i.e.,

$$\tilde{T}_n(x,y) = \frac{1}{M}\sum_{r=1}^{M}\left(D_n^r - \langle D_n\rangle\right)I_n^r(x,y), \quad (9)$$

where $\langle D_n\rangle$ is the average value for the detected sequence $|D_n^r\rangle$.

III. COMPUTER SIMULATION RESULTS

3.1. Feasibility of the Proposal

To verify the feasibility of the proposal, four binary and grayscale images (shown in Fig. 3) with 128×128 pixels are taken as the secret images. In addition, a 4×4 orthogonal matrix O is adopted to modulate the detected sequences of the CGI, for example, O=[1/$\sqrt{2}$ -1/2 0 -1/2; 0 1/2 -1/$\sqrt{2}$ -1/2; 1/$\sqrt{2}$ 1/2 0 1/2; 0 1/2 1/$\sqrt{2}$ -1/2]. Thus the address codes o_1=[1/$\sqrt{2}$ -1/2 0 -1/2]^T , o_2=[0 1/2 -1/$\sqrt{2}$ -1/2]^T, o_3=[1/$\sqrt{2}$ 1/2 0 1/2]^T, and o_4=[0 1/2 1/$\sqrt{2}$ -1/2]^T refer to the four secret images for four users.

Based on the principle of CGI [21, 22], the retrieved images are present in Figs. 4 and 5, respectively corresponding to the binary and grayscale images under the conditions that the address code and the decryption key are matched or unmatched. Because of the limited resolution of CGI [21, 22], the number of measurements needed to make the decryption image achieve acceptable quality for grayscale

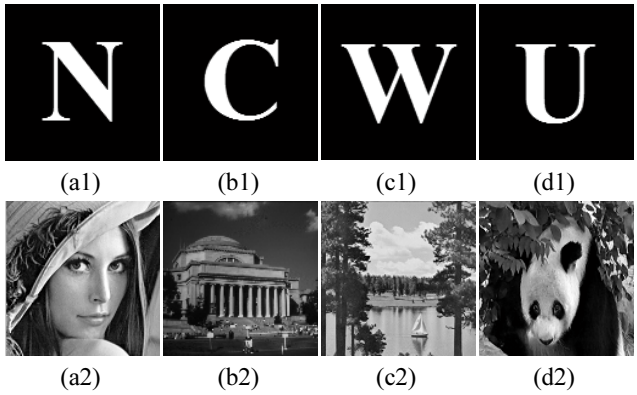

FIG. 3. Four original secret images adopted in this simulation, (a1)-(d1) binary and (a2)-(d2) grayscale images.

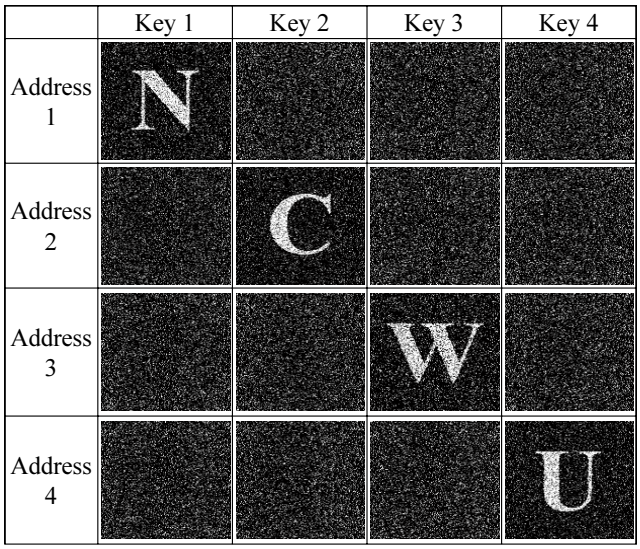

FIG. 4. Retrieved binary images under the conditions that the address code and the key are matched or unmatched.

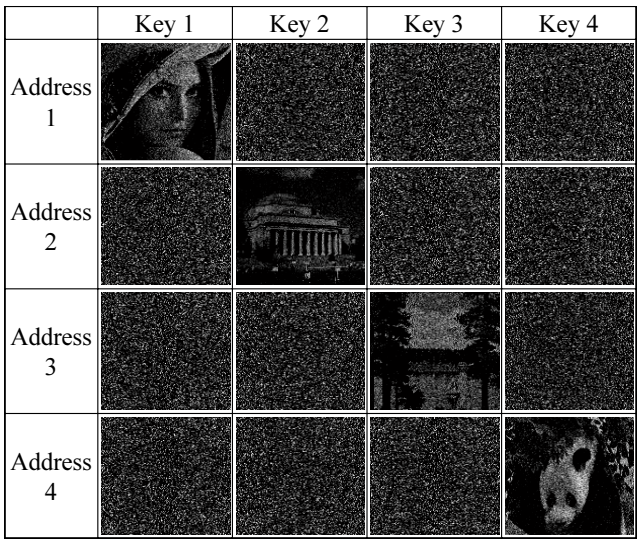

FIG. 5. Retrieved grayscale images under the conditions that the address code and the key are matched or unmatched.

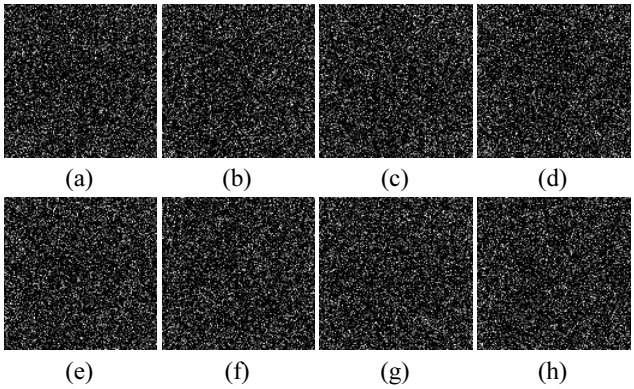

FIG. 6. Retrieved images (a)-(d) only by the decryption keys, and (e)-(h) by the wrong address codes.

image is larger than binary image. Here, we take the number of measurements M=10000 for binary images and M=20000 for grayscale images. As can be seen from the results, no matter binary or grayscale images, the secret images can be recovered only when the address codes and the decryption keys are matched and no cross-talk exists in them, otherwise the decrypted images are random noise patterns.

3.2. Security Analysis

In encryption, the random-phase masks are taken as the encryption key and each vector in the orthogonal matrix is an address code for each user. There are two security levels in the encryption scheme to ensure the security of the secret images. Subsequently, we take the binary images as an example to further test the security of the proposal. Firstly, the four decryption keys are directly utilized to retrieve the secret images in absence of the address codes, the results are shown in Fig. 6(a)-(d). Furthermore, a wrong orthogonal matrix (such as O′=[1 2 1 1; -2 1 -1 1; 1 1 -2 -1; -1 1 1 -2]), which is randomly selected as the address codes, and the correct decryption keys are adopted in the decryption process, the recovered images are shown in Fig. 6(e)-(h). The results indicated that the secret images cannot be retrieved whether by not using the address codes or by using the wrong address codes.

IV. CONCLUSION

In this paper, we propose a simple and convenient optical encryption scheme for multiple users. This scheme adopts two encryption levels: CGI and orthogonal modulation. The CGI encrypts the secret image into an intensity vector rather than the complex-valued matrix, which reduces the data amount of the ciphertext and brings convenience for post-processing. Other, an orthogonal matrix is also utilized to modulate the detected intensity sequences from the CGI system. According to the property of the orthogonal matrix, each of the detected sequence corresponding to a secret image can be extracted from the ciphertext by a row vector of the orthogonal matrix. Thus all the row vectors of the orthogonal matrix are regarded as the address codes for all the secret images. This function may bring convenience in the application of multiusers. The secret images can be decrypted only when the address code and the decryption key are matched. However, the decrypted images contain serious noise, which is unavoidable for CGI but in some extent can be reduced by increasing the number of measurements or adopting other improved CGI [24, 25].

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grants No. 61205003, 61177009, 61475104 and 61201101), the Program for Innovative Research Team (in Science and Technology) in University of Henan Province (IRTSTHN) (Grants No. 13IRTSTHN023), the Innovation Scientists and Technicians Troop Construction Projects of Henan Province and the Young Backbone Teachers in University of Henan Province (Grants No. 2014GGJS-068).

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
2. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120-155 (2014).
3. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887-889 (2000).
4. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584-1586 (2004).
5. Z. Liu and S. Liu, "Random fractional Fourier transform," Opt. Lett. **32**, 2088-2090 (2007).
6. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589-636 (2009).
7. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**, 118-120 (2010).
8. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," Opt. Lett. **38**, 1425-1427 (2013).
9. X. Meng, L. Cai, X. Xu, X. Yang, X. Shen, G. Dong, and Y. Wang, "Two-step phase-shifting interferometry and its application in image encryption," Opt. Lett. **31**, 1414-1416 (2006).
10. Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. **33**, 2443-2445 (2008).
11. S. Yuan, X. Zhou, M. S. Alam, X. Lu, and X. Li, "Information hiding based on double random-phase encoding and public-key cryptography," Opt. Express **17**, 3270-3284 (2009).
12. N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun. **284**, 735-739 (2011).
13. S. K. Rajput, D. Kumar, and N. K. Nishchal, "Photon counting

imaging and phase mask mutiplexing for multiple image authentication and hologram security," Appl. Opt. **54**, 1657-1666 (2015).
14. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**, 1644-1646 (2005).
15. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**, 1044-1046 (2006).
16. J. Wu, W. Liu, Z. Liu, and S. Liu, "Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase," Opt. Commun. **338**, 164-167 (2015).
17. P. Kumar, A. Kumar, J. Joseph, and K. Singh, "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," Opt. Lett. **34**, 331-333 (2009).
18. M. He, Q. Tan, L. Cao, Q. He, and G. Jin, "Security enhanced optical encryption system by random phase key and permutation key," Opt. Express **17**, 22462-22473 (2009).
19. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," Phys. Rev. A **52**, R3429-R3432 (1995).
20. R. S. Bennink, S. J. Bentley, and R. W. Boyd, ""Two-photon" coincidence imaging with a classical source," Phys. Rev. Lett. **89**, 113601 (2002).
21. J. H. Shapiro, "Computational ghost imaging," Phys. Rev. A **78**, 061802 (2008).
22. Y. Bromberg, O. Katz, and Y. Silberberg, "Ghost imaging with a single detector," Phys. Rev. A **79**, 053840 (2009).
23. P. Clemente, V. Duran, E. Tajahuerce, V. Torres-Company, and J. Lancis, "Single-pixel digital holography," Phys. Rev. A **86**, 041803 (2012).
24. B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, "Normalized ghost imaging," Opt. Express **20**, 16892-16901 (2012).
25. W. Wang, X. Hu, J. Liu, S. Zhang, J. Suo, and G. Situ, "Gerchberg-Saxton-like ghost imaging," Opt. Express **23**, 28416-28422 (2015).
26. P. Clemente, V. Duran, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**, 2391-2393 (2010).
27. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," Appl. Phys. Lett. **101**, 101108 (2012).
28. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**, 221106 (2013).
29. W. Chen and X. Chen, "Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption," Europhys. Lett. **109**, 14001 (2015).
30. J. Li, J. Li, Y. Pan, and R. Li, "Compressive optical image encryption," Sci. Rep. **5**, 10374 (2015).
31. W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," Europhys. Lett. **110**, 44002 (2015).
32. S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique," Opt. Commun. **353**, 90-95 (2015).
33. Z. Liu, M. A. Ahmad, and S. Liu, "Image sharing scheme based on combination theory," Opt. Commun. **281**, 5322-5325 (2008).
34. S. H. Jeon and S. K. Gil, "Optical secret key sharing method based on Diffie-Hellman key exchange algorithm," J. Opt. Soc. Korea **18**, 477-484 (2014).
35. S. H. Jeon and S. K. Gil, "Optical implementation of asymmetric cryptosystem combined with D-H secret key sharing and triple DES," J. Opt. Soc. Korea **19**, 592-603 (2015).
36. M. N. Islam, M. A. Karim, and K. V. Asari, "Information security using multiple reference-based optical joint transform correlation and orthogonal code," Opt. Laser Technol. **50**, 8-13 (2013).
37. I. H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," J. Opt. Soc. Korea **18**, 201-206 (2014).
38. I. H. Lee and M. Cho, "Double random phase encryption based orthogonal encoding technique for color images," J. Opt. Soc. Korea **18**, 129-133 (2014).