Hybrid Optical Encoding Structures for Two-Layer Optical Information Authentication

Wen Chen[1,2]
[1]Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
[2]The Hong Kong Polytechnic University Shenzhen Research Institute,
Shenzhen 518057, China
e-mail: owen.chen@polyu.edu.hk

***Abstract*—In recent years, optical information security has become an important research topic. In this paper, two-layer optical information authentication method is studied by using hybrid optical encoding structures. Digital holographic setup and computer-generated hologram principle are applied respectively for the first-layer and second-layer optical information authentication. The analyses and numerical results demonstrate that the method is promising.**

Keywords-computer holography; digital holography; optical information authentication; optical security and encryption; optical information processing

I. INTRODUCTION

Optical security [1] has attracted much current attention. Some optical setups [2]–[6], such as digital holography and diffractive imaging, have been developed to improve security and robustness of optical systems. It has been found recently that optical information authentication [7]–[15] can be implemented based on optical encoding structures, and additional layers can be generated for security enhancement. For instance, Pérez-Cabré et al. [7] applied photon-counting approach to generate the compressed complex-valued wavefront in CCD plane, and the decoded image is noisy without disclosure of original information. Chen et al. [8] proposed to apply the compressed phase-only hologram for optical information authentication. Various methods and structures [9]–[15] have been further developed for optical information authentication to improve the flexibility and performance. However, it is always desirable that advanced structures and strategies can be continuously developed to enrich this research area.

In this paper, hybrid optical encoding structures are developed for two-layer optical information authentication. In the first layer, double random phase encoding is combined with digital holographic principle to generate a phase-only pattern in CCD plane. In the second layer, multiple input images are individually encoded by using computer-generated hologram principle, and the generated phase-only holograms are further multiplied (synthesized) and compressed. Subsequently, the synthetic phase-only hologram is embedded into the previous phase-only pattern (i.e., generated by double random phase encoding) to produce the ciphertext (a noisy phase-only pattern). The computational results illustrate that two-layer optical information authentication method is effective and promising.

II. THEORETICAL ANALYSIS

In the first layer, double random phase encoding and digital holography are applied to extract a phase-only pattern in CCD plane, and a schematic setup is shown in Fig. 1. The first random phase-only mask is placed just behind the sparse input image, and the second phase-only mask is placed in spatial frequency domain. In this paper, fractional Fourier transform (FrFT) [2] is applied. Complex-valued wavefront in CCD plane is extracted by using digital holographic principle (such as off-axis or in-line) [1],[6],[15], and then only its phase part is maintained.

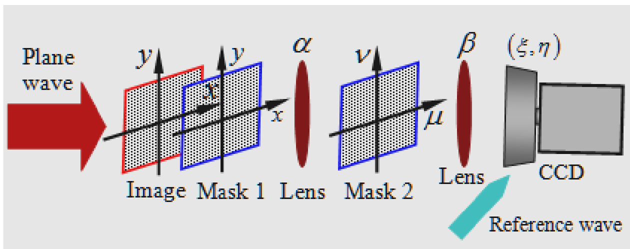


Figure 1. A schematic for optical encoding using double random phase encoding and digital holography in the FrFT domain. The input image is "Baboon" (http://sipi.usc.edu/database), and is sparse.

The encoding process at object wave path can be described by

$$O(\xi,\eta) = \mathrm{FrFT}_{\beta,\beta}\left(\left\{\mathrm{FrFT}_{\alpha,\alpha}\left[I(x,y)\mathrm{M1}(x,y)\right]\right\}\mathrm{M2}(\mu,\nu)\right), \quad (1)$$

where α and β denote FrFT function orders [2], $M1(x, y)$ and $M2(\mu, \nu)$ denote random phase-only masks, and $I(x, y)$ denotes a compressed input image. Here, only 2.0% pixels of the original image are randomly selected and maintained to be used as the input image $I(x, y)$. Optical methods, such as digital holography [1],[6],[15], can be applied to record intensity patterns, and complex-valued wavefront $O(\xi,\eta)$ in CCD plane is correspondingly extracted. Only phase part of the extracted complex-valued wavefront $O(\xi,\eta)$ is maintained, i.e., denoted as $P(\xi,\eta)$.

In the second layer, three input images (without compression) are independently encoded by using computer-generated hologram principle, and a schematic setup is shown in Fig. 2. An iterative method based on the modified Gerchberg-Saxton algorithm [8],[15] is applied to generate a phase hologram for each input image. Subsequently, the phase holograms are multiplied and compressed to generate a synthetic phase hologram $H(\xi,\eta)$. Finally, non-zero pixels of $H(\xi,\eta)$ replace the corresponding pixels of $P(\xi,\eta)$ to generate the ciphertext $C(\xi,\eta)$. In practice, the advanced hiding methods [16]–[20] may be applied instead of the direct replacement operation.

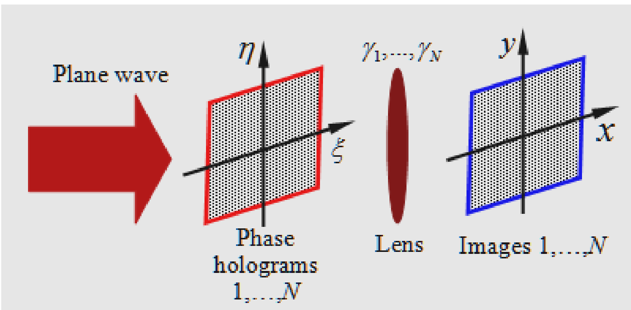
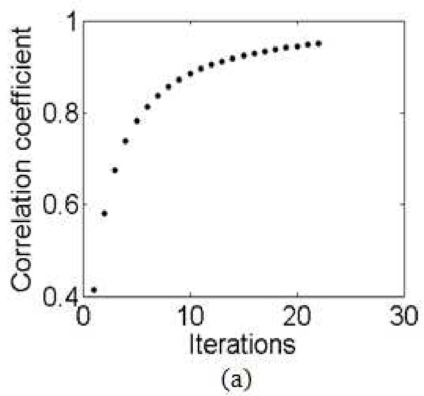


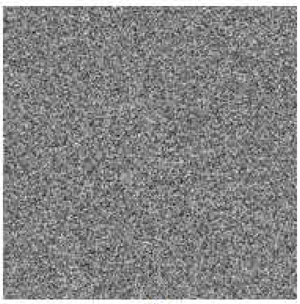
Figure 2. A schematic for optical encoding using computer-generated hologram principle in FrFT domain. The input images are "Barbara", "Airplane", and "Goldhill". During the decoding, the image plane is replaced by using a CCD camera. *N*=3.

During the decoding, the ciphertext $C(\xi,\eta)$ is directly applied for decoding the input image based on double random phase encoding system in the first layer. In the second layer, synthetic phase hologram $H(\xi,\eta)$ should be extracted from $C(\xi,\eta)$ by using the preset security keys (such as random position map), and then a compressed phase hologram corresponding to each input image is individually extracted for the decoding, such as using phase-hologram key. Since compressed input image or compressed phase hologram has been used, the decoded images are noisy and optical correlation approach [7]–[15] is implemented for information authentication.

III. RESULTS AND DISCUSSION

In the first layer, FrFT function orders α and β are 0.35 and 0.65, respectively. 2.0% pixels of original image (512×512 pixels) are randomly selected and maintained to be used as the input image $I(x, y)$. Plane wave is generated for the illumination, and two phase-only masks are randomly distributed in the range of [0, 2pi]. In the second layer, three input images (without compression) are individually encoded by using computer-generated hologram principle, and FrFT function orders ($\gamma_1, \gamma_2, \gamma_3$) are respectively set as 0.25, 0.55 and 0.80. A typically iterative process using computer-generated hologram is shown in Fig. 3(a). Only 25.0% pixels of each generated phase-only hologram (i.e., corresponding to each input image in Fig. 2) are randomly selected and maintained, and for simplicity the same random-position map is used. In practice, different compression percentages can be flexibly applied to process phase-only holograms for effective authentications. The generated ciphertext $C(\xi,\eta)$ (phase-only pattern) is shown in Fig. 3(b). It is seen in Fig. 3(b) that only one noisy phase-only pattern is generated as ciphertext. Some decoding and authentication results are shown in Figs. 4(a)–4(h), when correct security keys are used. It is illustrated that the decoded images are effectively authenticated in the two layers without information disclosure.





(b)

Figure 3. (a) A typically iterative process (threshold: correlation coefficient of 0.95), and (b) the ciphertext $C(\xi,\eta)$.

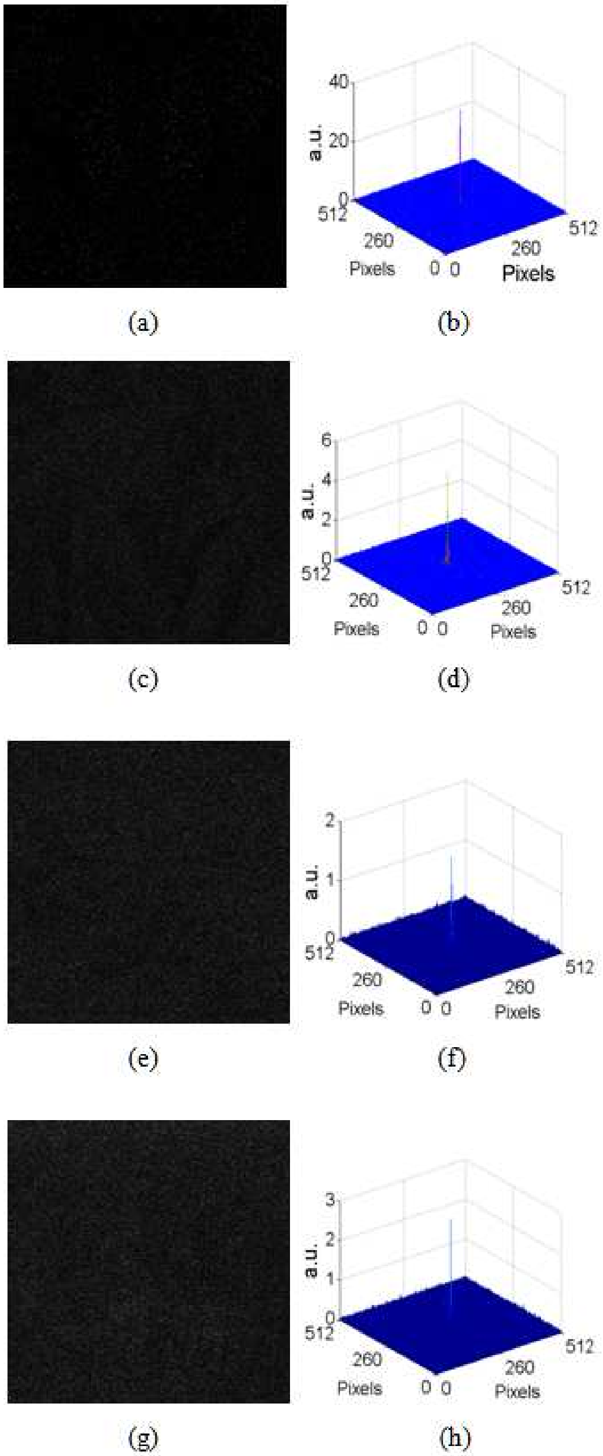


Figure 4. Decoding and authentication results: (a) an image decoded based on the setup in Fig. 1, and (b) authentication result. Three images decoded based on the setup in Fig. 2: (c), (e), (g) decoded images, and (d), (f), (h) the corresponding authentication results.

IV. CONCLUSIONS

Two-layer optical information authentication method has been presented by using hybrid optical encoding structures. Digital holographic structure (with double random phase encoding) and computer-generated hologram principle are used for the first-layer and second-layer optical information authentication, respectively. The numerical results demonstrate that the method is feasible and effective, and can provide an alternative for optical information authentication and optical security [1],[21]–[46].

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (NSFC) (Grant No. 61605165, 61575178), the Hong Kong Research Grants Council Early Career Scheme under Grant No. 25201416, Shenzhen Science and Technology Innovation Commission through Basic Research Program under Grant No. JCYJ20160531184426473, and The Hong Kong Polytechnic University (Fund No. 1-ZE5F).

REFERENCES

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20, pp. 767–769, 1995.

[2] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett., vol. 25, pp. 887–889, 2000.

[3] W. Chen and X. Chen, "Space-based optical image encryption," Opt. Express, vol. 18, pp. 27095–27104, 2010.

[4] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett., vol. 35, pp. 3817–3819, 2010.

[5] X. F. Meng, L. Z. Cai, X. F. Xu, X. L. Yang, X. X. Shen, G. Y. Dong, and Y. R. Wang, "Two-step phase-shifting interferometry and its application in image encryption," Opt. Lett., vol. 31, pp. 1414–1416, 2006.

[6] O. Matoba, T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," Proc. IEEE, vol. 97, pp. 1128–1148, 2009.

[7] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett., vol. 36, pp. 22–24, 2011.

[8] W. Chen, X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," IEEE Photon. J., vol. 5, pp. 6900113, 2013.

[9] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," J. Opt., vol. 16, pp. 025402, 2014.

[10] W. Chen, G. Situ, and X. Chen, "High-flexibility optical encryption via aperture movement," Opt. Express, vol. 21, pp. 24680–24691, 2013.

[11] W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett., vol. 38, pp. 546–548, 2013.

[12] W. Chen, "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," IEEE Photon. J., vol. 8, pp. 6900209, 2016.

[13] W. Chen and X. Chen, "Digital holography-secured scheme using only binary phase or amplitude as ciphertext," Appl. Opt., vol. 55, pp. 6740–6746, 2016.

[14] W. Chen and X. Chen, "Marked ghost imaging," Appl. Phys. Lett., vol. 104, pp. 251109, 2014.

[15] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon., vol. 6, pp. 120–155, 2014.

[16] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proc. IEEE, vol. 87, pp. 1062–1078, 1999.

[17] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no.12, pp. 1673–1687, Dec. 1997.

[18] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," IEE Electron. Lett., vol.38, no. 25, pp. 1646–1648, Dec. 2002.

[19] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Syst. J., vol. 35, no. 3–4, pp. 313–336, 1996.

[20] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding image watermarks in DC component," IEEE Trans. Circuits Syst.: Video Technol., vol. 10, no. 6, pp. 974–979, Sep. 2000.

[21] W. Chen, "Optical cryptosystem based on single-pixel encoding using the modified Gerchberg–Saxton algorithm with a cascaded structure," J. Opt. Soc. Am. A, vol. 33, pp. 2305–2311, 2016.

[22] W. Chen, "Correlated-photon secured imaging by iterative phase retrieval using axially-varying distances," IEEE Photon. Technol. Lett., vol. 28, pp. 1932–1935, 2016.

[23] W. Chen, "Optical data security system using phase extraction scheme via single-pixel detection," IEEE Photon. J., vol. 8, pp. 7801507, 2016.

[24] X. Wang, W. Chen, S. Mei, and X. Chen, "Optically secured information retrieval using two authenticated phase-only masks," Sci. Rep., vol. 5, pp. 15668, 2015.

[25] X. Wang, W. Chen, and X. Chen, "Optical encryption and authentication based on phase retrieval and sparsity constraints," IEEE Photon. J., vol. 7, pp. 7800310, 2015.

[26] X. Wang, W. Chen, and X. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," Opt. Express, vol. 23, pp. 6239–6253, 2015.

[27] X. Wang, W. Chen, and X. Chen, "Optical image hiding using double-phase retrieval algorithm based on nonlinear cryptosystem under vortex beam illumination," J. Opt., vol. 17, pp. 035704, 2015.

[28] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett., vol. 38, pp. 3198–3201, 2013.

[29] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," Opt. Lett., vol. 38, pp. 1425–1427, 2013.

[30] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using fractional Fourier transform," Opt. Eng., vol. 42, pp. 1583–1588, 2003.

[31] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," Opt. Express, vol. 18, pp. 12033–12043, 2010.

[32] P. Kumar, A. Kumar, J. Joseph, and K. Singh, "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," Opt. Lett., vol. 34, pp. 331–333, 2009.

[33] L. Chen and D. Zhao, "Optical image encryption with Hartley transforms," Opt. Lett., vol. 31, pp. 3438–3440, 2006.

[34] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt. Laser Technol., vol. 57, pp. 327–342, 2014.

[35] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon., vol. 1, pp. 589–636, 2009.

[36] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett., vol. 31, pp. 1044–1046, 2006.

[37] N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun., vol. 284, pp. 735–739, 2011.

[38] T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A, vol. 25, pp. 2608–2617, 2008.

[39] 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, vol. 17, pp. 22462–22473, 2009.

[40] S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography," Opt. Lett., vol. 28, pp. 167–169, 2003.

[41] B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett., vol. 25, pp. 28–30, 2000.

[42] B. Javidi and A. Sergent, "Fully phase encoded key and biometrics for security verification," Opt. Eng., vol. 36, pp. 935–942, 1997.

[43] G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett., vol. 30, pp. 1306–1308, 2005.

[44] O. Matoba and B. Javidi, "Encrypted optical memory systems based on multidimensional keys for secure data storage and communications," IEEE Circ. Dev. Mag., vol. 16, pp. 8–15, 2000.

[45] X. Wang, D. Zhao, F. Jing, and X. Wei, "Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics," Opt. Express, vol. 14, pp. 1476–1486, 2006.

[46] W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on Arnold transform and interference method," Opt. Commun., vol. 282, pp. 3680–3685, 2009.