This is the Pre-Published Version.

The following publication W. Chen, "Three-Dimensional Optical Correlation Based on Binary Computer-Generated Hologram," 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), Cairns, QLD, Australia, 2018, pp. 1340-1343 is available at https://doi.org/10.1109/ISIE.2018.8433733.

Three-Dimensional Optical Correlation Based on Binary Computer-Generated Hologram

Wen Chen[1,2]

[1]The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China

[2]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China

Email: owen.chen@polyu.edu.hk

***Abstract*—In this paper, three-dimensional (3D) optical correlation is presented based on binary computer-generated hologram. The 2D input image is divided into some squared blocks, which are placed in 3D space. These blocks are encoded into a phase-only pattern, and the generated phase pattern is further binarized. It is numerically illustrated that high security can be achieved in the system, and decryption result using only one axial position does not contain sufficient information for correct correlation. It is also demonstrated that the binary phase-only pattern can be flexibly generated for the decoding. The 3D optical correlation based on binary computer-generated hologram can effectively enrich 3D optical security area.**

Keywords—optical correlation; binary computer-generated hologram; 3D space; phase retrieval

I. INTRODUCTION

Optical security [1]–[13] has attracted much attention in recent years, since optics possesses some remarkable characteristics (such as parallel processing). Since Refregier and Javidi [1] proposed double random phase encoding technique, optical encryption has been widely studied. Various transform domains [2]–[11] have been used, and various infrastructures [2]–[13], such as asymmetric structure [12],[13], have been designed and applied in optical security systems. Although attack algorithms [14],[15] can be applied to extract phase keys in double random phase encoding, some corresponding approaches [3],[5],[16] are also applicable for security enhancement. For instance, it is illustrated in Ref. [16] that phase key in spatial frequency domain can be continuously updated to make it against the attacks.

Pérez-Cabré et al. [17] developed a method using photon-counting approach to compress complex-valued wavefront in double random phase encoding system. It is demonstrated that the decoded image can be correctly verified without information visualization [17]. It was also found that phase retrieval and ghost imaging [18]–[27] can be applied for optical information authentication. Recently, 3D optical correlation [28] has been further proposed, and it was demonstrated that system security could be enhanced (i.e., compared with previous works). However, it is desirable that more alternatives can be developed to enhance the flexibility.

In this paper, 3D optical correlation is presented based on binary computer-generated hologram. The 2D input image is divided into some squared blocks, which are placed in 3D space. These blocks are encoded into a phase-only pattern, and the generated phase pattern is further binarized. It is illustrated that high security can be achieved in the system, and decryption result using only one axial position does not contain sufficient information for a correct correlation. It is also demonstrated that the binary phase-only pattern can be flexibly generated for the decoding. The 3D optical correlation based on binary computer-generated hologram can effectively enrich 3D optical security area.

II. PRINCIPLES

Figure 1 shows a schematic setup for 3D optical correlation based on binary computer-generated hologram. The collimated plane wave is generated for the illumination, and the encoding process is conducted based on an iterative approach between spatial space and reciprocal space. Here, the 2D input image is divided into some squared blocks which are placed in 3D space [23],[28]–[31]. Each block contains some neighboring pixels of the input image. During the iterative retrieval, some data, such as the input image placed in 3D space and a series of axial distances, are applied as known parameters, and the encoding objective is to generate an approximated phase-only pattern.

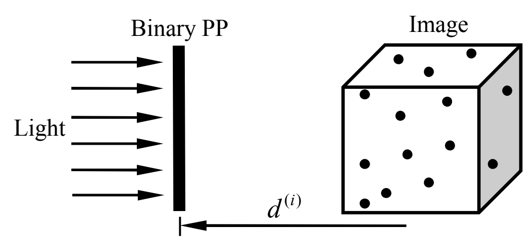


Fig. 1. A schematic setup for 3D optical correlation based on binary computer-generated hologram: PP, phase-only pattern; *i*, block index (1,2,3,……,*K*); *d*, axial distance.

The iterative encoding process is described as follows:

(i) Symbol *i* (1,2,3,……,*K*) is used to denote the series of squared blocks, and each block contains 16×16 neighboring pixels of the input image. Each block is placed at a random axial position. In the initial stage, a random phase-only pattern (in a range of [0, 2pi]) is used as a guess, i.e., denoted as $M^{(i,n)}(\mu,\nu)$. Symbol *n* denotes the iteration number, and (μ,ν) denotes coordinate for the phase-only pattern plane.

(ii) Wave propagation is conducted between the phase pattern plane and the image plane.

$$O(\xi,\eta) = \mathrm{WP}_{d^{(i)}}\left[M^{(i,n)}(\mu,\nu)\right], \tag{1}$$

where WP denotes free-space wave propagation [32], $d^{(i)}$ denotes the axial distance, and $O(\xi,\eta)$ denotes complex-valued wavefront in the image plane. The symbol (ξ,η) denotes coordinate for the input image plane.

(iii) A constraint [28],[30] is applied in the image plane for updating the complex-valued wavefront $O(\xi,\eta)$ using a specific block (i.e., within the block *i*) to generate an updated complex-valued wavefront $O'(\xi,\eta)$.

(iv) Subsequently, back propagation process is conducted by:

$$O^{(i,n)}(\mu,\nu) = \mathrm{WP}_{-d^{(i)}}\left[O'(\xi,\eta)\right], \tag{2}$$

where $O^{(i,n)}(\mu,\nu)$ denotes the wavefront in phase-only pattern plane. Hence, an updated phase-only pattern can be generated by using a constraint [33]–[35].

$$\hat{M}^{(i,n)}(\mu,\nu) = \frac{O^{(i,n)}(\mu,\nu)}{\left|O^{(i,n)}(\mu,\nu)\right|}, \tag{3}$$

where | | denotes a modulus operation, and $\hat{M}^{(i,n)}(\mu,\nu)$ denotes the updated phase-only pattern.

(v) The updated phase-only pattern is further used, and the steps (ii)–(iv) are repeatedly applied. After all blocks (i.e., *i*=*K*) are processed, a preset threshold is used to judge whether the iterative process can be stopped. If the threshold cannot be satisfied, the updated phase-only pattern is further used for the next iteration, i.e., *n*=*n*+1. When a new iteration starts, the block symbol *i* should be reset as 1. If the threshold can be satisfied, the finally generated phase-only pattern is denoted as $M(\mu,\nu)$.

(vi) Finally, an average value of $angle[M(\mu,\nu)]$ (where *angle* denotes phase extraction) can be calculated and used as a threshold for the binarization, hence a binary phase distribution can be correspondingly generated as ciphertext, i.e., $M_b(\mu,\nu)$. In practice, a coefficient or factor can be multiplied by the calculated average value to be employed as a threshold for the binarization operation.

For the decoding, binary phase-only pattern and setup parameters are applied. A decoded image $\hat{I}(\xi,\eta)$ can be obtained by [28],[30],[31]

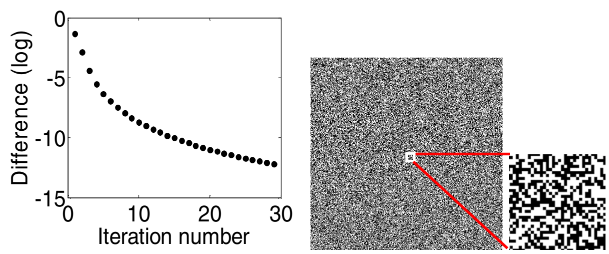
$$\hat{I}(\xi,\eta) = \underset{(\xi,\eta)}{\Im}\left(\underset{(\xi,\eta)}{\Re}\left\{\left|\mathrm{WP}_{d^{(i)}}\left[M_b(\mu,\nu)\right]\right|^2\right\}\right), \tag{4}$$

where $\Re$ denotes selection operation in transverse domain [28], and $\Im$ denotes incorporation operation in transverse domain [28]. When the series of axial distances $d^{(i)}$ is available, a CCD camera can be axially translated to sequentially record a series of intensity patterns during the decoding. Here, nonlinear correlation algorithm [17]–[28] is applied to verify the decoded image $\hat{I}(\xi,\eta)$ by correlating with the original input image $I(\xi,\eta)$ which is stored in a separated database [18].

III. Results and discussion

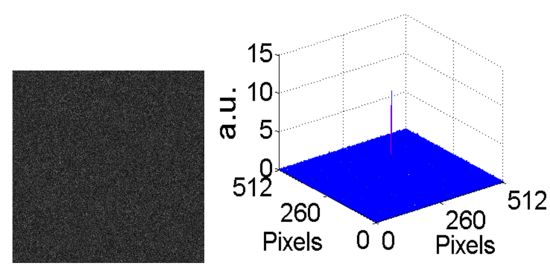
The schematic setup in Fig. 1 is computationally conducted to verify the validity. The plane wave with wavelength of 630.0 nm is applied for the illumination, and a recording device with 512×512 pixels and $4.65\mu m$ pixel size can be used. During the encoding, a binary phase-only pattern is generated as ciphertext, and an average value of $angle[M(\mu,\nu)]$ is calculated and used as a threshold. The series of axial distances $d^{(i)}$ is randomly distributed in a range of [6.0 cm, 15.0 cm]. Here, grayscale image "Baboon" (http://sipi.usc.edu/database/) is used as an input image.

Figure 2(a) shows a relationship between the number of iterations and the calculated difference (logarithm scale) during the encoding. The threshold is set as 0.000005. It can be seen that only 29 iterations are needed, and a rapid convergence rate can be achieved in the iterative process. Figure 2(b) shows a generated binary phase-only pattern which is used as ciphertext. When an authorized receiver uses correct ciphertext and security keys, a decoded image is obtained in Fig. 3(a). Due to the designed strategy no information can be visually observed, and a correlation distribution is generated in Fig. 3(b). It is illustrated that the decoded image in Fig. 3(a) can be effectively verified.



(a) (b)

Fig. 2. (a) A relationship between the number of iterations and the calculated difference (logarithm scale) during the encoding, and (b) the generated binary phase-only pattern. A small area has been enlarged to clearly show some information in the ciphertext.



(a) (b)

Fig. 3. (a) A decoded image obtained when correct ciphertext and security keys are used, and (b) the corresponding correlation distribution. The correlation coefficient (CC) for (a) is 0.0354.

Performance of system parameters is further analyzed. When only the binary phase-only pattern is wrongly used during the decoding, a decoded image is shown in Fig. 4(a). The corresponding correlation distribution is generated in Fig. 4(b). When only the wavelength contains an error of 2.0 nm during the decoding, a decoded image is shown in Fig. 4(c). The corresponding correlation distribution is generated in Fig.

4(d). When only the series of axial distances is wrong during the decoding, a decoded image is shown in Fig. 4(e). The corresponding correlation distribution is generated in Fig. 4(f). When the decoding process is conducted by using only an axial position (i.e., 10.0 cm) during the decoding, a decoded image is shown in Fig. 4(g). The corresponding correlation distribution is generated in Fig. 4(h). The CC values for Figs. 4(a), 4(c), 4(e) and 4(g) are -0.0021, 0.0056, -0.0004 and 0.0012, respectively. It is illustrated in Figs. 4(b), 4(d), 4(f) and 4(h) that when security keys or ciphertext are not correctly applied, only noisy nonlinear correlation maps can be generated.

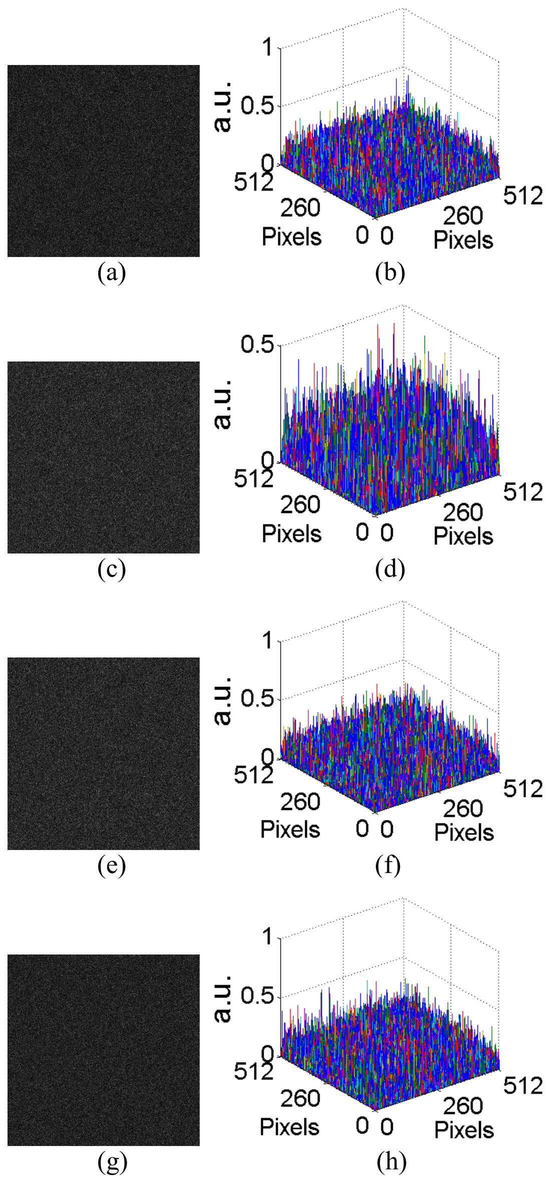


Fig. 4. (a) A decoded image obtained when only the binary phase-only pattern is wrongly used, and (b) the corresponding correlation distribution. (c) A decoded image obtained when only the wavelength is wrong (error of 2.0 nm) during the decoding, and (d) the corresponding correlation distribution. (e) A decoded image obtained when only the series of axial distances is wrong during the decoding, and (f) the corresponding correlation distribution. (g) A decoded image obtained when the decoding process is conducted by using only one axial position (i.e., 10.0 cm), and (h) the corresponding correlation distribution.

In this study, the binarization operation can be flexibly implemented. The average value of $angle[M(\mu,v)]$ can be further multiplied by a factor, such as 1.5, 1.9 and 0.5. The multiplication result can be used as a threshold for the binarization operation to generate binary phase. When correct ciphertext and security keys are used, a decoded image is obtained in Fig. 5(a). In this case, a factor of 1.5 is used to be multiplied by the calculated average value to generate a threshold for the binarization operation, and other parameters are set as the same as those used for Figs. 3(a) and 3(b). The corresponding correlation distribution is generated as shown in Fig. 5(b). When the multiplication factor is respectively set as 1.9 and 0.5, the decryption results and correlation distributions are correspondingly obtained in Figs. 5(c)–5(f). It can be seen in Figs. 5(b), 5(d) and 5(f) that the decoded images can also be correctly verified.

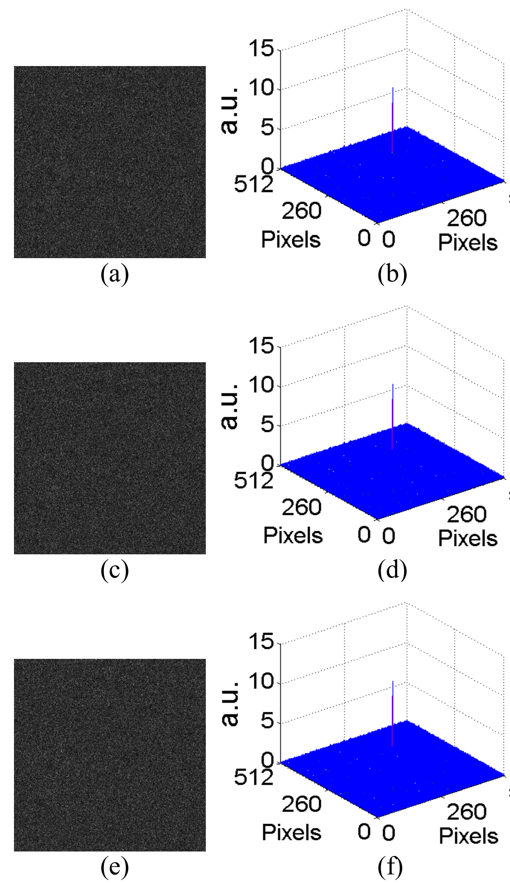


Fig. 5. Multiplication factor of 1.5: (a) a decoded image obtained when correct ciphertext and security keys are used, and (b) the corresponding correlation distribution. Multiplication factor of 1.9: (c) a decoded image obtained when correct ciphertext and security keys are used, and (d) the corresponding correlation distribution. Multiplication factor of 0.5: (e) a decoded image obtained when correct ciphertext and security keys are used, and (f) the corresponding correlation distribution.

IV. CONCLUSIONS

The 3D optical correlation has been presented based on binary computer-generated hologram. It is numerically illustrated that high security can be achieved in the system, and the sectional decryption does not generate sufficient information for a correct correlation. It is also demonstrated that the binary phase-only pattern can be flexibly generated for the decoding and correlation. The 3D optical correlation based on binary computer-generated hologram can effectively enrich 3D optical security area.

ACKNOWLEDGEMENTS

This work was supported by the National Natural Science Foundation of China (NSFC) (61605165), Hong Kong Research Grants Council Early Career Scheme (25201416), Shenzhen Science and Technology Innovation Commission (JCYJ20160531184426473), and The Hong Kong Polytechnic University (4-BCDY, G-YBVU, 4-ZZHM and 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] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express vol. 14, pp. 8552–8560, 2006.

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

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

[6] H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett. vol. 34, pp. 3917–3919, 2009.

[7] Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. vol. 33, pp. 2443–2445, 2008.

[8] 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.

[9] 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.

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

[11] W. Chen, "Modulating phase via rotation for optical encoding based on correlated photon imaging," IEEE Photon. Technol. Lett. vol. 28, pp. 540–543, 2016.

[12] W. Liu, Z. Liu, and S. Liu, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm," Opt. Lett. vol. 38, pp. 1651–1653, 2013.

[13] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. vol. 35, pp. 118–120, 2010.

[14] A. Carnicer, M. M. Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. vol. 30, pp. 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. vol. 31, pp. 1044–1046, 2006.

[16] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express vol. 15, pp. 10253–10265, 2007.

[17] 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.

[18] W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL (Europhysics Letters) vol. 110, pp. 44002 (5pp), 2015.

[19] W. Chen and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," Opt. Lasers Eng. vol. 73, pp. 123–127, 2015.

[20] 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.

[21] W. Chen and X. Chen, "Marked ghost imaging," Appl. Phys. Lett. vol. 104, pp. 251109 (5pp), 2014.

[22] W. Chen and X. Chen, "Optical color-image verification using multiple-pinhole phase retrieval," J. Opt. vol. 16, pp. 075403 (12pp), 2014.

[23] W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. vol. 103, pp. 221106 (4pp), 2013.

[24] 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.

[25] W. Chen, "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," IEEE Photon. J. vol. 8, pp. 6900209 (9pp), 2016.

[26] 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 (9pp), 2015.

[27] 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.

[28] W. Chen, "3D Gerchberg-Saxton optical correlation," IEEE Photon. J. vol. 10, pp. 7800409 (9pp), 2018.

[29] W. Chen and X. Chen, "Optical cryptography network topology based on 2D-to-3D conversion and phase-mask extraction," Opt. Lasers Eng. vol. 51, pp. 410–416, 2013.

[30] W. Chen and X. Chen, "Interference-based optical image encryption using three-dimensional phase retrieval," Appl. Opt. vol. 51, pp. 6076–6083, 2012.

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

[32] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York, McGraw-Hill, 1996.

[33] R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of phase from image and diffraction plane pictures," Optik (Stuttgart) vol. 35, pp. 237–246, 1972.

[34] J. R. Fienup, "Phase retrieval algorithms: a comparison," Appl. Opt. vol. 21, pp. 2758–2769, 1982.

[35] W. Chen, "Computer-generated hologram using binary phase with an aperture," Appl. Opt. vol. 56, pp, 9126–9131, 2017.