Computer-Generated Hologram Authentication via Optical Correlation

Wen Chen
Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
E-mail: owen.chen@polyu.edu.hk

***Abstract*-Computer-generated hologram (CGH) has attracted much attention over the past decades, and has been widely applied in many areas, such as display, security and optical tweezer. In this paper, CGH-based authentication approach is presented by using optical correlation. After the original image is sparsified, phase-only mask is iteratively extracted as ciphertext based on CGH system. It is illustrated that the decoded information can be effectively and correctly authenticated by using optical correlation.**

I. INTRODUCTION

In recent years, optical security technologies [1]–[9] have been widely studied, since optical means possesses some remarkable advantages, such as parallel processing and multiple-dimensional. Since double random phase encoding [1] was proposed, a number of infrastructures and algorithms [5],[10]–[15] have been developed and integrated into optical security systems. Although some optical security systems are vulnerable to the attacks [16] due to the inherent linearity property, the designed attack algorithms are usually developed and applied by using strong assumptions, such as the same keys for encoding different plaintexts. Hence, when the keys can be easily updated, system security would be dramatically enhanced.

In optical encoding field, computer-generated hologram (CGH) [17]–[24] provides a promising tool for securing information. In CGH system, an object or input data/image can be iteratively or non-iteratively encoded into phase-only or amplitude-only masks. Since the extracted mask information can be embedded into spatial light modulator for optical decoding, it can facilitate practical applications, such as ID and packaging checking. The CGH encoding is usually conducted by using an iterative approach between real and reciprocal spaces. For instance, Gerchberg-Saxton algorithm [25] is one of the most popular phase extraction algorithms, which has been applied for optical security. Hwang and Chang et al. [20] proposed a modified Gerchberg-Saxton algorithm and phase modulation approach for optical encoding. Xiao et al. [21] proposed an improved encoding approach for optical encryption based on cascaded phase retrieval approach. Zhang and Wang [22] further developed a novel method by using non-iterative interference to extract two phase-only masks as ciphertexts.

Recently, authentication with photon-counting imaging [26] has been developed as an alternative for security enhancement, and a combination of photon-counting optical encryption [26] and decoded-information authentication [5],[27]–[32] can be considered as a new approach for optical security. However, sparse complex-valued wavefront in the CCD plane [26] should be extracted and applied for the decoding and authentication, which may enhance the difficulty to optically implement.

In this paper, CGH-based authentication is presented by using optical correlation. The original image is sparsified before the encoding, and phase-only mask is iteratively extracted as ciphertext based on CGH system. It is found that there is a potential to implement the decoding process by using a fully-optical means, and the decoded image can be effectively authenticated by using optical correlation approach.

II. THEORETICAL ANALYSIS

During the encoding, the collimated plane wave is generated for the illumination, and light wavelength is 632.8nm. Here, two separated and different cases are studied: (1) only one extracted phase-only mask M1 as shown in Fig. 1(a), and (2) one fixed phase-only mask M1 and one extracted phase-only mask M2 as shown in Fig. 1(b).

In the first case, the input image is sparsified before the encoding, and the sparsified input image is denoted as $\tilde{P}(\mu,\nu)$. A CGH-based approach, i.e., an iterative phase retrieval algorithm, is applied to iteratively encode the sparsified input image into phase-only mask M1. Objective of input-image encoding is to find the approximate phase-only mask M1 under the given constraints [27], such as the sparsified input image and setup parameters. In the initial iteration, phase-only mask M1 is initialized to be randomly distributed in a range of $[0, 2\pi]$, and $M_1^{(n)}(\xi,\eta)$ is used to denote phase-only mask M1 at the nth iteration (n=1,2,3,……). Complex-valued wavefront $O^{(n)}(\mu,\nu)$ in the input image plane is described by

$$O^{(n)}(\mu,\nu)=\mathrm{FrT}_{\lambda,d_1}\left[M_1^{(n)}(\xi,\eta)\right], \tag{1}$$

where λ is light wavelength, d_1 denotes axial distance between phase-only mask (M1) plane and the input image plane, and FrT denotes free-space wave propagation [33].

After complex-valued wavefront is obtained in the input image plane, a constraint [5],[27] is applied as follows:

$$\hat{O}^{(n)}(\mu,\nu)=\left[\tilde{P}(\mu,\nu)\right]^{1/2} O^{(n)}(\mu,\nu)/\left|O^{(n)}(\mu,\nu)\right|, \quad (2)$$

where $\hat{O}^{(n)}(\mu,\nu)$ denotes the updated complex-valued wavefront in the input image plane, and | | denotes modulus operation. Finally, the updated phase-only mask M1 $\left[\text{i.e., } \hat{M}_1^{(n)}(\xi,\eta)\right]$ can be obtained by [5],[27]

$$\hat{M}_1^{(n)}(\xi,\eta)=\frac{\mathrm{FrT}_{\lambda,-d_1}\left[\hat{O}^{(n)}(\mu,\nu)\right]}{\left|\mathrm{FrT}_{\lambda,-d_1}\left[\hat{O}^{(n)}(\mu,\nu)\right]\right|}, \quad (3)$$

where $\mathrm{FrT}_{\lambda,-d_1}$ denotes wave back-propagation [33].

In this case, correlation coefficient [5],[27] is calculated between the intermediately decoded image and the sparse input image $\tilde{P}(\mu,\nu)$ to monitor the iterative process. If the calculated correlation coefficient is smaller than a preset threshold (i.e., 0.996), the updated phase-only mask $\hat{M}_1^{(n)}(\xi,\eta)$ is further used for the next iteration (i.e., n=n+1). Otherwise, phase-only mask M1 can be determined and denoted as $M_1(\xi,\eta)$.

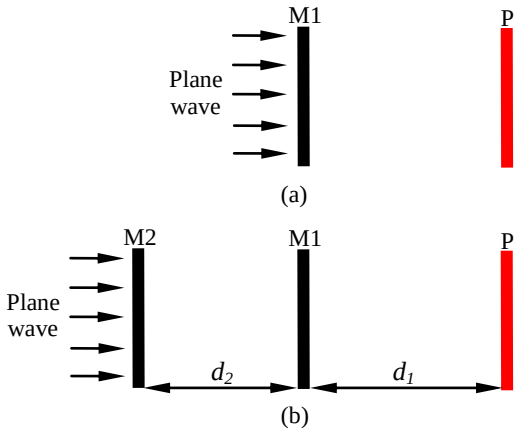

Fig. 1. Schematic setup for CGH-based encoding and decoding with (a) only one phase-only mask (i.e., the first case) and (b) two phase-only masks (i.e., the second case): M, phase-only mask; P, the sparse input image. The plane wave can be generated by combining a pinhole and a lens. During the encoding, the sparse image location is considered as input plane, and phase-only mask locations are the output planes. During the decoding, the sparse image can be replaced by a detector as output plane, and phase-only mask locations are considered as input planes.

In the second case, the input image is also sparsified before the encoding, and the sparsified input image is denoted as $\tilde{P}(\mu,\nu)$. A CGH-based approach, i.e., an iterative phase retrieval algorithm, is applied to iteratively encode the sparsified input image into phase-only mask M2, and one additional phase-only mask M1 is pre-defined and randomly distributed in a range of $[0, 2\pi]$. Objective of input-image encoding is to find an approximate phase-only mask M2 under some given constraints, such as the fixed phase-only mask M1, the sparsified input image and setup parameters. In the initial iteration, the phase-only mask M2 is initialized to be randomly distributed in a range of $[0, 2\pi]$, and $M_2^{(n)}(x,y)$ is used to denote phase-only mask M2 at the nth iteration (n=1,2,3,……). Complex-valued wavefront $O^{(n)}(\mu,\nu)$ in the input image plane is described by [5],[27]

$$O^{(n)}(\mu,\nu)=\mathrm{FrT}_{\lambda,d_1}\left(\left\{\mathrm{FrT}_{\lambda,d_2}\left[M_2^{(n)}(x,y)\right]\right\}M_1(\xi,\eta)\right), \quad (4)$$

where d_2 denotes axial distance between phase-only mask (M2) plane and phase-only mask (M1) plane, and $M_1(\xi,\eta)$ denotes the pre-defined and fixed phase-only mask M1 used in the second case.

After complex-valued wavefront is obtained in the input image plane, a constraint is applied as follows [5],[27]:

$$\hat{O}^{(n)}(\mu,\nu)=\left[\tilde{P}(\mu,\nu)\right]^{1/2} O^{(n)}(\mu,\nu)/\left|O^{(n)}(\mu,\nu)\right|. \quad (5)$$

Finally, the updated phase-only mask M2 $\left[\text{i.e., } \hat{M}_2^{(n)}(x,y)\right]$ can be obtained by [27]

$$\hat{M}_2^{(n)}(x,y)=\frac{\mathrm{FrT}_{\lambda,-d_2}\left(\left\{\mathrm{FrT}_{\lambda,-d_1}\left[\hat{O}^{(n)}(\mu,\nu)\right]\right\}\left[M_1(\xi,\eta)\right]^*\right)}{\left|\mathrm{FrT}_{\lambda,-d_2}\left(\left\{\mathrm{FrT}_{\lambda,-d_1}\left[\hat{O}^{(n)}(\mu,\nu)\right]\right\}\left[M_1(\xi,\eta)\right]^*\right)\right|}, \quad (6)$$

where asterisk denotes complex conjugate, and $\mathrm{FrT}_{\lambda,-d_2}$ denotes wave back-propagation [33].

In this case, correlation coefficient is also calculated to monitor the iterative process. If the calculated correlation coefficient is smaller than a preset threshold (i.e., 0.996), the updated phase-only mask $\hat{M}_2^{(n)}(x,y)$ is further used for the next iteration (i.e., n=n+1). Otherwise, phase-only mask M2 can be determined and denoted as $M_2(x,y)$. Here, it has been further analyzed that additional phase-only masks, such as M1, can be placed in the designed CGH-based system to enhance system security, and these additional phase-only masks may act as security keys rather than ciphertexts. It is worth noting that the first and second cases are independent.

In the first case, the decoding process can be conducted by using optical means, and is described by

$$\tilde{P}'(\mu,\nu)=\left|\mathrm{FrT}_{\lambda,d_1}\left[M_1(\xi,\eta)\right]\right|^2, \quad (7)$$

where $\tilde{P}'(\mu,\nu)$ denotes a decoded input image.

In the second case, the decoding process can also be conducted by using optical means, and is described by

$$\tilde{P}'(\mu,\nu)=\left|\mathrm{FrT}_{\lambda,d_1}\left(\left\{\mathrm{FrT}_{\lambda,d_2}\left[M_2(x,y)\right]\right\}M_1(\xi,\eta)\right)\right|^2. \quad (8)$$

Since only few data of the original image $P(\mu,\nu)$ are used as the input, the decoded image just renders noisy information. Here, optical correlation [5],[26],[27],[31] is applied to authenticate the decoded image as follows:

$$C(\mu,\nu)=\left|\mathrm{IFT}\left(\left[\mathrm{FT}(P)\right]\left\{\left[\mathrm{FT}\left(\tilde{P}'\right)\right]\right\}^{*}\left|\left[\mathrm{FT}(P)\right]\left\{\left[\mathrm{FT}\left(\tilde{P}'\right)\right]\right\}^{*}\right|^{w-1}\right)\right|^2, \quad (9)$$

where w denotes strength of applied nonlinearity [5],[26],[27],[31], $C(\mu,\nu)$ denotes the generated correlation

map, and FT and IFT denote Fourier transform and inverse Fourier transform, respectively. For the sake of brevity, only a flow chart for the second case is further illustrated in Fig. 2.

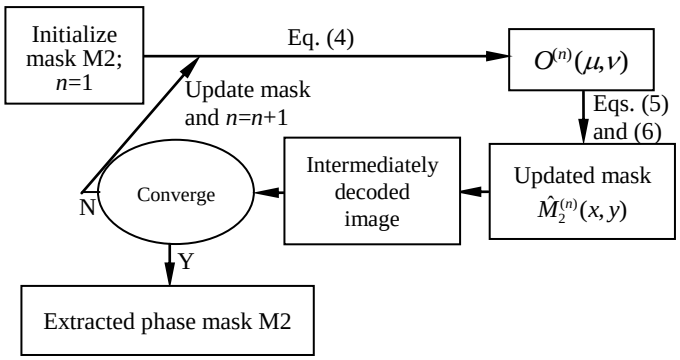

Fig. 2. Flow chart for illustrating the encoding process in the second case.

III. RESULTS AND DISCUSSION

The setups shown in Figs. 1(a) and 1(b) are numerically conducted to show the feasibility and effectiveness of CGH-based authentication method. The plane wave is generated to illustrate phase-only mask M1 in Fig. 1(a) or phase-only mask M2 in Fig. 1(b), and the light wavelength is 632.8 nm. The axial distances d_1 and d_2 are 20.0 mm and 30.0 mm, respectively. The original image as shown in Fig. 3(a) is sparsified, and 98.0% of the pixels in the original image $P(\mu,\nu)$ are set as zero. The generated sparse input image $\tilde{P}(\mu,\nu)$ is shown in Fig. 3(b). During the decoding, a CCD camera (512×512 pixels and pixel size of $4.65\,\mu m$) can be used to record the decoded image.

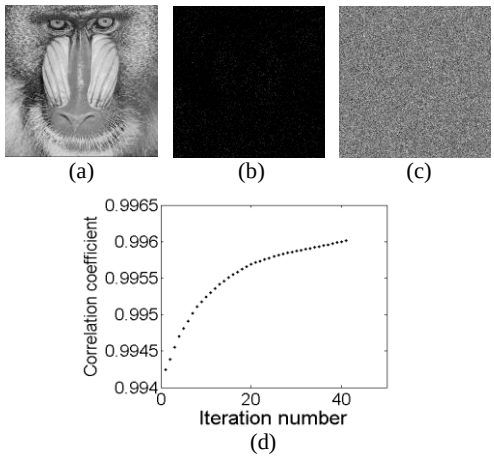

Fig. 3. (a) The original image $P(\mu,\nu)$, (b) the sparse input image $\tilde{P}(\mu,\nu)$, (c) the extracted phase-only mask M1, and (d) a relationship between the iteration number and correlation coefficients during the encoding.

In the first case, the iterative phase retrieval algorithm is applied to extract phase-only mask M1 under the given parameters, such as wavelength, distance and the sparse input image. The extracted phase-only mask M1 is shown in Fig. 3(c). It can be seen in Fig. 3(c) that the sparse input image is fully encoded, and the obtained phase-only mask is noisy. This extracted phase-only mask can be considered as ciphertext, which is stored or transmitted to the receiver. To show the iterative process, a relationship between the iteration number and correlation coefficients is shown in Fig. 3(d). Only 41 iterations are requested, and a rapid convergence rate is achieved during the encoding.

In the first case, when all parameters and mask are correctly applied during the decoding, a decoded image is obtained in Fig. 4(a). Since only few data of the original image $P(\mu,\nu)$ have been used during the encoding, only noise-like image can be obtained during the decoding. Here, the decoded image is further authenticated, and the generated correlation output is shown in Fig. 4(d). It can be seen in Fig. 4(d) that only one remarkable peak is obtained, which means the decoded image being correctly verified. In other words, it can also be verified that the receiver is an authorized one. Performance of some parameters is further analyzed. Figure 4(b) shows a decoded image, when only axial distance d_1 is incorrectly applied (with an error of 2.0 mm) during the decoding. Figure 4(e) shows a generated correlation output corresponding to Fig. 4(b). Figure 4(c) shows a decoded image, when only light wavelength is incorrectly applied (with an error of 15.0 nm) during the decoding. Figure 4(f) shows a generated correlation output corresponding to Fig. 4(c). It can be seen in Figs. 4(e) and 4(f) that when setup parameters are wrongly used during the decoding, the generated authentication outputs are noisy.

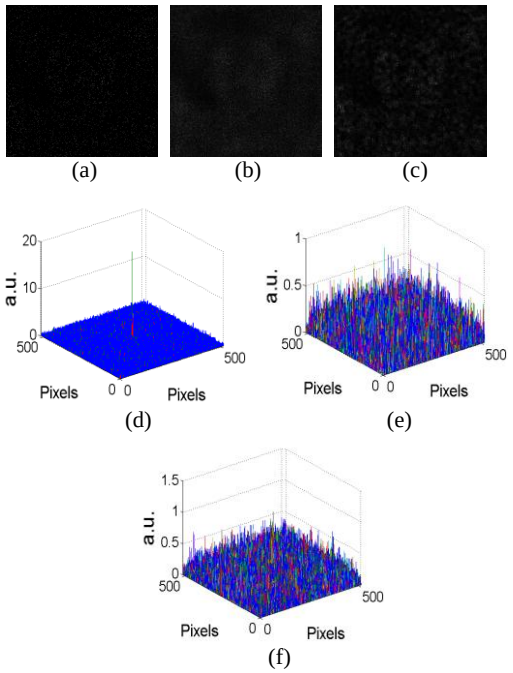

Fig. 4. (a) A decoded image obtained when all parameters and mask are correctly applied, (b) a decoded image obtained when only axial distance d_1 is wrong during the decoding, (c) a decoded image obtained when only light wavelength is wrong during the decoding, and (d)–(f) the generated authentication outputs respectively corresponding to (a)–(c).

In the second case, the iterative phase retrieval algorithm is applied to extract phase-only mask M2 under the given parameters, such as wavelength, distance, fixed phase-only mask M1 and sparse input image. The fixed phase-only mask M1 is shown in Fig. 5(a), and the extracted phase-only mask M2 is shown in Fig. 5(b). It can be seen in Fig. 5(b) that the sparse input image $\tilde{P}(\mu,\nu)$ is fully encoded, and the extracted phase-only mask is noisy. To show the iterative process, a relationship between the iteration number and correlation coefficients is shown in Fig. 5(c). Only 34 iterations are requested, and a rapid convergence rate is achieved during the encoding.

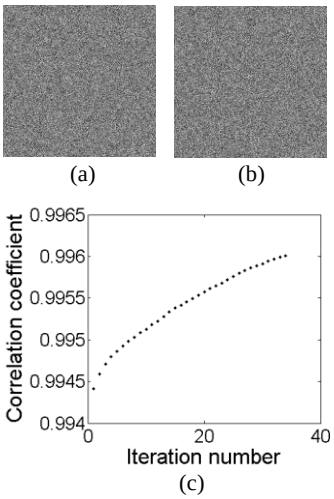

Fig. 5. (a) The fixed phase-only mask M1, (b) the extracted phase-only mask M2, and (c) a relationship between the iteration number and correlation coefficients during the encoding.

In the second case, when all parameters and masks are correctly applied during the decoding, a decoded image is obtained in Fig. 6(a). Since only few data of the original image $P(\mu,\nu)$ have been used during the encoding, only noise-like image can be obtained during the decoding. Here, the decoded image is further authenticated, and the generated correlation output is shown in Fig. 6(e). It can be seen in Fig. 6(e) that only one remarkable peak is obtained, which means the decoded image being correctly verified. Performance of some parameters and masks is further analyzed. Figure 6(b) shows a decoded image, when only axial distance d_2 is incorrectly applied (with an error of 2.0 mm) during the decoding. Figure 6(f) shows a generated correlation output corresponding to Fig. 6(b). Figure 6(c) shows a decoded image, when only phase-only mask M1 is incorrectly employed during the decoding. Figure 6(g) shows a generated correlation output corresponding to Fig. 6(c). Figure 6(d) shows a decoded image, when only phase-only mask M2 is incorrectly used during the decoding. Figure 6(h) shows a generated correlation output corresponding to Fig. 6(d). It can be seen in Figs. 6(f)–6(h) that when setup parameters or masks are wrongly used during the decoding, the generated authentication outputs are noisy.

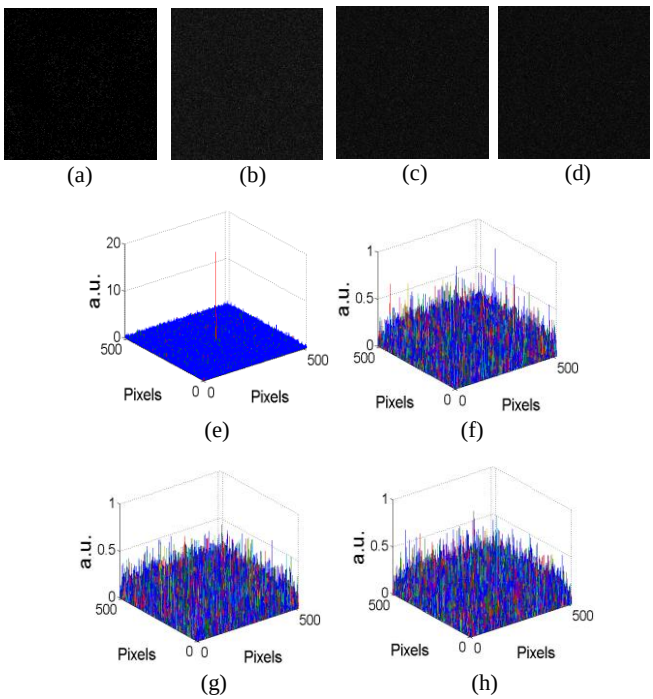

Fig. 6. (a) A decoded image obtained when all parameters and masks are correctly applied, (b) a decoded image obtained when only axial distance d_2 is wrong during the decoding, (c) a decoded image obtained when only phase-only mask M1 is wrong during the decoding, (d) a decoded image obtained when only phase-only mask M2 is wrong during the decoding, and (e)–(h) the generated authentication outputs respectively corresponding to (a)–(d).

IV. CONCLUSIONS

The CGH-based authentication has been presented by using optical correlation. The original image is sparsified before the encoding, and phase-only mask is iteratively extracted as ciphertext based on CGH system. The decoding process can be optically implemented, since spatial light modulator can be applied. The simulation results demonstrate that the decoded image can be effectively and accurately authenticated by using optical correlation algorithm. In addition, performance of system parameters and masks has also been illustrated, and the authentication method presented here generates an additional security protection scheme over conventional CGH-based encoding approach.

ACKNOWLEDGMENT

This work was supported by the startup grant (1-ZE5F) from The Hong Kong Polytechnic University.

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] B. Javidi, "Securing information with optical technologies," *Phys. Today*, vol. 50, pp. 27–32, 1997.

[3] 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.

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

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

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

[8] W. Chen, "Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification," *Appl. Opt.*, vol. 54, pp. 10711–10716, 2015.

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

[10] 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.

[11] 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.

[12] A. Alfalou and C. Brosseau, "Dual encryption scheme of images using polarized light," *Opt. Lett.*, vol. 35, pp. 2185–2187, 2010.

[13] J. Liu, X. Xu, Q. Wu, J. T. Sheridan, and G. Situ, "Information encryption in phase space," *Opt. Lett.*, vol. 40, pp. 859–862, 2015.

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

[15] 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.

[16] 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.

[17] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.*, vol. 35, pp. 2464–2469, 1996.

[18] Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," *Appl. Opt.*, vol. 39, pp. 5295–5301, 2000.

[19] E. G. Johnson and J. D. Brasher, "Phase encryption of biometrics in diffractive optical elements," *Opt. Lett.*, vol. 21, pp. 1271–1273, 1996.

[20] 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.

[21] Y. L. Xiao, X. Zhou, S. Yuan, Q. Liu, and Y. C. Li, "Multiple-image optical encryption: an improved encoding approach," *Appl. Opt.*, vol. 48, pp. 2686–2692, 2009.

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

[23] P.W.M. Tsang, Y. T. Chow, and T. C. Poon, "Generation of phase-only Fresnel hologram based on down-sampling," *Opt. Express*, vol. 22, pp. 25208–25214, 2014.

[24] P.W.M. Tsang and T. C. Poon, "Fast generation of digital holograms based on warping of the wavefront recording plane," *Opt. Express*, vol. 23, pp. 7667–7673, 2015.

[25] 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.

[26] 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.

[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 (13pp), 2013.

[28] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *J. Opt.*, vol. 16, pp. 025402 (7pp), 2014.

[29] W. Chen, X. Wang, and X. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," *J. Opt.*, vol. 17, pp. 035702 (12pp), 2015.

[30] 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 (10pp), 2015.

[31] F. Sadjadi and B. Javidi, *Physics of the Automatic Target Recognition* (Springer, Berlin, 2007).

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

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