Digital holography-secured scheme using only binary phase or amplitude as ciphertext

WEN CHEN[1,*] AND XUDONG CHEN[2]

[1]*Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China*
[2]*Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore*
**Corresponding author: owen.chen@polyu.edu.hk*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

A digital holography-secured scheme is presented by using binary phase or amplitude. The input image is encrypted based on double random phase encoding (DRPE), and complex-valued wavefront in the CCD plane is extracted by using digital holography. Subsequently, only phase component of the extracted complex-valued wavefront is maintained, and is further binarized. Different from conventional methods, an interesting finding in this paper is that in addition to binary phase, binary amplitude originating from the binarized phase pattern can also be applied as ciphertext. During optical decoding, the decrypted image cannot visually render clear information about the input, and the authentication is further conducted. Binary phase or amplitude pattern can be flexibly applied as ciphertext, and the fully optical approach can be implemented for the decoding. The ciphertext is effectively compressed, which can facilitate the storage and transmission in practical applications. © 2016 Optical Society of America

OCIS codes: *(200.4740) Optical processing; (090.1995) Digital holography; (100.5090) Phase-only filters.*

http://dx.doi.org/10.1364/AO.99.099999

1. INTRODUCTION

Since double random phase encoding (DRPE) [1] was proposed by Refregier and Javidi, optical encryption technologies have attracted more and more attention. In DRPE, two statistically-independent random phase-only masks are respectively placed in input plane and spatial frequency plane, and stationary white noise can be generated as ciphertext [1]. Until now, a number of optical principles and configurations [2–8], such as holography [2] and ghost imaging [8], have been developed for optical security.

In recent years, some optical encryption systems are proven vulnerably to attack algorithms [9,10] due to the inherent linearity property, and attack algorithms, such as known-plaintext attack [9] and chosen-ciphertext attack [10], can be applied to approximately extract phase-only masks. To eliminate the vulnerability, security enhancement approaches [11–15] are further developed. Qin and Peng [11] proposed to integrate nonlinear structure into DRPE using phase truncation scheme, and the generated decryption keys are related to the input image. Frauel et al. [12] proposed effective methods to enhance system security, such as updating the encoding keys. Pérez-Cabré et al. [14] combined DRPE and photon-counting imaging for optical encoding and authentication. In Ref. [14], the decoded image can be verified, and complex-valued wavefront in the CCD plane is still requested. It is desirable that ciphertext can be further compressed, and phase or amplitude component of complex-valued wavefront in the CCD plane is applied as ciphertext for the fully optical decoding.

In this paper, a digital holography-secured scheme is presented by using binary phase or amplitude. The input image is encrypted by using DRPE, and complex-valued wavefront in the CCD plane is extracted by using digital holography. Subsequently, only phase component of the extracted complex-valued wavefront is maintained, and is further binarized to be applied as ciphertext. Different from conventional methods, an interesting finding in this study is that in addition to binary phase, binary amplitude originating from the binarized phase pattern can also be applied as ciphertext. During optical decoding, the decrypted image cannot visually render clear information related to the input, and the authentication can be further conducted. An additional security layer may be established in the proposed optical security system, and ciphertext is effectively compressed.

2. THEORETICAL ANALYSIS

Figure 1 shows a schematic setup for the proposed digital holography-secured scheme. The laser, with wavelength of 630.0 nm, is collimated by combination of a pinhole and a lens, and is divided into two separated beams, i.e., object beam and reference beam. Statistically-independent random phase-only masks M1 and M2 with complex transmittances $\exp[j M_1(\mu,\nu)]$ and $\exp[j M_2(\xi,\eta)]$ (where $j=\sqrt{-1}$) are placed at object wave path, and piezoelectric transducer (PZT) can be used to modulate phase shifts at reference wave path. Symbols (μ,ν) and (ξ,η) respectively denote coordinates of input image plane and phase-only mask (M2) plane, and random phase-only mask M1 is placed just behind the input image $I(\mu,\nu)$.

Object wave in the CCD plane can be described by

$$O'(x,y)=\mathrm{FrT}_{\lambda,d_2}\left\{\left(\mathrm{FrT}_{\lambda,d_1}\left\{I(\mu,\nu)\exp\left[jM_1(\mu,\nu)\right]\right\}\right)\exp\left[jM_2(\xi,\eta)\right]\right\}, \quad (1)$$

where (x,y) denotes coordinate of CCD plane, $O'(x,y)$ denotes object wavefront in the CCD plane, d_1 and d_2 denote axial distances, λ denotes

light wavelength, and FrT denotes free-space wave propagation [16]. To describe free-space wave propagation process, paraxial or small-angle approximation can be applied, and convolution method [2,16] can also be carried out. Here, object wavefront in the CCD plane is described by

$$O'(x,y)=\left\{\left\{I(\mu,\nu)\exp\left[jM_1(\mu,\nu)\right]\right\}\otimes\Im(\mu,\nu;d_1)\right)\exp\left[jM_2(\xi,\eta)\right]\Big\}\otimes\Im(\xi,\eta;d_2), \tag{2}$$

where $\otimes$ stands for convolution, and $\Im(\mu,\nu;d_1)$ and $\Im(\xi,\eta;d_2)$ are point pulse functions respectively described by

$$\Im(\mu,\nu;d_1)=\frac{\exp(j2\pi d_1/\lambda)}{jd_1\lambda}\exp\left[\frac{j\pi}{d_1\lambda}(\mu^2+\nu^2)\right], \tag{3}$$

$$\Im(\xi,\eta;d_2)=\frac{\exp(j2\pi d_2/\lambda)}{jd_2\lambda}\exp\left[\frac{j\pi}{d_2\lambda}(\xi^2+\eta^2)\right]. \tag{4}$$

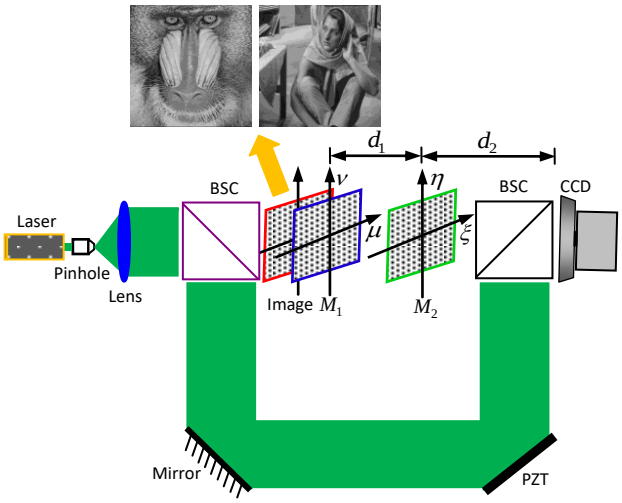

Fig. 1. A schematic setup for the digital holography-secured scheme using binary phase or amplitude: BSC, beam splitter cube; CCD, charge-coupled device; PZT, piezoelectric transducer for phase shifting; *M*, random phase-only mask; d_1 and d_2, axial distances. Random phase-only mask M1 is placed just behind the input image. Here, all input images are normalized before the encoding.

In-line digital holography [2,17] is applied here, and three digital holograms $H_i(x,y)$ can be obtained by using a CCD camera via the interference between object wave $O'(x,y)$ and phase-shifted reference wave $R_i(x,y)$.

$$H_i(x,y)=\left[O'(x,y)+R_i(x,y)\right]\left[O'(x,y)+R_i(x,y)\right]^*, \tag{5}$$

where integer $i=1,2$ and 3, and asterisk denotes complex conjugate. The in-line digital holograms are sequentially obtained, when phase shift of the reference wave is respectively set as 0, $\pi/2$ and π. Object wavefront in the CCD plane can be extracted by [17,18]

$$O(x,y)=\frac{1-j}{4}\left\{H_1(x,y)-H_2(x,y)+j\left[H_2(x,y)-H_3(x,y)\right]\right\}, \tag{6}$$

where $O(x,y)$ denotes object wavefront extracted in the CCD plane. In this study, the plane wave is applied at reference path, and amplitude of reference wave is considered as one. The extracted complex-valued object wavefront $O(x,y)$ is further described by $A(x,y)\exp[jP(x,y)]$, where $A(x,y)$ denotes amplitude component and $\exp[jP(x,y)]$ denotes phase component.

Here, the extracted object wavefront $A(x,y)\exp[jP(x,y)]$ is compressed, and only phase component $\exp[jP(x,y)]$ is maintained. Subsequently, the phase component is binarized, and binarization process can be described by

$$P_b(x,y)=\begin{cases}1 & \text{if } P(x,y)\geq Ave\left[P(x,y)\right]\\ 0 & \text{if } P(x,y)<Ave\left[P(x,y)\right]\end{cases}, \tag{7}$$

where $P_b(x,y)$ denotes a binary map, and *Ave* denotes an average value. Finally, the binary phase pattern $\exp[jP_b(x,y)]$ [here the phase values are of 0 and 1] is applied as ciphertext and transmitted to the receiver. It will also be illustrated that binary amplitude, i.e., $P_b(x,y)$, can be applied as ciphertext. This finding can enhance application flexibility of the proposed optical security scheme.

For the decoding, the fully optical approach can be implemented, since binary phase or amplitude pattern can be employed as ciphertext. When the ciphertext, i.e., binary phase or amplitude pattern, is available, the decoding process can be respectively implemented by

$$\hat{I}(\mu,\nu)=\left|\mathrm{FrT}_{\lambda,-d_1}\left(\left(\mathrm{FrT}_{\lambda,-d_2}\left\{\exp\left[jP_b(x,y)\right]\right\}\right)\left\{\exp\left[jM_2(\xi,\eta)\right]\right\}^*\right)\right|, \tag{8}$$

$$\hat{I}(\mu,\nu)=\left|\mathrm{FrT}_{\lambda,-d_1}\left(\left\{\mathrm{FrT}_{\lambda,-d_2}\left[P_b(x,y)\right]\right\}\left\{\exp\left[jM_2(\xi,\eta)\right]\right\}^*\right)\right|, \tag{9}$$

where $\hat{I}(\mu,\nu)$ denotes a decoded image, symbol || denotes modulus operation, and $\mathrm{FrT}_{\lambda,-d_1}$ and $\mathrm{FrT}_{\lambda,-d_2}$ denote back propagation [16]. Since binary phase or amplitude is applied as ciphertext, the decoded image will not visually render clear information related to the input and information authentication is further conducted for establishing an additional security layer for the proposed optical security scheme. The decoded image is verified by using nonlinear correlation [2,14,19–30]:

$$C(\mu,\nu)=\left|\mathrm{IFT}\left(\left|\left\{\mathrm{FT}\left[\hat{I}(\mu,\nu)\right]\right\}\left\{\mathrm{FT}\left[I(\mu,\nu)\right]\right\}^*\right|^{w-1}\left\{\mathrm{FT}\left[\hat{I}(\mu,\nu)\right]\right\}\left\{\mathrm{FT}\left[I(\mu,\nu)\right]\right\}^*\right)\right|^2, \tag{10}$$

where $C(\mu,\nu)$ denotes the generated nonlinear correlation distribution, *w* denotes strength of applied nonlinearity [2,14,19–30], and FT and IFT denote Fourier transform and inverse Fourier transform, respectively. Original input images can be stored in a separated database [2,20,21], and only an interface is accessible to the receiver for conducting the authentication operation without observation of the complete input images [2,14,20–30]. Various parameters in standard correlation outputs can be defined and stored in the database to further enhance the security, such as via the comparison in the authentication step. To further illustrate the proposed method aforementioned, a flow chart is given in Fig. 2.

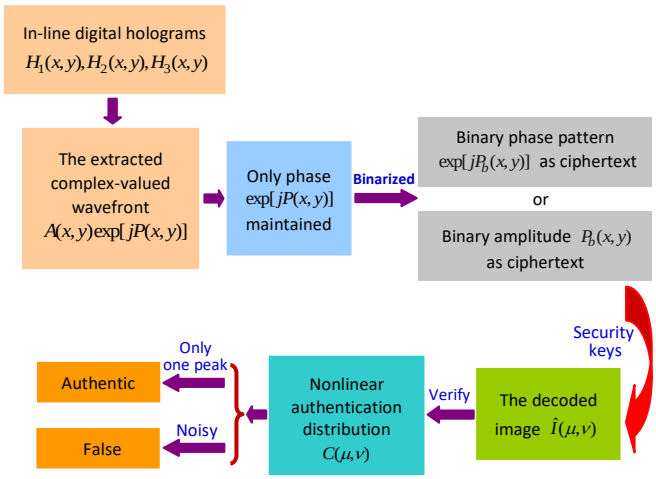

Fig. 2. Flow chart for illustrating optical encryption, decryption and authentication process.

3. RESULTS AND DISCUSSION

Figure 1 shows a schematic setup for the proposed digital holography-secured scheme using binary phase or amplitude pattern, and numerical simulations are conducted. The collimated plane wave with wavelength of 630.0 nm is applied for the illumination. Statistically-independent random phase-only masks M1 and M2, with 512×512 pixels, are placed at object wave path, and phase values are randomly distributed in the range of $[0, 2\pi]$. Axial distances d_1 and d_2 are 5.0 cm and 8.0 cm, respectively. At reference wave path, phase shift is sequentially set as 0, $\pi/2$ and π. Three digital holograms can be obtained by using a CCD camera (512×512 pixels and pixel size of 4.65 microns) as shown in Figs. 3(a)–3(c). An input image called "Baboon" (512×512 pixels, http://sipi.usc.edu/database) is used and shown in Fig. 1. When the wave propagation conditions [16] are satisfied, different sizes (such as 256×256 pixels) of input images can also be applied and encoded by using the proposed scheme. In practice, the input image with small size can be enlarged by numerical methods before the encoding. The proposed scheme is more suitable for optically authenticating grayscale image (such as also with a normalization operation) rather than binary image. Here, the input images are normalized before the encoding. Object wavefront $A(x,y)\exp[jP(x,y)]$ is extracted in the CCD plane, and amplitude component $A(x,y)$ and phase component $\exp[jP(x,y)]$ are shown in Figs. 3(d) and 3(e), respectively. In the proposed optical security system, phase component is maintained, and its binarized form is further generated as ciphertext and shown in Fig. 3(f). To clearly show the binarization operation, an inset has been given to illustrate an enlarged part of Fig. 3(f). In this study, it is found that either binary phase pattern $\exp[jP_b(x,y)]$ or binary amplitude $P_b(x,y)$ can be applied as ciphertext.

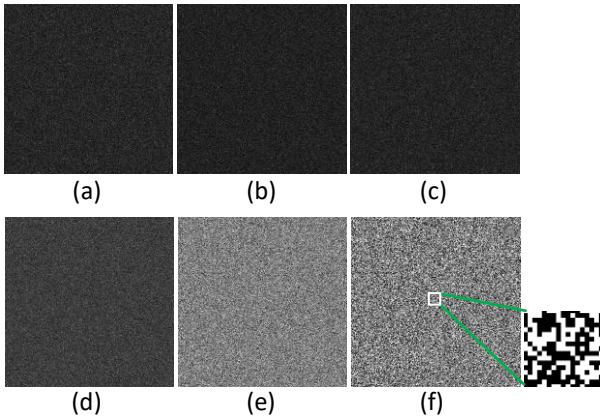

Fig. 3. (a)–(c) Three holograms obtained when phase shift at reference wave path is (a) 0, (b) $\pi/2$ and (c) π, (d) amplitude component $A(x,y)$, (e) phase component $\exp[jP(x,y)]$, and (f) binary phase as ciphertext. An inset is given to clearly illustrate binarization operation.

When binary phase pattern $\exp[jP_b(x,y)]$ [here the phase values are binary] is applied as ciphertext, a decoded image as shown in Fig. 4(a) is obtained by using correct keys. Correlation coefficient (CC) and mean squared error (MSE) [2,5,22] for Fig. 4(a) are 0.0384 and 0.3471, respectively. It can be seen in Fig. 4(a) that since only binary phase pattern is employed as ciphertext, information related to the input image cannot be visually rendered. Here, optical information authentication [2,14,20–29] is further conducted, and nonlinear authentication distribution corresponding to Fig. 4(a) is shown in Fig. 4(e). It can be seen in Fig. 4(e) that only one remarkable peak can be observed at the center of the generated nonlinear authentication output, which means the decoded image being authentic. In the proposed optical security system, setup parameters, such as phase-only mask M2, wavelength and distances, are considered as keys. Performance of system keys is further analyzed. Figure 4(b) shows a decoded image, when only the random phase-only mask M2 is incorrectly used for the decoding. CC and MSE values for Fig. 4(b) are 0.0040 and 0.3545, respectively. Figure 4(f) shows a nonlinear authentication distribution corresponding to Fig. 4(b). Figure 4(c) shows a decoded image, when only the wavelength contains an error of 1.0 nm during the decoding. CC and MSE values for Fig. 4(c) are 0.0059 and 0.3528, respectively. Figure 4(g) shows nonlinear authentication distribution corresponding to Fig. 4(c). It can be seen in Figs. 4(f) and 4(g) that only noisy background is generated. It is also indicated that the receiver does not have correct keys, and the receiver is not an authorized person. For the sake of brevity, performance of other keys, such as distances, is not presented here. Since ciphertext should be stored or transmitted to the receiver, it may be contaminated, such as by noise. Figure 4(d) shows a decoded image, when the ciphertext is contaminated by additive white Gaussian noise (zero mean noise with 0.06 variance). In this case, noisy ciphertext $\exp[jP'_b(x,y)]$ is applied for the decoding, where $P'_b(x,y)$ denotes the values after noise contamination. In Fig. 4(d), all keys are correctly applied, and CC and MSE values for Fig. 4(d) are 0.0361 and 0.3475, respectively. Figure 4(h) shows nonlinear authentication distribution corresponding to Fig. 4(d). It can be seen in Fig. 4(h) that high robustness against contamination is achieved in the proposed optical security scheme.

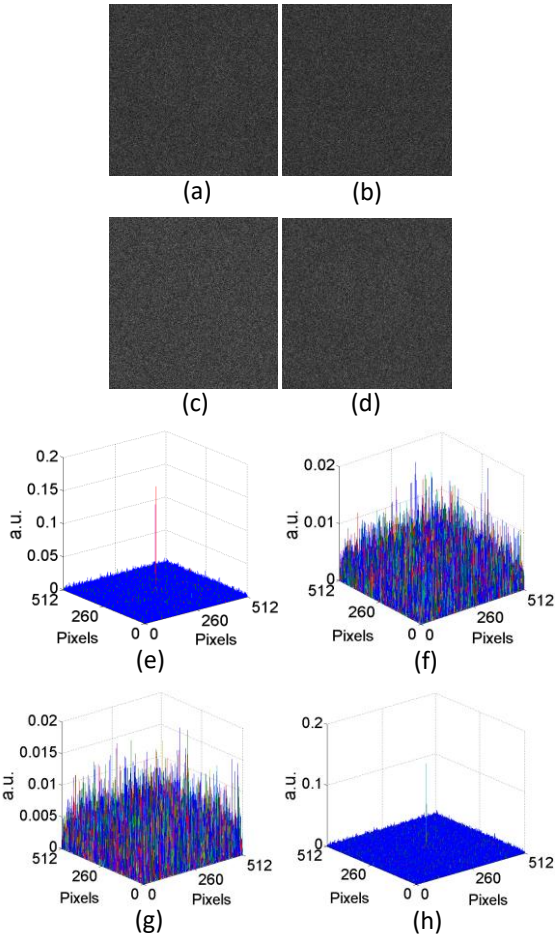

Fig. 4. Binary phase pattern $\exp[jP_b(x,y)]$ as ciphertext: (a) a decoded image obtained by using correct security keys, (b) a decoded image obtained when only the random phase-only mask M2 is incorrectly used for the decoding, (c) a decoded image obtained when only the wavelength contains an error of 1.0 nm during the decoding, (d) a decoded image obtained when the ciphertext is contaminated by additive white Gaussian noise (zero mean noise with 0.06 variance), and (e)–(h) nonlinear authentication distributions respectively corresponding to (a)–(d).

When binary amplitude $P_b(x,y)$ is applied as ciphertext, the proposed optical security scheme is also feasible. A decoded image is obtained as shown in Fig. 5(a), when all security keys are correctly applied (such as by authorized receiver). CC and MSE values for Fig. 5(a) are 0.0888 and 0.1340, respectively. It can be seen in Fig. 5(a) that since only binary amplitude is employed as ciphertext, information related to the input image cannot be

visually rendered. Nonlinear authentication distribution corresponding to Fig. 5(a) is shown in Fig. 5(e). It can be seen in Fig. 5(e) that only one remarkable peak is observed, and the proposed method is effective by using binary amplitude $P_b(x,y)$ as ciphertext. In practice, the input image can be compressed (i.e., some pixels set as zeros) without loss of major information before the encoding to further enhance invisibility of the decoded images, when binary amplitude $P_b(x,y)$ is applied as ciphertext. Performance of security keys is further analyzed. Figure 5(b) shows a decoded image, when only random phase-only mask M2 is incorrectly used for the decoding. CC and MSE values for Fig. 5(b) are -0.0018 and 0.1460, respectively. Figure 5(f) shows a nonlinear authentication distribution corresponding to Fig. 5(b). Figure 5(c) shows a decoded image, when only the wavelength contains an error of 1.0 nm during the decoding. CC and MSE values for Fig. 5(c) are 0.0164 and 0.1438, respectively. Figure 5(g) shows nonlinear authentication distribution corresponding to Fig. 5(c). It can be seen in Figs. 5(f) and 5(g) that noisy background is also generated, when security keys are wrong for the decoding. Figure 5(d) shows a decoded image, when the ciphertext $P_b(x,y)$ is contaminated by additive white Gaussian noise (zero mean noise with 0.06 variance). In Fig. 5(d), all security keys are correctly applied, and CC and MSE values for Fig. 5(d) are 0.0791 and 0.1539, respectively. Figure 5(h) shows a nonlinear authentication distribution corresponding to Fig. 5(d). It can be seen in Fig. 5(h) that high robustness against contamination can also be achieved, when amplitude $P_b(x,y)$ is applied as ciphertext. It has been illustrated that either binary phase or binary amplitude can be applied as ciphertext for optical decoding and authentication. This finding can enhance system flexibility in practical applications.

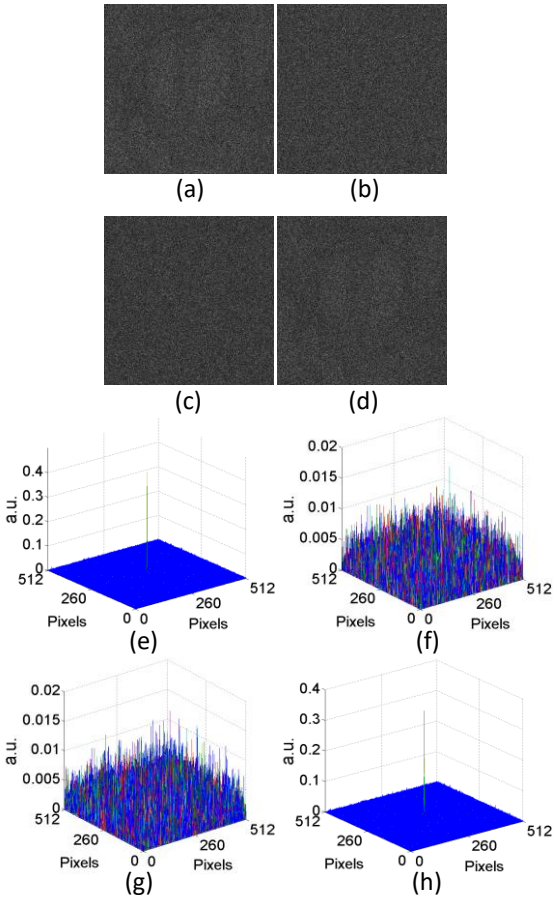

Fig. 5. Binary amplitude $P_b(x,y)$ as ciphertext: (a) a decoded image obtained by using correct keys, (b) a decoded image obtained when only random phase-only mask M2 is wrongly used for the decoding, (c) a decoded image obtained when only the wavelength contains an error of 1.0 nm during the decoding, (d) a decoded image obtained when ciphertext $P_b(x,y)$ is contaminated by additive white Gaussian noise (zero mean noise with 0.06 variance), and (e)–(h) nonlinear authentication distributions respectively corresponding to (a)–(d).

It is worth noting that when amplitude component $A(x,y)$ [see Eq. (6)] of the extracted object wavefront $A(x,y)\exp[jP(x,y)]$ is binarized as $A_b(x,y)$ to be applied as ciphertext, the decoded image cannot be correctly authenticated by using the proposed method. In this case, it is not possible to apply the proposed decoding and authentication process for producing correct verification outputs. When all keys are correctly applied and binary amplitude $A_b(x,y)$ is applied as ciphertext, a decoded image is obtained as shown in Fig. 6(a). The CC and MSE values for Fig. 6(a) are -0.002 and 0.1334, respectively. Nonlinear authentication distribution corresponding to Fig. 6(a) is shown in Fig. 6(b). It can be seen in Fig. 6(b) that only noisy background is obtained in the generated authentication distribution, when $A_b(x,y)$ is applied as ciphertext. In this case, although the proposed method here cannot be applied to produce the correct verification output, an iterative phase retrieval algorithm [23] might be studied and applied to extract a decode image for the authentication. Various parameters generated from the standard correlation outputs may be pre-defined and stored in the database to further enhance system security. However, as seen in Figs. 4 and 5, either binary phase-only pattern $\exp[jP_b(x,y)]$ or binary amplitude $P_b(x,y)$ can be applied as ciphertext for the proposed method, hence it is indicated that the phase $\exp[jP(x,y)]$ plays a more important role than the amplitude $A(x,y)$ in this application (i.e., using the proposed method via direct back-propagation for optical decryption implementation). This phenomenon is consistent with those observed in other studies [31–33].

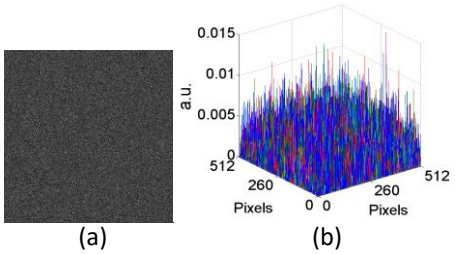

Fig. 6. Binary amplitude $A_b(x,y)$ as ciphertext: (a) a decoded image obtained by using correct keys, and (b) nonlinear authentication distribution corresponding to (a).

Discrimination capability of the proposed optical security system is further analyzed, when different images are also encoded by using the optical setup in Fig. 1. Another input image (i.e., "Barbara" with 512×512 pixels, from http://sipi.usc.edu/database) is encoded. Figure 7(a) shows a decoded image, when all security keys are correctly applied for the decoding. In this case, the parameters are the same as those used for Fig. 4(a). The phase pattern $\exp[jP_b(x,y)]$ is applied as ciphertext. Figure 7(b) shows a nonlinear authentication distribution obtained between the original input image (i.e., "Baboon") and the decoded image in Fig. 7(a). It can be seen in Fig. 7(b) that only noisy authentication distribution is obtained, and discrimination capability of the proposed method is guaranteed. Figure 7(c) shows a decoded image, when all keys are correctly applied for the decoding and binary amplitude $P_b(x,y)$ is applied as ciphertext. In this case, the input image "Barbara" is encoded, and all other parameters are the same as those used for Fig. 5(a). Figure 7(d) shows nonlinear authentication distribution obtained between the original input image (i.e., "Baboon") and the decoded image in Fig. 7(c). It is demonstrated that discrimination capability can also be guaranteed, when binary amplitude $P_b(x,y)$ is applied as ciphertext. A number of tests have been done by using a series of different input images for analyzing discrimination capability, and the proposed optical scheme can always work well. To clearly show the evaluation results for the decoded images, the CC and MSE values are further shown in Table 1.

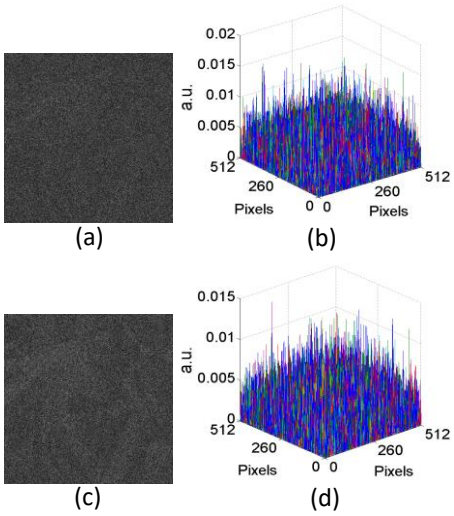

Fig. 7. Discrimination capability test: when binary phase pattern $\exp[jP_b(x,y)]$ is used as ciphertext, (a) a decoded image obtained by using correct keys and (b) nonlinear authentication distribution obtained between the original input image (i.e., "Baboon") and that in (a). When binary amplitude pattern $P_b(x,y)$ is used as ciphertext, (c) a decoded image obtained by using correct keys and (d) nonlinear authentication distribution obtained between the original input image (i.e., "Baboon") and that in (c).

Table 1. The CC and MSE values for the decrypted images

	CC value	MSE value		CC value	MSE value
Fig. 4(a)	0.0384	0.3471	Fig. 5(c)	0.0164	0.1438
Fig. 4(b)	-0.0040	0.3545	Fig. 5(d)	0.0791	0.1539
Fig. 4(c)	0.0059	0.3528	Fig. 6(a)	-0.0020	0.1334
Fig. 4(d)	0.0361	0.3475	Fig. 7(a)	0.0528	0.4152
Fig. 5(a)	0.0888	0.1340	Fig. 7(c)	0.1137	0.1551
Fig. 5(b)	-0.0018	0.1460			

Performance of the proposed method and comparison to previous work are briefly described as follows:

(1) The main objective and the developed method in this study are different from those in Ref. [4]. The work in Ref. [4] focuses on high-quality image decoding, and our study focuses on optical decoded-image authentication. Binary pattern is generated by using real and imaginary parts of CCD-plane complex data in Ref. [4], hence the original input image can be largely recovered. Different from that in Ref. [4], phase information of complex data in CCD plane is maintained and binarized in this study. Hence, the decoded images are generated without the disclosure of large original information, and do not visually render clear information about the input image.

(2) When original information is visually rendered during the decoding, the input image can be first compressed before the encoding. When the decoded image does not contain sufficient information for the verification, the modified ciphertext, such as $A(x,y)\exp[jP_b(x,y)]$, can be applied for the decoding and verification. For instance, when the image "Lena" (with 512×512 pixels, from http://sipi.usc.edu/database) is used as an input and binary amplitude $P_b(x,y)$ is applied as ciphertext, the decoded images and authentication distributions are obtained in Figs. 8(a)–8(d). The results in Figs. 8(a) and 8(b) are obtained when the input image is not compressed before the encoding, and the results in Figs. 8(c) and 8(d) are obtained when only 5.0% pixels of the input image are randomly selected and maintained (others are set as zero) before the encoding. It can be seen that a little silhouette about the input image might be observed in Fig. 8(a), and no useful information about the input image can be visually rendered in Fig. 8(c). The decoded image in Fig. 8(c) can still be effectively verified as illustrated in Fig. 8(d).

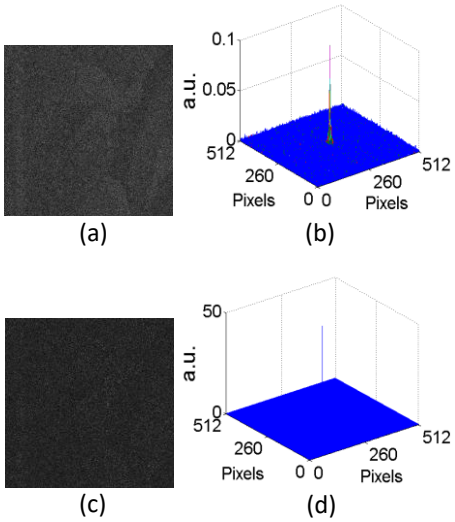

Fig. 8. The image "Lena" is used as an input and binary amplitude $P_b(x,y)$ is applied as ciphertext. No compression of the input image before the encoding: (a) a decoded image using correct keys, and (b) the corresponding authentication distribution. Compression of the input image (only 5.0% pixels are maintained) before the encoding: (c) a decoded image using correct keys, and (d) the corresponding authentication distribution.

4. CONCLUSIONS

A digital holography-secured scheme has been presented by using binary phase or amplitude. The numerical results demonstrate that during optical decoding, the decrypted image cannot visually render clear information related to the input, and the effective authentication can be further conducted. Binary phase or binary amplitude pattern can be flexibly applied as ciphertext, and the fully optical implementation becomes possible for the decoding and authentication. Different from previous works [14,20–30], an interesting finding in this study is that in addition to binary phase, binary amplitude originating from the binarized phase pattern can also be applied as ciphertext. The ciphertext is effectively compressed, which can facilitate the storage or transmission in practical applications.

Funding. 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. **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. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).
4. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. **37**, 565–569 (1998).
5. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**, 3817–3819 (2010).
6. 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 **18**, 12033–12043 (2010).
7. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," Opt. Lett. **38**, 3198–3201 (2013).

8. W. Chen and X. Chen, "Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption," EPL **109**, 14001 (2015).
9. 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).
10. 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. **30**, 1644–1646 (2005).
11. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**, 118–120 (2010).
12. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253–10265 (2007).
13. T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A **25**, 2608–2617 (2008).
14. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22–24 (2011).
15. L. Sui, K. Duan, J. Liang, and X. Hei, "Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps," Opt. Express **22**, 10605–10621 (2014).
16. J. W. Goodman, *Introduction to Fourier Optics,* 2nd ed. (New York, McGraw-Hill, 1996).
17. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," Opt. Lett. **22**, 1268–1270 (1997).
18. W. Chen and X. Chen, "Space-based optical image encryption," Opt. Express **18**, 27095–27104 (2010).
19. F. Sadjadi and B. Javidi, *Physics of Automatic Target Recognition* (New York, Springer, 2007).
20. W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL **110**, 44002 (2015).
21. W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett. **38**, 546–548 (2013).
22. X. G. Wang, W. Chen, S. Mei, and X. Chen, "Optically secured information retrieval using two authenticated phase-only masks," Sci. Rep. **5**, 15668 (2015).
23. W. Chen, "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," IEEE Photon. J. **8**, 6900209 (2016).
24. W. Chen, "Multiple-wavelength double random phase encoding with CCD-plane sparse-phase multiplexing for optical information verification," Appl. Opt. **54**, 10711–10716 (2015).
25. W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," J. Opt. **16**, 025402 (2014).
26. D. Fan, X. F. Meng, Y. Wang, X. Yang, X. Pan, X. Peng, W. Q. He, G. Dong, and H. Chen, "Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing," Appl. Opt. **54**, 3204–3215 (2015).
27. W. Chen and X. Chen, "Marked ghost imaging," Appl. Phys. Lett. **104**, 251109 (2014).
28. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**, 221106 (2013).
29. W. Chen, X. G. Wang, and X. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," J. Opt. **17**, 035702 (2015).
30. I. Moon, F. Yi, M. Han, and J. Lee, "Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms," Appl. Opt. **55**, 4328–4335 (2016).
31. A. V. Oppenheim and J. S. Lim, "The importance of phase in signals," Proc. IEEE **69**, 529–541 (1981).
32. A. W. Lohmann, D. Mendlovic, and G. Shabtay, "Significance of phase and amplitude in the Fourier domain," J. Opt. Soc. Am. A **14**, 2901–2904 (1997).
33. T. Alieva and M. L. Calvo, "Importance of the phase and amplitude in the fractional Fourier domain," J. Opt. Soc. Am. A **20**, 533–541 (2003).