The following publication Yin Xiao, Lina Zhou, and Wen Chen, "Optical information authentication using phase-only patterns with single-pixel optical detection," Appl. Opt. 60, B1-B7 (2021) is available at https://dx.doi.org/10.1364/AO.414419.

Optical information authentication using phase-only patterns with single-pixel optical detection

YIN XIAO, LINA ZHOU, AND WEN CHEN*

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
**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

In this paper, we propose and experimentally demonstrate phase-only authentication based on single-pixel optical imaging through scattering media. The propagating wave is sequentially modulated by using a series of random amplitude-only patterns embedded in a spatial light modulator (SLM), and then a series of one-dimensional (1D) intensity values are recorded by the single-pixel (bucket) detector. Subsequently, an intensity pattern just before the SLM is retrieved by using a correlation algorithm, and then further propagates back to the object plane in which the object phase pattern is recovered to serve as reference. Then, some single-pixel intensity values are randomly selected from the recorded data, and 1-bit compression is applied to the randomly selected data in order to generate 1D binary signals as ciphertext. A series of random amplitude-only patterns corresponding to the randomly selected single-pixel intensity values serve as principal keys. In scattering environment, the proposed method is able to carry out phase-only authentication without visually rendering the plaintext, which has not been previously studied. It is found that phase-only authentication is sensitive to security keys, and the proposed method possesses high security. In addition, the proposed method is highly robust to noise contamination and data-loss contamination. Optical experimental results demonstrate feasibility and effectiveness of the proposed method.

1. INTRODUCTION

Optical means provides a promising tool for encoding information owing to its intrinsic characteristics, e.g., high-speed processing and multi-dimension operation. Optical encryption techniques have been developed rapidly over the past decades, since double random phase encoding (DRPE) scheme [1] was proposed. However, the DRPE system has been demonstrated to be vulnerable to some attacks, e.g., chosen-ciphertext attack [2], chosen-plaintext attack [3], known-plaintext attack [4,5] and other attacks [6]. It has been recently found that optical authentication [7] can be studied to recognize the decoded information without visually rendering the plaintext, which provides an extra security layer.

In recent years, ghost imaging (GI) [8–15] has been successfully applied for optical security [16–22]. Different from two-dimensional ciphertext recorded by using a CCD camera in conventional optical encryption systems, ciphertext generated in the GI is a series of single-pixel values recorded by using a single-pixel bucket detector without spatial resolution. In GI-based optical encryption scheme, the one-dimensional (1D) ciphertext is beneficial to data storage and transmission, and simultaneously system security can be enhanced. Most GI-based encryption and authentication technologies focus on the studies and usage of amplitude information. However, phase is more important than amplitude in many applications in the optical field [23]. It is meaningful to authenticate the decoded phase information by taking advantage of GI technique. The studies about phase-only authentication based on GI techniques have not been carried out. Although digital holography is a powerful tool to recover phase information of an object [24–29], its capability is limited through scattering media. Therefore, it is promising to apply the GI into digital holography to overcome the challenges existing in conventional GI-based encryption systems, since the GI is robust to scattering media [30–32]. The GI technique is applied to digital holography, and the CCD used in conventional digital holography is replaced by using a spatial light modulator (SLM) and a single-pixel detector. In this case, digital hologram is numerically retrieved by using the GI method. This method is called as 'single-pixel (ghost) holography'.

In this paper, phase-only authentication based on single-pixel imaging through scattering media is experimentally demonstrated for the first time to our knowledge. In the experimental setup, both object wave and reference wave are disturbed by scattering media, and the propagating wave pattern just before the SLM is sequentially modulated by a series of random amplitude-only patterns. After propagating through another diffuser, the modulated wave is sequentially recorded by using a single-pixel bucket detector. Subsequently, correlation algorithm is used to extract an intensity pattern just before the SLM, and then the extracted intensity pattern propagates back to the object plane for the recovery of object phase pattern as reference. Then, some single-pixel values are randomly selected from the recorded data, and 1-bit compression is further

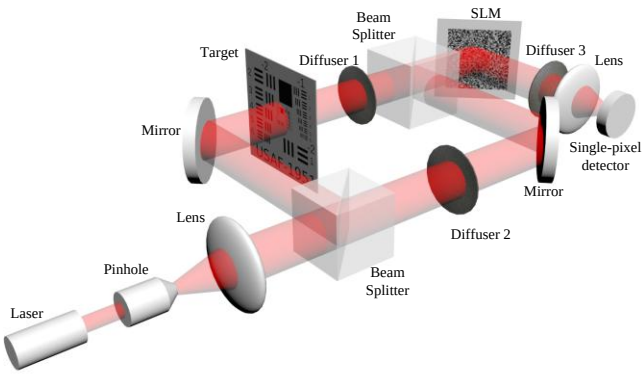

Fig. 1. Schematic experimental setup: SLM, spatial light modulator.

applied to the randomly selected data to generate binary signals as ciphertext. A series of random amplitude-only patterns corresponding to the randomly selected data serve as principal keys, and axial distance, pixel size and wavelength serve as supplementary keys. By using security keys and ciphertext, a decrypted phase pattern in the object plane can be recovered. Nonlinear correlation is further conducted to authenticate the decrypted phase pattern with its reference phase without visually rendering the plaintext. In scattering environment, the proposed method is able to implement phase-only authentication. It is also found that phase-only authentication is sensitive to security keys, and high security is achieved. In addition, the proposed method is robust to noise contamination and data-loss contamination. In practical applications, information security is of high importance. For data storage and transmission, it is meaningful and significant to reduce the data storage memory and ensure the data transmission with security. In addition, after data transmission, especially through a complex environment, it is crucial to effectively authenticate the information. The proposed method can be applied to resolve the relevant problems.

2. EXPERIMENTAL SETUP

A schematic experimental setup is shown in Fig. 1. A He-Ne laser with wavelength of 633.0 nm is expanded by a pinhole and collimated by a lens with focal length of 50.0 mm. After passing through a beam splitter cube, the collimated beam is split into two beams. One beam interacts with a target (Edmund, negative 1951 USAF target), and then is disturbed by a diffuser (Thorlabs, DG10-600). The other beam is also disturbed by a diffuser (Thorlabs, DG10-600). The two beams interfere just before a SLM (Holoeye, LC-R720), and the propagating wave pattern is sequentially modulated by a series of random amplitude-only patterns embedded in the SLM. The modulated wave pattern further propagates through another diffuser (Thorlabs, DG10-220), and then is recorded by using a single-pixel bucket detector (Newport, 918D-UV-OD3R) without spatial resolution.

In the experimental setup, when a number of random amplitude-only patterns (i.e., 5000 patterns) are sequentially embedded into the SLM, a series of single-pixel intensity values are correspondingly recorded. By using the random amplitude-only patterns P_i and the recorded single-pixel values B_i, correlation algorithm is first applied to retrieve an intensity pattern H_{ref} just before the SLM.

$$H_{ref} = \frac{1}{T}\sum_{i=1}^{T}\left(B_i - \langle B_i \rangle\right)\left(P_i - \langle P_i \rangle\right), \qquad (1)$$

where T denotes the number of measurements, and $\langle \bullet \rangle = \sum_i / T$ denotes an ensemble average over T measurements.

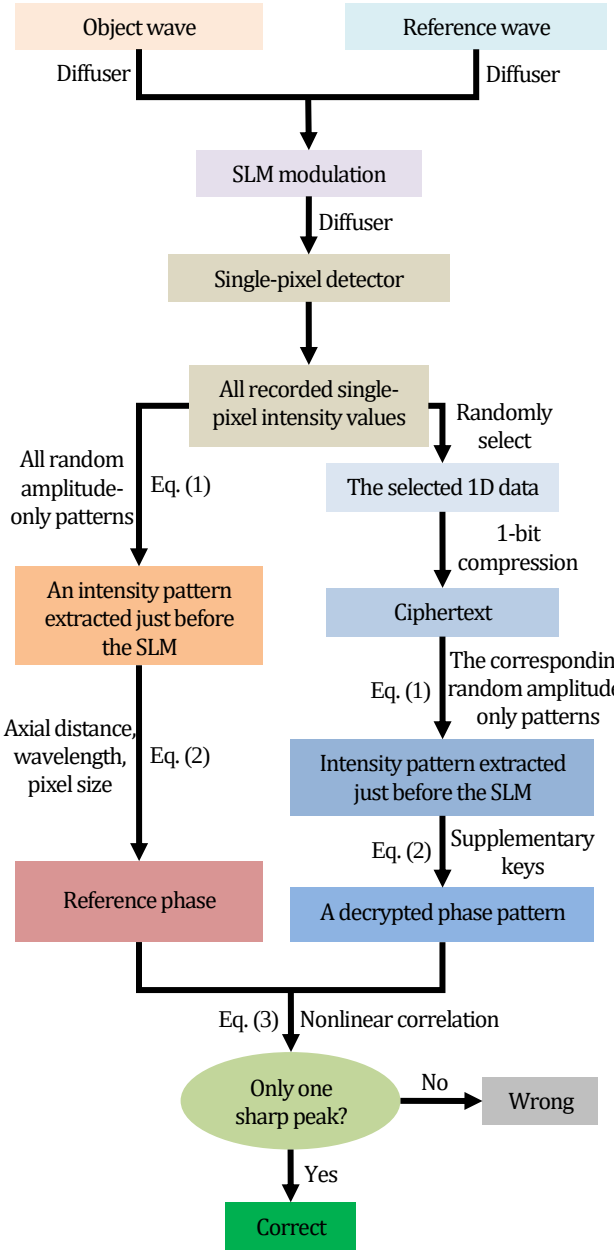

Fig. 2. Flow chart for the proposed method.

The retrieved intensity pattern numerically propagates back to the object plane using free-space wave propagation principle, and an object phase pattern can be extracted to serve as reference from the reference object O_{ref}.

$$O_{ref}(x,y) = IFT\left\{FT\left[H_{ref}(x,y)\right]ST(\mu,\nu)\right\}, \qquad (2)$$

where FT and IFT respectively denote Fourier transform and inverse Fourier transform, (x,y) and (μ,ν) respectively denote coordinates of spatial domain and frequency domain, and $ST(\mu,\nu)$ denotes transfer function.

Subsequently, some single-pixel intensity values (i.e., 2000) are

randomly selected from the totally recorded single-pixel values, and then 1-bit compression is applied to the randomly selected data to generate 1D binary signals as ciphertext. A series of random amplitude-only patterns corresponding to the randomly-selected single-pixel values serve as principal security keys, and axial propagation distance, wavelength and pixel size serve as supplementary keys. An intensity pattern extracted just before the SLM can be obtained, when the ciphertext and principal security keys are applied in Eq. (1). By further using supplementary keys, the extracted intensity pattern propagates back to the object plane and then a decrypted phase pattern at the object plane can be recovered.

The decrypted phase pattern is further authenticated by using its reference phase via nonlinear correlation [7,33–39].

$$NC = \left| IFT\left(|\Phi|^{k} \times \frac{\Phi}{|\Phi|} \right) \right|^{2}, \tag{3}$$

where $\Phi = FT(\mathrm{Ref})\left[FT(\mathrm{Dec})\right]^{*}$, NC denotes the generated nonlinear correlation map, asterisk denotes complex conjugate, k denotes nonlinear strength, Ref denotes reference information, and Dec denotes the decrypted information.

Nonlinear correlation is used here due to the better correlation peak, the better peak-to-sidelobe ratio and the narrower correlation width compared with linear correlations. When there is only one sharp peak in the generated nonlinear correlation map, it means that the receiver possesses correct keys or is an authorized person. If there is only noisy background in the generated nonlinear correlation map, it means that the receiver is an unauthorized person or does not have correct keys. A flow chart for the proposed method is shown in Fig. 2.

3. EXPERIMENTAL RESULTS AND DISCUSSION

Two different regions in the USAF1951 target, as indicated in Fig. 3(a), are chosen to be respectively served as object 1 and object 2. A reflective object is used to be served as object 3 as shown in Fig. 3(b), and the setup in Fig. 1 can be simply modified for the reflection case.

In the experiments, 5000 random amplitude-only patterns are generated and sequentially embedded into the SLM to modulate the propagating wave pattern. Then, 5000 single-pixel intensity values are sequentially recorded by using the single-pixel bucket detector. Subsequently, 2000 single-pixel intensity values are further randomly selected from the recorded data, and then 1-bit compression is applied to the randomly selected 1D data to generate binary signals as ciphertext as typically shown in Fig. 3(c). The number of binary signals (i.e., single-pixel ciphertext) is selected based on peak-to-energy (PCE). The PCE is defined as the ratio between the maximum intensity peak value and the total energy of nonlinear correlation output in the generated nonlinear correlation map.

$$\mathrm{PCE} = \frac{\max NC}{\sum\sum NC}. \tag{4}$$

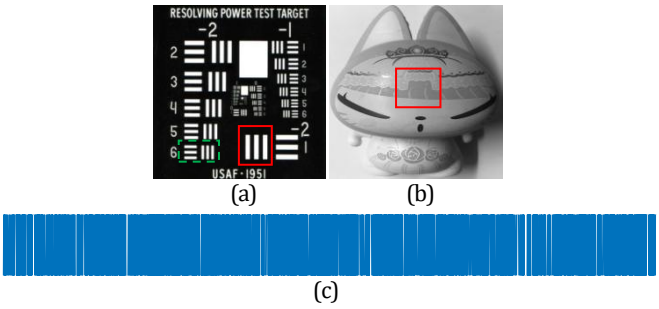

Fig. 3. (a) Two transmission objects: the region inside the dashed-line box represents object 1 and the region inside the solid-line box represents object 2, (b) region of a reflective object (indicated by the solid-line box) used as object 3, and (c) typical ciphertext (i.e., a series of binary signals).

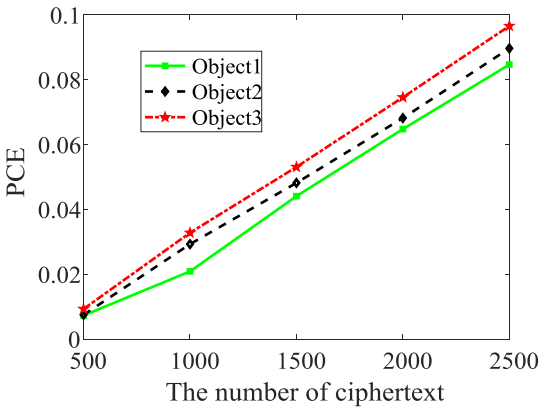

Fig. 4. The PCE values versus the number of binary signals (i.e., ciphertext).

For the three objects in Figs. 3(a) and 3(b), the PCE values are calculated with respect to the number of binary signals, and the results are shown in Fig. 4. As seen in Fig. 4, the PCE values show a nearly linear growth relationship with the number of binary signals. It is found that when the number of binary signals is 2000, nonlinear correlations between reference phase and the decrypted phase patterns are always satisfactory, i.e., only one sharp peak with flat background in the generated nonlinear correlation maps without visually rendering original information.

Feasibility and effectiveness of the proposed method are first analyzed, and experimental results are shown in Fig. 5. The three reference phase patterns respectively corresponding to the three objects in Fig. 3 are recovered as shown in Figs. 5(a)–5(c). Subsequently, three decrypted phase patterns as shown in Figs. 5(d), 5(h) and 5(l) are recovered by using correct security keys, which respectively correspond to the three objects. When the decrypted phase patterns are nonlinearly correlated with their corresponding reference phase patterns, nonlinear correlation maps are generated as respectively shown in Figs. 5(e), 5(j) and 5(o). Since the decryption is conducted by using correct keys, there is only one sharp peak in the generated nonlinear correlation map which means that the decrypted information is correctly authenticated without visually rendering

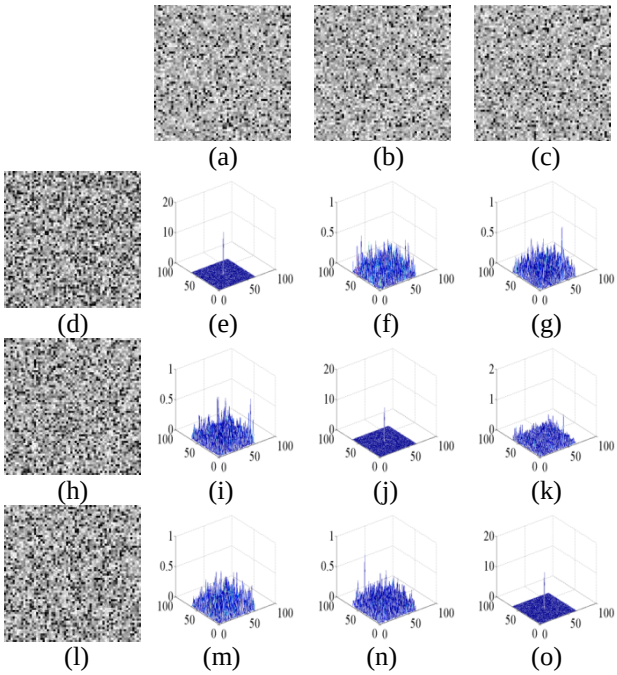

Fig. 5. (a)–(c) Three reference phase patterns respectively corresponding to three objects in Figs. 3(a) and 3(b), (d), (h) and (l) three decrypted phase patterns respectively corresponding to the three objects, (e), (j) and (o) nonlinear correlation maps generated between reference phase and their correspondingly decrypted phase patterns when correct keys are used for the decoding, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps generated between incorrect references and the decrypted phase patterns.

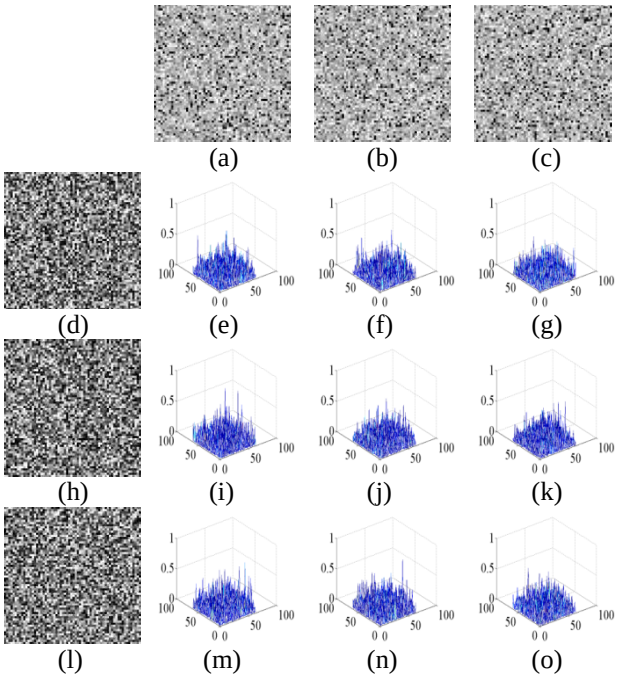

Fig. 6. (a)–(c) Three reference phase patterns respectively corresponding to the three objects in Figs. 3(a) and 3(b), (d), (h) and (l) three decrypted phase patterns obtained by using wrong amplitude-only patterns, and (e)–(g), (i)–(k) and (m)–(o) nonlinear correlation maps generated between reference phase patterns and the decrypted phase patterns.

original information (i.e., the plaintext). When the decrypted phase pattern is nonlinearly correlated with incorrect references stored in a database, there is only noisy background in the generated nonlinear correlation maps, as respectively shown in Figs. 5(f), 5(g), 5(i), 5(k), 5(m) and 5(n). The experimental results shown in Figs. 5(a)–5(o) demonstrate that the proposed method is able to correctly authenticate the decrypted phase patterns, and simultaneously possesses high discrimination capability.

To evaluate system security, the decryption is also conducted by using wrong amplitude-only patterns (i.e., wrong principal security keys). Three reference phase patterns shown in Figs. 6(a)–6(c) are the same as those shown in Figs. 5(a)–5(c). When wrong amplitude-only patterns are applied to recover the decrypted phase patterns, three decrypted phase patterns are obtained and shown in Figs. 6(d), 6(h) and 6(l), respectively. In this case, these three decrypted phase patterns cannot be correctly authenticated, and all generated nonlinear correlation maps contain only noisy backgrounds, as shown in Figs. 6(e)–6(g), 6(i)–6(k) and 6(m)–6(o).

It is further found that the proposed method is also sensitive to supplementary keys, e.g., axial distance between the target and the SLM. For the sake of brevity, the PCE values are calculated only with respect to different axial distances between the target and the SLM, and the results are shown in Fig. 7. In this case, all other security keys are correct. Since the axial distance of 2.0 cm is used in the experiments, the PCE value achieves its maximum when the axial distance used for the decoding is equivalent to 2.0 cm. It is also demonstrated in Fig. 7 that a small deviation (e.g., 1.0 mm) in the axial distance leads to a dramatic decrease in the PCE values. Therefore, it has been demonstrated that high security can be achieved in the proposed method.

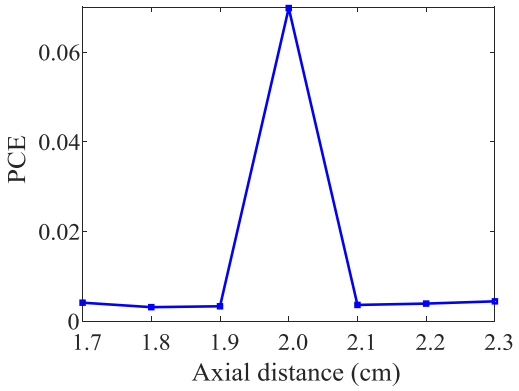

Fig. 7. The PCE values versus axial propagation distances.

It is also necessary to investigate noise contamination during data (ciphertext) storage and transmission. The ciphertext contaminated by noise is described by $B' = B + L \times G$, where B denotes binary signals, B' denotes the ciphertext contaminated by noise, L represents noise level, and G represents Gaussian noise with mean of 0 and variance of 1.0. Here, object 1 is used as a typical example to illustrate phase-only authentication under noise contamination. The decrypted phase patterns as shown in Figs. 8(a)–8(d) are obtained by using noise levels of 0.2, 0.4, 0.6 and 0.8, respectively. The reference phase pattern is shown in Fig. 8(e). When the decrypted phase patterns are nonlinearly correlated with reference phase, the generated nonlinear correlation maps are respectively shown in Figs. 8(f)–8(i). It can be seen in Figs. 8(f)–8(i) that the proposed method possesses high robustness against

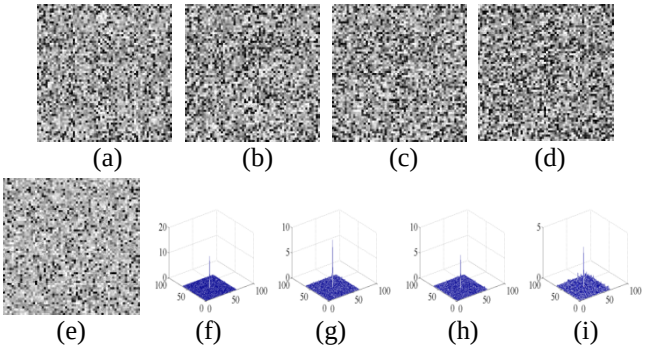

Fig. 8. (a)–(d) Decrypted phase patterns respectively using noise level of 0.2, 0.4, 0.6, 0.8, (e) reference phase pattern corresponding to object 1, and (f)–(i) nonlinear correlation maps respectively between reference phase and the decrypted phase patterns (i.e., (a)-(d)).

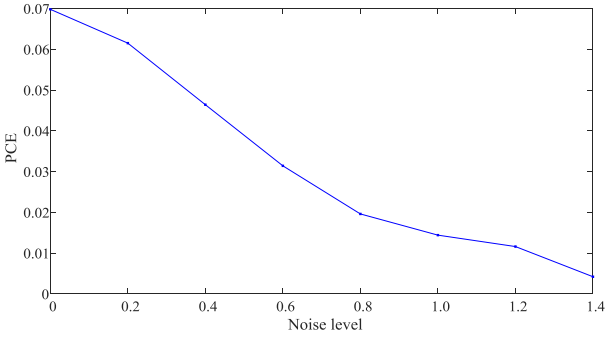

Fig. 9. The PCE values versus noise levels.

noise contamination, since the nonlinear correlation maps always show only one apparently sharp peak. Robustness of the proposed method against noise is further tested in a larger range of noise levels, and the PCE values with respect to different noise levels are shown in Fig. 9. It is found that when the PCE value is larger than 0.01, there is only one apparently sharp peak in the generated nonlinear correlation distributions. Hence, the proposed method is feasible and effective even when the noise level approaches to 1.2.

Ciphertext loss could also happen during data storage and transmission. Hence, it is necessary to evaluate robustness of the proposed method against ciphertext loss. Here, the loss percentage is defined as the ratio between the number of lost elements and the total number of elements in the ciphertext. Object 1 is also used as a typical example to illustrate phase-only authentication under ciphertext-loss contamination. Four decrypted phase patterns shown in Figs. 10(a)–10(d) are obtained when there is a loss percentage of 20.0%, 40.0%, 60.0% and 80.0% respectively in the ciphertext. Figure 10(e) shows the reference phase pattern corresponding to object 1. When reference phase is nonlinearly correlated respectively with the decrypted phase patterns, the generated nonlinear correlation maps are shown in Figs. 10(f)–10(i). As seen in Figs. 10(f)–10(h), there is only one sharp peak with flat background in the generated nonlinear correlation maps without visually rendering the plaintext, which means that the authentication is correct and correct security keys have been used. When ciphertext loss level reaches 80.0% as shown in Fig. 10(i), there is much noise and the authentication is considered as 'incorrect'. Performance of the proposed method against ciphertext-loss contaminations is further shown in Fig. 11, in which the PCE values with respect to different ciphertext-loss levels are calculated. The PCE values can keep above 0.01 when the noise level reaches 60.0%. Hence,

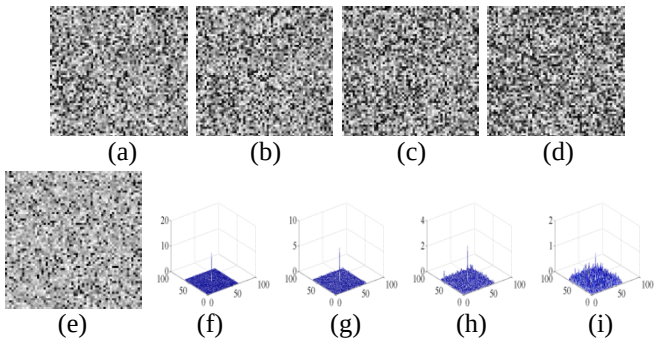

Fig. 10. (a)-(d) The decrypted phase patterns respectively obtained by using ciphertext-loss levels of 20.0%, 40.0%, 60.0% and 80.0%, (e) reference phase pattern corresponding to object 1, and (f)-(i) nonlinear correlation maps respectively generated between reference phase (i.e., (e)) and the decrypted phase (i.e., (a)-(d)).

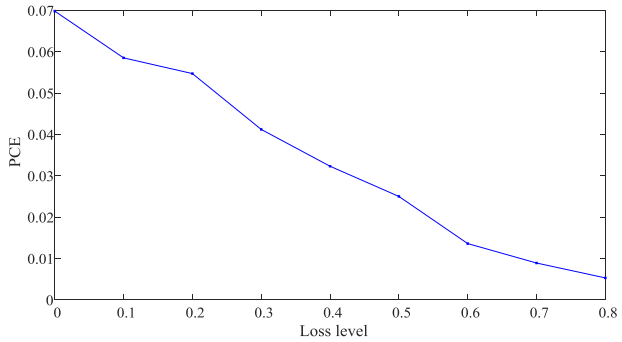

Fig. 11. The PCE values versus ciphertext-loss levels.

high robustness against ciphertext-loss contamination is achieved in the proposed method.

To further evaluate performance of the proposed method through different scattering media, more complicated scattering environments are constructed, as shown in Figs. 12(a)–12(c). In Fig. 12(a), there are two cascaded diffusers placed at the object wave path, and one diffuser placed at the reference wave path is unchanged, i.e., the same as that shown in Fig. 1. In Fig. 12(b), the diffuser placed at the object wave path is the same as that shown in Fig. 1, and two cascaded diffusers are placed at the reference wave path. In Fig. 12(c), there are multiple cascaded diffusers placed at both object wave and reference wave paths.

For the sake of brevity, only the experimental setup in Fig. 12(c) is further studied, and the results are shown in Fig. 13. Figures 13(a)–13(c) show reference phase patterns respectively corresponding to the three objects in Figs. 3(a) and 3(b), and Figs. 13(d), 13(h) and 13(l) show the decrypted phase patterns obtained by using correct security keys respectively corresponding to the three objects. When the decrypted phase patterns are nonlinearly correlated respectively with their corresponding reference phase patterns, the generated nonlinear correlation maps are shown in Figs. 13(e), 13(j) and 13(o), respectively. All nonlinear correlation maps contain only one sharp peak, which means that the phase-only authentication is correct without visually rendering original information and correct security keys have been used by the receivers. When the incorrect references at the database are used to be nonlinearly correlated with the decrypted phase patterns, only noisy backgrounds are obtained in the generated nonlinear correlation maps, as shown in Figs. 13(f), 13(g), 13(i), 13(k), 13(m) and 13(n). It is demonstrated that the proposed method is effective and robust in different scattering environments.

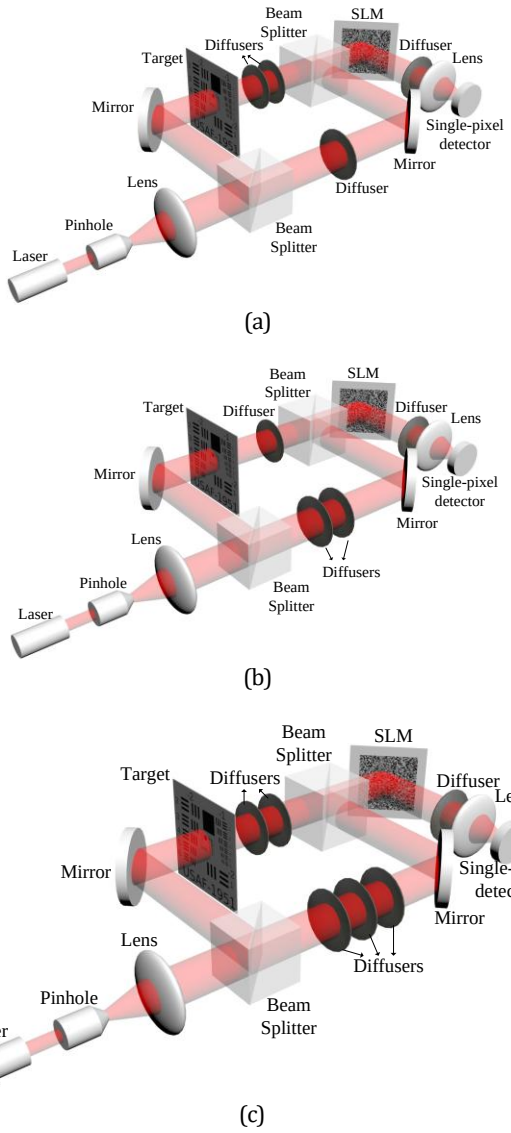

Fig. 12. (a) Two cascaded diffusers placed at object wave path, (b) two cascaded diffusers placed at reference wave path, and (c) multiple cascaded diffusers at both object wave and reference wave paths.

4. CONCLUSION

We have experimentally demonstrated phase-only authentication based on single-pixel optical imaging through scattering media. The experimental results have systematically demonstrated feasibility and effectiveness of the proposed method. The proposed method is effective and robust when scattering environments are applied, which makes it promising and meaningful in practical applications. Phase-only authentication through scattering media is sensitive to security keys, and high security can be achieved. In addition, it is demonstrated that the proposed method possesses high robustness against noise contamination and data-loss contamination. The proposed method using phase-only authentication can be easily extended to other optical security setups, and could open up a different research perspective for optical security.

Funding. National Natural Science Foundation of China (NSFC) (61605165); Hong Kong Research Grants Council (25201416).

Disclosures. The authors declare no conflicts of interest.

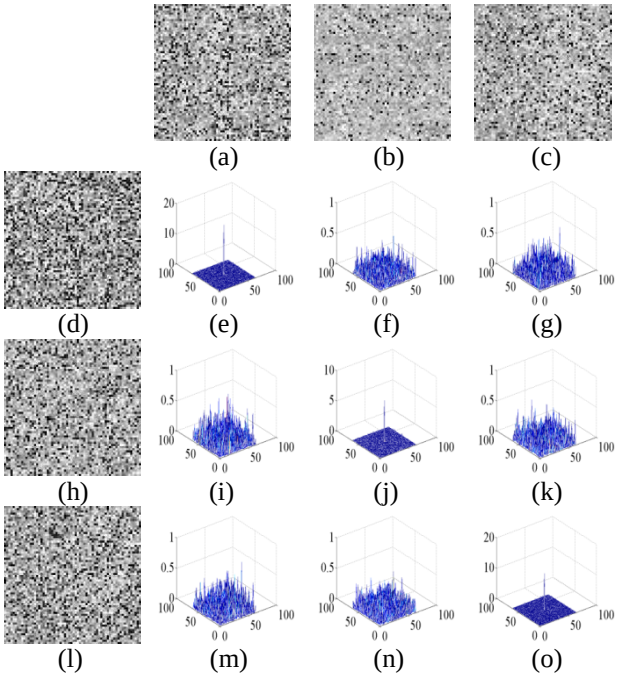

Fig. 13. (a)–(c) Three reference phase patterns respectively corresponding to the three objects, (d), (h) and (l) three decrypted phase patterns respectively corresponding to the three objects by using correct security keys, (e), (j) and (o) nonlinear correlation maps generated between reference phase and their correspondingly decrypted phase patterns, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps generated between incorrect references and the decrypted phase patterns.

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20(7), 767–769 (1995).
2. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. 30(13), 1644–1646 (2005).
3. J. J. Wu, W. Liu, Z. J. Liu, and S. T. Liu, "Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings," Opt. Commun. 338, 164–167 (2015).
4. X. Peng, P. Zhang, H. Z. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. 31(8), 1044–1046 (2006).
5. S. K. Rajut and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform," Appl. Opt. 52(4), 871–878 (2013).
6. C. L. Guo, I. Muniraj, and J. T. Sheridan, "Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," Appl. Opt. 55(17), 4720–4728 (2016).
7. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. 36(1), 22–24 (2011).
8. J. H. Shapiro, "Computational ghost imaging," Phys. Rev. A 78(6), 061802R (2008).
9. Y. Bromberg, O. Katz, and Y. Silberberg, "Ghost imaging with a single detector," Phys. Rev. A 79(5), 053840 (2009).
10. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. 103(22), 221106 (2013).

11. M. F. Duarte, M. A. Davenport, D. Takhar, J. N. Laska, T. Sun, K. F. Kelly, and R. G. Baraniuk, "Single-pixel imaging via compressive sampling," IEEE Signal Process Mag. 25(2), 83–91 (2008).
12. B. Sun, M. P. Edgar, R. Bowman, L. E. Vittert, S. Welsh, A. Bowman, and M. J. Padgett, "3D computational imaging with single-pixel detectors," Science 340(6134), 844–847 (2013).
13. Z. B. Zhang, X. Ma, and J. G. Zhong, "Single-pixel imaging by means of Fourier spectrum acquisition," Nat. Commun. 6, 6225 (2015).
14. X. H. Chen, I. N. Agafonov, K. H. Luo, Q. Liu, R. Xian, M. V. Chekhova, and L. A. Wu, "High-visibility, high-order lensless ghost imaging with thermal light," Opt. Lett. 35(8), 1166–1168 (2010).
15. N. Tian, Q. C. Guo, A. Wang, D. L. Xu, and L. Fu, "Fluorescence ghost imaging with pseudothermal light," Opt. Lett. 36(16), 3302–3304 (2011).
16. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. 35(14), 2391–2393 (2010).
17. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," Appl. Phys. Lett. 101(10), 101108 (2012).
18. W. Chen and X. D. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett. 38(4), 546–548 (2013).
19. W. Chen and X. D. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL 110(4), 44002 (2015).
20. W. Chen and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," Opt. Lasers Eng.73, 123–127 (2015).
21. H. Hai, S. X. Pan, M. H. Liao, D. J. Lu, W. Q. He, and X. Peng, "Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning," Opt. Express 27(15), 21204-21213 (2019).
22. L. F. Chen, B. Y. Peng, W. W. Gan, and Y. Q. Liu, "Plaintext attack on joint transform correlation encryption system by convolutional neural network," Opt. Express 28(19), 28154-28163 (2020).
23. A. V. Oppenheim and J. S. Lim, "The importance of phase in signals," Proceedings of the IEEE 69(5), 529-541 (1981).
24. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng. 43(10), 2233–2238 (2004).
25. M. Takeda, K. Nakano, H. Suzuki, and M. Yamaguchi, "Encrypted sensing based on digital holography for fingerprint images," Opt. Photon. J. 5, 6–14 (2015).
26. M. T. Shiu, Y. K. Chew, H. T. Chan, X. Y. Wong, and C. C. Chang, "Three-dimensional information encryption and anticounterfeiting using digital holography," Appl. Opt. 54(1), A84–A88 (2015).
27. P. Marquet, B. Rappaz, P. J. Magistretti, E. Cuche, Y. Emery, T. Colomb, and C. Depeursinge, "Digital holographic microscopy: a noninvasive contrast imaging technique allowing quantitative visualization of living cells with subwavelength axial accuracy," Opt. Lett. 30(5), 468– 470 (2005).
28. B. Kemper and G. von Bally, "Digital holographic microscopy for live cell applications and technical inspection," Appl. Opt. 47(4), A52– A61 (2008).
29. B. Rappaz, F. Charrière, C. Depeursinge, P. Magistretti, and P. Marquet, "Simultaneous cell morphometry and refractive index measurement with dual-wavelength digital holographic microscopy and dye–enhanced dispersion of perfusion medium," Opt. Lett. 33(7), 744–746 (2008).
30. P. L. Zhang, W. L. Gong, X. Shen, and S. S. Han, "Correlated imaging through atmospheric turbulence," Phys. Rev. A 82(3), 033817 (2010).
31. X. D. Chen, *Computational Methods for Electromagnetic Inverse Scattering* (Wiley-IEEE, 2018).
32. Y. Xiao, L. N. Zhou, and W. Chen, "Direct single-step measurement of Hadamard spectrum using single-pixel optical detection," IEEE Photon. Tech. Lett. 31(11), 845–848 (2019).
33. Y. Xiao, L. N. Zhou, and W. Chen, "Experimental demonstration of ghost-imaging-based authentication in scattering media," Opt. Express 27(15), 20558–20566 (2019).
34. O. Matoba, T. Nomura, E. Péréz-Cabré, M. S. Millan, and B. Javidi, "Optical techniques for information security," Proc. IEEE 97(6), 1128–1148 (2009).
35. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. 6(2), 120–155 (2014).
36. B. Javidi, "Nonlinear joint power spectrum based optical correlation," Appl. Opt. 28(12), 2358–2367 (1989).
37. W. Chen, "Single-shot in-line holographic authentication using phase and amplitude modulation," Opt. Lasers Eng. 121, 473–478 (2019).
38. W. Chen, X. G. Wang, and X. D. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," J. Opt. 17(3), 035702 (2014).
39. Y. Xiao, L. N. Zhou, and W. Chen, "Secured single-pixel ghost holography," Opt. Lasers Eng. 128, 106045 (2020).