Research Article | Vol. 27, No. 15 | 22 Jul 2019 | OPTICS EXPRESS 20558
Optics EXPRESS

Experimental demonstration of ghost-imaging-based authentication in scattering media

YIN XIAO,[1] LINA ZHOU,[1] AND WEN CHEN[1,2,*]

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

Abstract: Optical imaging in scattering media and its applications are challenging and meaningful. In this paper, we propose and experimentally verify a new optical authentication method using structured-detection-based ghost imaging (GI) in scattering media. Object wave is disturbed by multiple diffusers, and then sequentially modulated by a series of random amplitude-only patterns embedded in a spatial light modulator (SLM). The modulated wave passes through another scattering medium, and its intensity is measured by using a single-pixel bucket detector without spatial resolution. During the decryption and authentication, a reference pattern is first retrieved by using all recorded single-pixel intensity signals. Subsequently, a small number of the recorded single-pixel intensity signals are further randomly selected, and a 1-bit compression operation is applied to these selected intensity signals to generate binary signals as ciphertext. The random amplitude-only patterns corresponding to the selected single-pixel intensity signals serve as principal security keys, and wavelength, axial distance and pixel size can serve as supplementary keys. Two strategies are further developed for the decryption and authentication. It is experimentally verified that the proposed method possesses high robustness and high discrimination capability. The proposed method established by using scattering media can significantly enrich optical security, and provides a promising approach for optical authentication.

1. Introduction

Optical means becomes a promising and important tool for securing information in recent years. In optical encryption, double random phase encoding was first proposed by Refregier and Javidi [1]. Other optical security systems have also been continuously studied which usually used CCD camera [2–9] for the recording, and cannot be effectively applied to encode and decode information in scattering media. Recently, ghost imaging (GI) has been studied and applied for optical security [10–20]. Different from other optical security methods using CCD camera, GI encoding employs a single-pixel bucket detector to collect signals, which can record a series of single-pixel intensity signals as ciphertext. In addition, GI encryption-based authentication [18,19] has also been developed to enhance system security. The GI encryption-based authentication method can effectively verify the decrypted information, and does not visually render object information [21]. However, a secure approach for the generation of reference data has not been effectively developed and applied. Although it has been demonstrated that the GI system is promising for optically securing information, the GI authentication has not been explored and verified in scattering media [22]. In addition, experimental demonstration of GI encryption and authentication in scattering media has also not been studied.

In this paper, we propose a new optical authentication method using structured-detection-based GI in scattering media. Object wave is disturbed by multiple diffusers, and then sequentially modulated by a series of random amplitude-only patterns embedded in a spatial light modulator (SLM). The modulated object wave passes through another scattering

#365882 https://doi.org/10.1364/OE.27.020558
Journal © 2019 Received 24 Apr 2019; revised 30 May 2019; accepted 30 May 2019; published 10 Jul 2019

Optics EXPRESS

medium, and its intensity is recorded by using a single-pixel bucket detector. Correlation algorithm in the GI is first used to retrieve a diffraction intensity pattern just before the SLM to be served as reference. Subsequently, a small number of the recorded single-pixel intensity signals are randomly selected, and a 1-bit compression operation is applied to these selected intensity signals to generate binary signals as ciphertext. Two strategies are further developed for the decryption and authentication. It is experimentally verified that the proposed method possesses high robustness and high discrimination capability, and provides a different research perspective for optical authentication.

2. Experimental setup and principles

A schematic for the experimental setup is shown in Fig. 1. A He-Ne laser beam with wavelength of 632.8 nm is expanded by a pinhole and collimated by a lens with focal length of 5.0 cm. Optical wave transmitting from the object (negative 1951 USAF target) is sequentially disturbed by two diffusers (Thorlabs DG10-600 and DG10-220). Subsequently, the propagating wave is sequentially modulated by a series of random amplitude-only patterns embedded in a SLM (Holoeye LC-R720). The reflected wave is further disturbed by another diffuser (Thorlabs DG10-120), and a single-pixel bucket detector (Newport 1936-R) is used to collect the light intensity. When scattering media continuously disturb object beam, there is no method in the literature to effectively address the decryption and authentication issue. Here, two strategies are proposed and experimentally verified to address the concern for GI encryption-based authentication in scattering media.

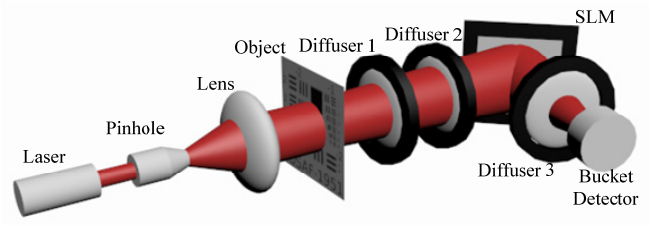


Fig. 1. The schematic experimental setup. SLM: spatial light modulator.

Since reference pattern needs to be generated for optical authentication, a diffraction intensity pattern just before the SLM is first retrieved by using correlation algorithm with all the recorded single-pixel signals (e.g., 5000) and random amplitude-only patterns embedded in the SLM. The retrieved diffraction intensity pattern is applied as reference for optical authentication, and the retrieval process is described in Fig. 2.

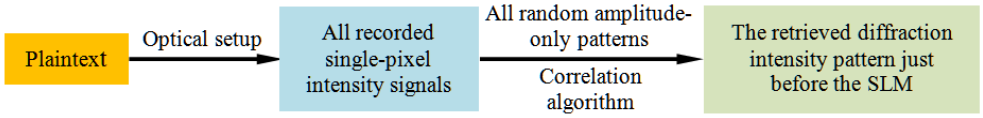


Fig. 2. Strategy I: procedure for retrieving a diffraction intensity pattern just before the SLM.

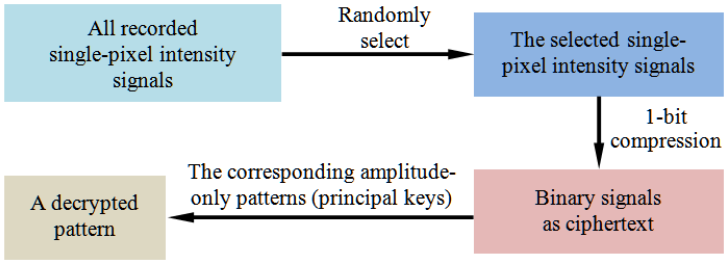


Fig. 3. Strategy I: procedure for ciphertext generation and the decryption.

Optics EXPRESS

Subsequently, a small number of the recorded single-pixel intensity signals (e.g., 500) are randomly selected, and their corresponding random amplitude-only patterns (embedded in the SLM) are used as principal security keys. A 1-bit compression operation is further applied to compress these selected single-pixel intensity signals to generate binary signals as ciphertext. The mean value of these selected single-pixel intensity signals is first calculated as a threshold in order to generate binary signals. By using the ciphertext and principal security keys, a decrypted intensity pattern just before the SLM is obtained which is correlated with the retrieved diffraction intensity pattern (see Fig. 2) to generate a nonlinear correlation distribution for optical authentication. When only one sharp peak is obtained in the nonlinear correlation map, it means that the receiver possesses correct keys or is an authorized person. When only a noisy correlation map is generated, it means that the receiver does not have correct security keys or is an unauthorized person. The above method is called "strategy I" in this study, and Fig. 3 further shows the process for ciphertext generation and the decryption.

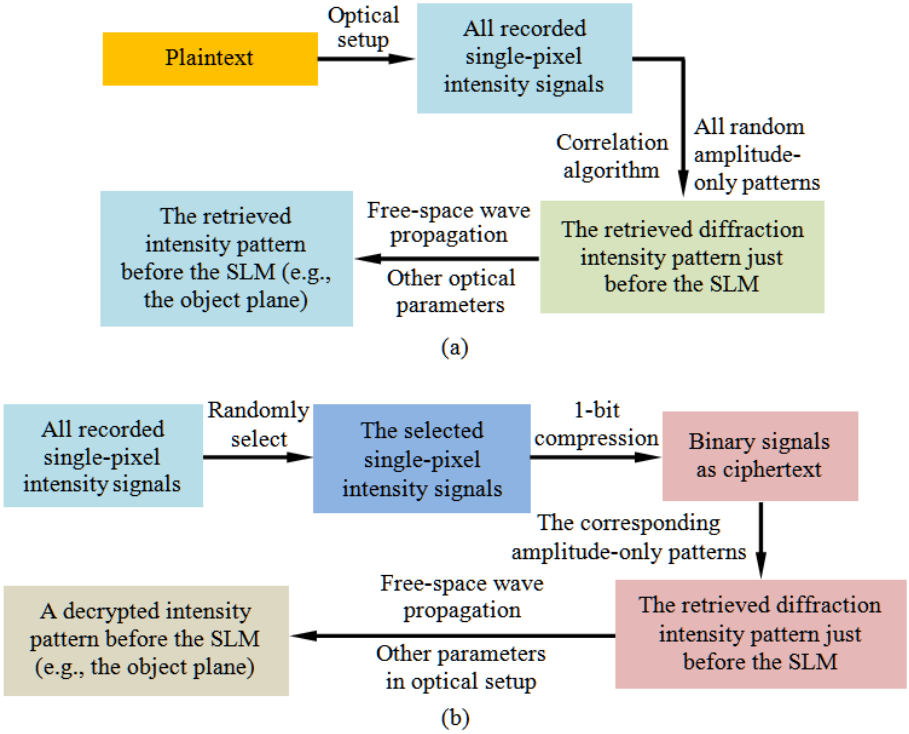


Fig. 4. Strategy II: (a) procedure for retrieving an intensity pattern before the SLM (e.g., the object plane) as a new reference, and (b) procedure for ciphertext generation and the decryption.

Alternatively, it is also feasible to develop and apply another strategy for the decryption and authentication. Reference pattern also needs to be generated for optical authentication, and a diffraction intensity pattern just before the SLM is first retrieved by using correlation algorithm with all the recorded signals and random amplitude-only patterns embedded in the SLM. The retrieved diffraction intensity pattern is further processed by using free-space wave propagation principle [23] to generate an intensity pattern before the SLM (e.g., the object plane) as a new reference for optical authentication, and the retrieval process is described in Fig. 4(a). Since scattering media are integrated, the reference pattern cannot be imitated in practice. Subsequently, a small number of the recorded single-pixel intensity signals are randomly selected, and their corresponding random amplitude-only patterns (embedded in the SLM) are used as principal security keys. A 1-bit compression operation is further applied to

Optics EXPRESS

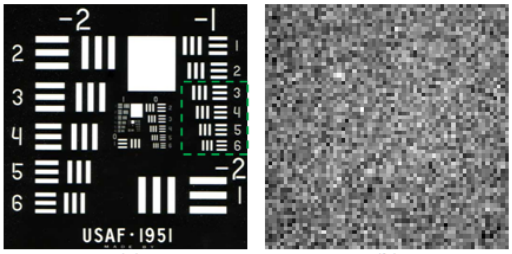
compress these selected single-pixel intensity signals to generate binary signals as ciphertext. By using the ciphertext and principal security keys, a diffraction intensity pattern just before the SLM is first retrieved and then free-space wave propagation principle is applied to retrieve a decrypted intensity pattern before the SLM (e.g., the object plane) which is correlated with the retrieved intensity pattern [see Fig. 4(a)] to generate a nonlinear correlation map for optical authentication. When only one sharp peak is obtained in the nonlinear correlation map, it means that the receiver possesses correct keys or is an authorized person. Otherwise, it means that the receiver does not have correct security keys or is an unauthorized person. The above method is called "strategy II" in this study, and Fig. 4(b) further shows the process for ciphertext generation and the decryption.

In addition to the diffusers used in experiments, different scattering media can flexibly be applied to disturb object waves during the recording, and different scattering layers can be flexibly designed and applied in the proposed method. The proposed optical setup takes advantage of structured-detection-based technique, which resolves the limitations existing in conventional structured illumination method. Moreover, optical setup before the SLM in Fig. 1 can be flexibly designed in practice to further enhance system complexity.

In the designed experimental setup, the diffusers 1 and 2 are cascaded and used as a typical example to construct a scattering environment, and the number of different diffusers can be flexibly designed and applied in the proposed method. For the diffuser 3, the ability to retrieve signals in scattering media is an important advantage of GI, and the diffuser 3 is used here only for the demonstration of the property of GI. In this paper, the objective is to study and experimentally demonstrate GI-based authentication in scattering media, which has never been investigated. It is worth noting that the GI-based authentication in scattering media is established over optical encryption and decryption layers without visually rendering object information.

3. Experimental demonstrations and discussion

As a typical example, the region inside the dashed-line box in Fig. 5(a) is used as an object to experimentally show the validity of the proposed method. In the proposed method, reference pattern is first generated and stored in a database for the subsequent optical authentication. 5000 random amplitude-only patterns are first generated and sequentially embedded into the SLM to modulate the propagating wave in the optical setup. Hence, a series of single-pixel intensity signals (e.g., 5000) can be correspondingly recorded by using single-pixel bucket detector (without spatial resolution). With the generated random amplitude-only patterns and all collected single-pixel data, it is straightforward to construct a diffraction intensity pattern just before the SLM by using correlation algorithm. The generated diffraction intensity pattern serves as reference, which is shown in Fig. 5(b). In the designed scattering environment, it is difficult to guess this reference, since scattering media, e.g., flexible use of different diffusers, are applied in practice.



(a) (b)

Fig. 5. (a) The region inside the dashed-line box to be used as an object in the experiments, and (b) a reference pattern generated just before the SLM.

Optics EXPRESS

To properly choose a nonlinear strength k for nonlinear correlation algorithm and the number of single-pixel intensity signals for the two developed decryption and authentication strategies, peak-to-correlation energy (PCE) is used here to analyze correlation distribution obtained between reference pattern and the decrypted pattern. The PCE is defined as a ratio between the maximum intensity peak value and the total energy of correlation output [21]. In this study, compression ratio used here is defined as the ratio between the number of randomly selected single-pixel intensity signals and the total number of the recorded single-pixel intensity signals.

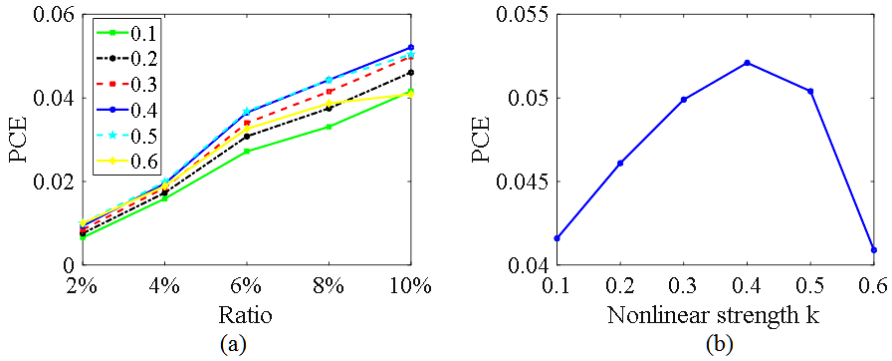


Fig. 6. Strategy I: (a) The PCE values versus compression ratios using different nonlinear strengths, and (b) the PCE values versus nonlinear strengths using a compression ratio of 10%.

In the decryption and authentication strategy I, PCE values are first calculated by using different compression ratios and different nonlinear strengths. As seen in Fig. 6(a), the higher PCE value means a better correlation, and the PCE values have a nearly linear growth with respect to the ratios. It is found that the developed optical authentication method shows good performance, when compression ratio is chosen as 10.0%. In this case, authentication quality is good, and simultaneously object information cannot be visually rendered. Using the compression ratio of 10%, there is a significant difference in the PCE values, when different nonlinear strengths are used, as illustrated in Fig. 6(b). It can also be seen in Fig. 6(b) that the PCE value has its maximum, when k is equal to 0.4. Hence, in the decryption and authentication strategy I, 10.0% single-pixel intensity signals (i.e., 500 recorded intensity signals) and their corresponding amplitude-only patterns are randomly selected. After 1-bit compression operation is applied to the randomly selected single-pixel intensity signals, binary signals are correspondingly obtained as ciphertext. The corresponding random amplitude-only patterns serve as principal keys for the decryption. Figure 7(a) shows a decrypted pattern obtained just before the SLM using the ciphertext and correct security keys, and compression ratio of 10.0% is applied. As seen in Fig. 7(a), the decrypted pattern does not visually render any plaintext. To verify the decrypted pattern, optical authentication using nonlinear correlation is further carried out between the decrypted pattern and the reference pattern given in Fig. 5(b), and the authentication distribution is shown in Fig. 7(b). Here, the optimized nonlinear strength of 0.4 is applied. It is clearly illustrated that only one sharp peak is generated in the nonlinear correlation map, hence the receiver possesses correct keys or is an authorized person. To illustrate discrimination capability of the proposed method, another object from the test sample USAF 1951 is generated, and its decrypted pattern obtained by using correct keys is also correlated with the reference pattern in Fig. 5(b). The optical authentication distribution is shown in Fig. 7(c), which contains only noisy background.

Optics EXPRESS

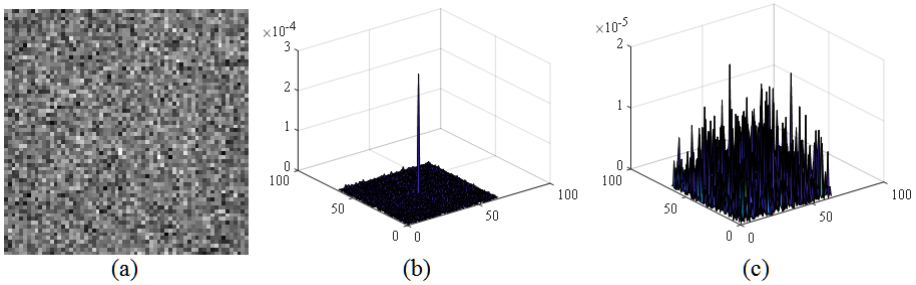


Fig. 7. (a) A decrypted pattern obtained by using correct security keys, (b) Nonlinear correlation map obtained between (a) and its reference pattern [i.e., Fig. 5(b)], and (c) nonlinear correlation map obtained between the decrypted pattern of another object and the reference pattern [i.e., Fig. 5(b)].

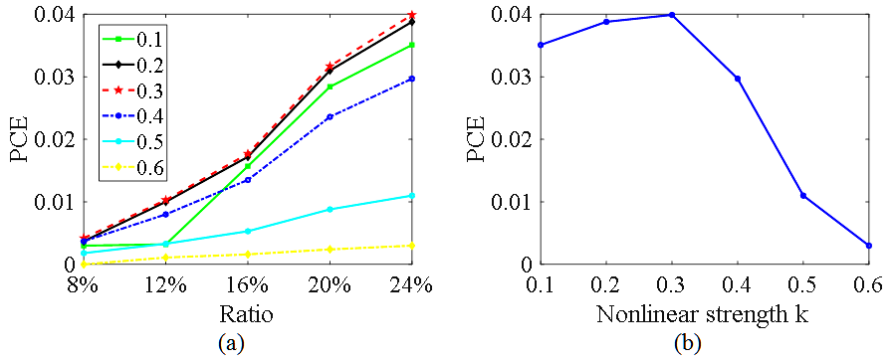


Fig. 8. Strategy II: (a) The PCE values versus compression ratios using different nonlinear strengths, and (b) the PCE values versus nonlinear strengths using a compression ratio of 24%.

In the decryption and authentication strategy II, PCE values are also calculated by using different compression ratios and different nonlinear strengths as shown in Fig. 8(a). In this case, it is found that when compression ratio is set as 24%, the nonlinear correlation map always has one sharp peak and a flat background. Simultaneously, the plaintext cannot be visually rendered. When compression ratio is selected as 24%, the PCE values obtained by using different nonlinear strengths are shown in Fig. 8(b). As seen in Fig. 8(b), the PCE value has its maximum, when k is equal to 0.3. Hence, in the decryption and authentication strategy II, compression ratio is set as 24% and nonlinear strength is set as 0.3. Here, the diffraction intensity pattern just before the SLM [i.e., reference stored in the database and shown in Fig. 5(b)] is further processed by using free-space wave propagation with supplementary security keys (e.g., axial distance of 2.0 cm), and an intensity pattern just behind the diffuser 2 is generated and used as a new reference as shown in Fig. 9(a). In this case, a decrypted intensity pattern just behind diffuser 2 can be generated via free-space wave propagation principle by using that in Fig. 7(a), which is shown in Fig. 9(b). In the decryption and authentication strategy II, supplementary keys, i.e., wavelength, pixel size and axial distance, are further used. The nonlinear correlation distribution generated between Figs. 9(a) and 9(b) is shown in Fig. 9(c). There is only one sharp peak in the generated nonlinear correlation map, which means that the receiver is an authorized person or has used correct security keys. Discrimination capability of the proposed method is further tested. When a decrypted pattern of another object (also from USAF 1951) obtained by using correct security keys is correlated with reference pattern in Fig. 9(a), the generated nonlinear correlation map contains only noisy background as shown in Fig. 9(d). In practice, axial distances can be flexibly used, such as 4.5 cm before the diffuser 2. Figures 10(a)–10(c) further show some decryption and authentication results, when a new reference pattern and a decrypted pattern are retrieved in

Optics EXPRESS

the object plane. In this case, axial distance of 4.5 cm, i.e., between the object plane and the SLM, is used.

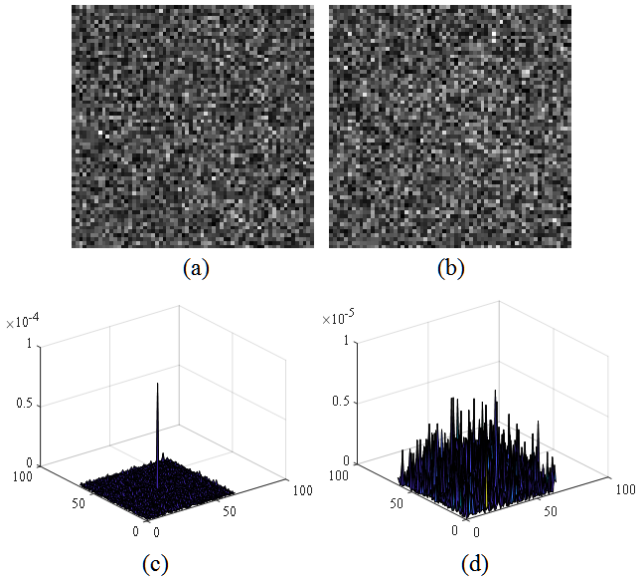


Fig. 9. Strategy II: (a) A new reference pattern (i.e., an intensity pattern just behind diffuser 2), (b) a decrypted pattern obtained just behind diffuser 2, (c) a nonlinear correlation map generated between (a) and (b), and (d) a nonlinear correlation map generated between a decrypted pattern of another object and reference pattern given in (a).

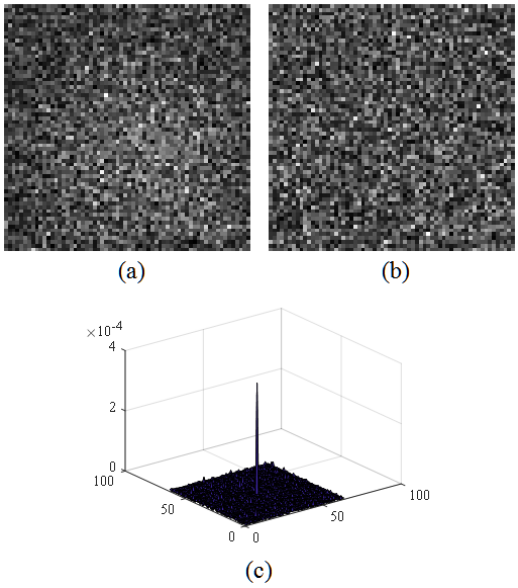


Fig. 10. (a) A diffraction intensity pattern retrieved in the object plane as a new reference, (b) a decrypted intensity pattern retrieved in the object plane, and (c) nonlinear correlation distribution generated between (a) and (b).

It is also found that when security keys are wrong during the decryption, the generated optical authentication distributions always contain only noisy background. Here, for the sake of brevity, only the PCE values using different axial distances are calculated in the decryption

Optics EXPRESS

and authentication strategy II, and the results corresponding to those in Fig. 9 are shown in Fig. 11. As seen in Fig. 11, there is the maximum PCE value only when a correct axial distance is used, and a difference from its correct axial distance value will lead to a decrease of PCE values calculated from the generated nonlinear correlation distribution.

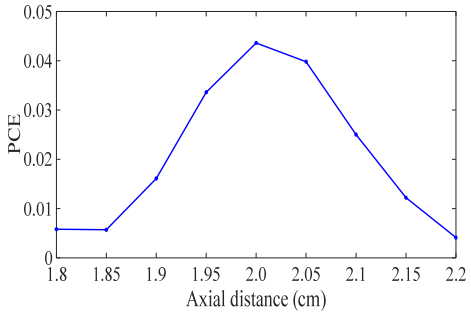


Fig. 11. The PCE values versus different axial distances in the decryption and authentication strategy II.

In practice, ciphertext could be further contaminated by noise during data storage or transmission. The ciphertext further contaminated by noise can be described by $B' = B + L \times G$, where B denotes binary signals (i.e., ciphertext), B' denotes the ciphertext contaminated by noise, L represents noise level, and G represents Gaussian noise with mean of 0 and variance of 1. The relationship between PCE values and noise levels is shown in Fig. 12(a). It is found that when the PCE value is larger than 0.01, there is an apparently sharp peak in the generated nonlinear correlation distributions. As shown in Fig. 12(a), in the decryption and authentication strategy I, the PCE values can be above 0.01 even when noise level achieves to 1. However, in the decryption and authentication strategy II, the PCE value is larger than 0.01 only when noise level is close to or smaller than 0.50. Hence, the decryption and authentication strategy I is more robust to noise contamination.

During data storage or transmission, occlusion contamination could also happen. Here, the loss percentage is defined as the ratio between the number of lost elements and the total number of elements in the ciphertext. As seen in Fig. 12(b), the decryption and authentication strategy I is more robust to information loss, since its tolerance to loss is more than 60.0%. In the decryption and authentication strategy II, the PCE value is above 0.01 only when loss level is smaller than 40.0%. Hence, there is a trade-off between the security and robustness against the contaminations. The decryption and authentication strategy II can achieve the higher security since supplementary keys are requested for the decryption, and the decryption and authentication strategy I can achieve the higher robustness against the contaminations.

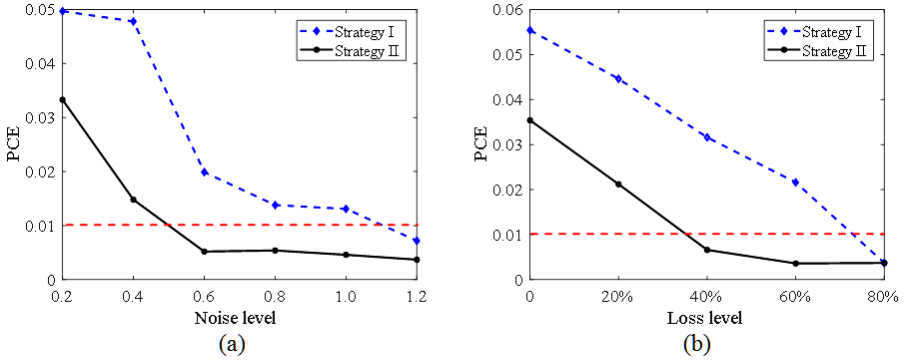


Fig. 12. (a) PCE values versus noise levels, and (b) PCE values versus loss levels.

Optics EXPRESS

4. Conclusions

We have proposed and experimentally verified a new GI-based authentication in scattering media, and complex environment has been effectively established for GI-based optical security for the first time to our knowledge. Feasibility and effectiveness of the proposed method have been experimentally demonstrated. Two decryption and authentication strategies have been developed, and the proposed method shows good performance. Although structured-detection-based GI in scattering media is studied here for optical security, it is straightforward to extend and apply the proposed method to other optical security methods. It is believed that the proposed method facilitates the investigation of optical security in scattering media which can open up a different research perspective for optical authentication.

Funding

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

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. X. F. Meng, L. Z. Cai, X. F. Xu, X. L. Yang, X. X. Shen, G. Y. Dong, and Y. R. Wang, "Two-step phase-shifting interferometry and its application in image encryption," Opt. Lett. **31**(10), 1414–1416 (2006).
3. 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. **38**(10), 1651–1653 (2013).
4. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photonics **1**(3), 589–636 (2009).
5. 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 **17**(25), 22462–22473 (2009).
6. X. Li, M. Zhao, Y. Xing, H. L. Zhang, L. Li, S. T. Kim, X. Zhou, and Q. H. Wang, "Designing optical 3D images encryption and reconstruction using monospectral synthetic aperture integral imaging," Opt. Express **26**(9), 11084–11099 (2018).
7. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," Opt. Lett. **38**(9), 1425–1427 (2013).
8. L. Chen and D. Zhao, "Optical image encryption with Hartley transforms," Opt. Lett. **31**(23), 3438–3440 (2006).
9. L. F. Chen, G. J. Chang, B. Y. He, H. D. Mao, and D. M. Zhao, "Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition," Opt. Lasers Eng. **88**, 221–232 (2017).
10. 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).
11. W. Chen and X. D. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**(22), 221106 (2013).
12. 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).
13. W. Chen and X. D. Chen, "Marked ghost imaging," Appl. Phys. Lett. **104**(25), 251109 (2014).
14. W. Chen, "Computer-generated hologram marked by correlated photon imaging," Appl. Opt. **57**(5), 1196–1201 (2018).
15. S. Li, X. R. Yao, W. K. Yu, L. A. Wu, and G. J. Zhai, "High-speed secure key distribution over an optical network based on computational correlation imaging," Opt. Lett. **38**(12), 2144–2146 (2013).
16. W. Chen, "Ghost identification based on single-pixel imaging in big data environment," Opt. Express **25**(14), 16509–16516 (2017).
17. Y. Qin and Y. Y. Zhang, "Information encryption in ghost imaging with customized data container and XOR operation," IEEE Photonics J. **9**(2), 7802208 (2017).
18. W. Chen and X. 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. S. Liansheng, C. Yin, L. Bing, T. Ailing, and A. K. Asundi, "Optical image encryption via high-quality computational ghost imaging using iterative phase retrieval," Laser Phys. Lett. **15**(7), 075204 (2018).
21. 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).
22. X. D. Chen, *Computational Methods for Electromagnetic Inverse Scattering* (Wiley-IEEE, 2018).
23. J. W. Goodman, *Introduction to Fourier Optics* (McGraw–Hill, 1996).