https://dx.doi.org/10.1016/j.optlaseng.2020.106045

Secured single-pixel ghost holography

Yin Xiao,[1] Lina Zhou,[1] 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
*Email: owen.chen@polyu.edu.hk

Abstract

In this paper, we propose and experimentally demonstrate a new optical security method using single-pixel ghost holography. The plaintext is optically encoded into a series of single-pixel data using the designed single-pixel ghost holography, and then a digital hologram just before spatial light modulator (SLM) is retrieved by using a correlation algorithm with all recorded single-pixel data to be stored as a reference in a database. Subsequently, some recorded single-pixel data are randomly selected, and random amplitude-only patterns corresponding to those selected single-pixel data serve as principal security keys. Other parameters, e.g., wavelength and axial distance, can be used as additional security keys. The 1-bit quantization operation is further applied to process those randomly-selected single-pixel data in order to generate binary signals as ciphertext. Finally, different strategies are developed and applied for optical authentication of the decrypted holograms or decrypted objects. Numerical analyses and optical experiments demonstrate that the proposed method possesses high security, high flexibility and high discrimination capability. It is also illustrated that the proposed method possesses high robustness against contaminations. It is believed that the proposed method can provide a promising strategy for greatly enriching optical security field. @ Elsevier, 2019.

Keywords: ghost holography; optical security; optical encryption; optical authentication; single-pixel detection; experimental demonstration

1. Introduction

Optical techniques have been developed rapidly over the past few decades, and have shown a great potential for information security due to their inherent characteristics, e.g., parallel processing, high speed processing and high degrees of freedom (such as wavelength, amplitude, phase, distance and polarization). In the process of optical encryption the original information (i.e., plaintext) is transformed into noise-like pattern (i.e., ciphertext), and in the process of optical decryption the plaintext can be extracted from ciphertext by using correct security keys. A simple and effective optical encryption system has been developed based on double random phase encoding (DRPE), which was first proposed by Refregier and Javidi [1]. However, it has been found that the DRPE scheme is vulnerable to the attacks [2–7] when some preset conditions are used. Various optical techniques and algorithms [8,9], such as asymmetric structure, have been further developed for optically securing information to enhance the security. Recently, it has also been found that optical authentication [10–12] can be further carried out over optical encryption layers to enhance optical system security.

In the optical security field, holography is a promising technique [13–15], since it has significant advantages for encoding amplitude and phase [16]. In the early period, photosensitive medium, such as photographic plate, was utilized to record interference patterns, and applications of conventional holographic methods are limited by the low efficiency and complicated procedure. Emergence of digital holography effectively resolves the problems to some extent, which utilizes 2D charged-coupled device (CCD) to record digital holograms. Digital holography has shown a great potential in many fields, e.g., biological imaging [17–19], optical encryption [20,21] and object recognition [22]. However, there are still some limitations which affect the application of digital holography to optical security, e.g., the low flexibility for designing various optical security systems due to only the usage of 2D CCD camera. It has been recently demonstrated that ghost imaging (GI) can also be used to optically encrypt and decrypt information, and the GI has obvious advantages in the conditions of low light and non-visible wavelength, especially in scattering environments [23–28]. The GI usually uses single-pixel detector to record the ciphertext during optical encryption. Hence, the GI can provide a way to resolve the problems existing in digital holography-based security systems, and can be effectively used to extend the applications of digital holography for optical encryption and authentication. Different from CCD camera with spatial resolution, the single-pixel bucket detector used in the GI does not have spatial resolution. In the GI-based security system, the decryption can be conducted by using various algorithms [29–33], and a commonly-used algorithm is developed by using higher-order intensity correlation [34–38]. Until now, no work has been conducted for optical encryption and authentication using single-pixel ghost holography to address the concerns about low system flexibility existing in conventional holography-based security systems. It is also desirable to exploiting practical methods for optical encryption and authentication using single-pixel ghost holography.

In this paper, we propose and demonstrate optical encryption and authentication based on single-pixel ghost holography. The plaintext is encoded into a series of single-pixel data using the designed single-pixel ghost holography, and then a digital hologram just before spatial light modulator (SLM) is retrieved by using correlation algorithm with all recorded single-pixel data as a reference. Subsequently, some recorded single-pixel data are randomly selected, and random amplitude-only patterns corresponding to those selected measurements serve as principal security keys. Other parameters, e.g., wavelength and axial distance, are used as additional security keys. The 1-bit quantization operation is further applied to process those randomly-selected single-pixel data in order to generate binary signals as ciphertext. Finally, two different strategies are proposed for optical authentication of the decrypted patterns without visually observing original information. In the first optical authentication strategy, ciphertext and security keys are used to generate a decrypted hologram just before the SLM. The decrypted hologram is further correlated with reference hologram (i.e.,

retrieved by using all recorded single-pixel data) stored in a database by using nonlinear correlation algorithm [12,39–42]. In the second optical authentication strategy, a reference object is further obtained from reference hologram by using free-space wave propagation principle [43,44] with additional security keys, and a decrypted object is also obtained from the decrypted hologram by using additional security keys. Subsequently, nonlinear correlation between reference object and the decrypted object is carried out. Numerical analyses and optical experimental results demonstrate that the proposed method possesses high flexibility, high security and high discrimination capability. The proposed method is also found to be robust against contaminations, which makes it meaningful in practical applications.

2. Principles

A schematic experimental setup for the proposed method is shown in Fig. 1. A laser beam is expanded by a pinhole and collimated by a lens. The laser beam is split into two beams by using a beam splitter cube, and the two beams are respectively called object wave and reference wave. The object wave interferes with reference wave just before the SLM plane. Here, in-line digital holography is studied with single-pixel structured detection architecture. The interference pattern is further modulated sequentially by a series of random amplitude-only patterns embedded in the SLM, and the total light intensity is sequentially collected by a single-pixel bucket detector without spatial resolution. Using the total number of measurements (e.g., 5000 recordings), a digital hologram just before the SLM can be retrieved by using a correlation algorithm [34–38] to be stored as a reference in a database, which can be further arranged in practice to be invisible to all receivers.

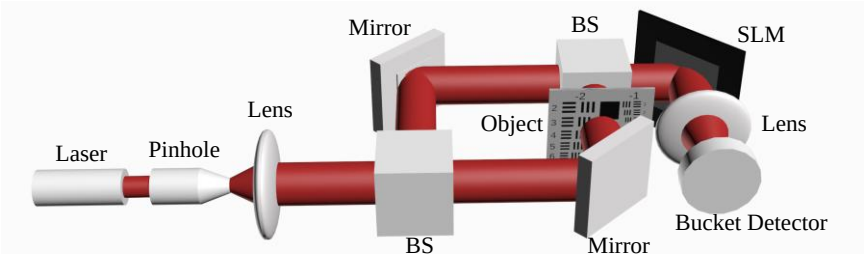

Fig. 1. Schematic experimental setup for the proposed method. SLM: spatial light modulator; BS, beam splitter.

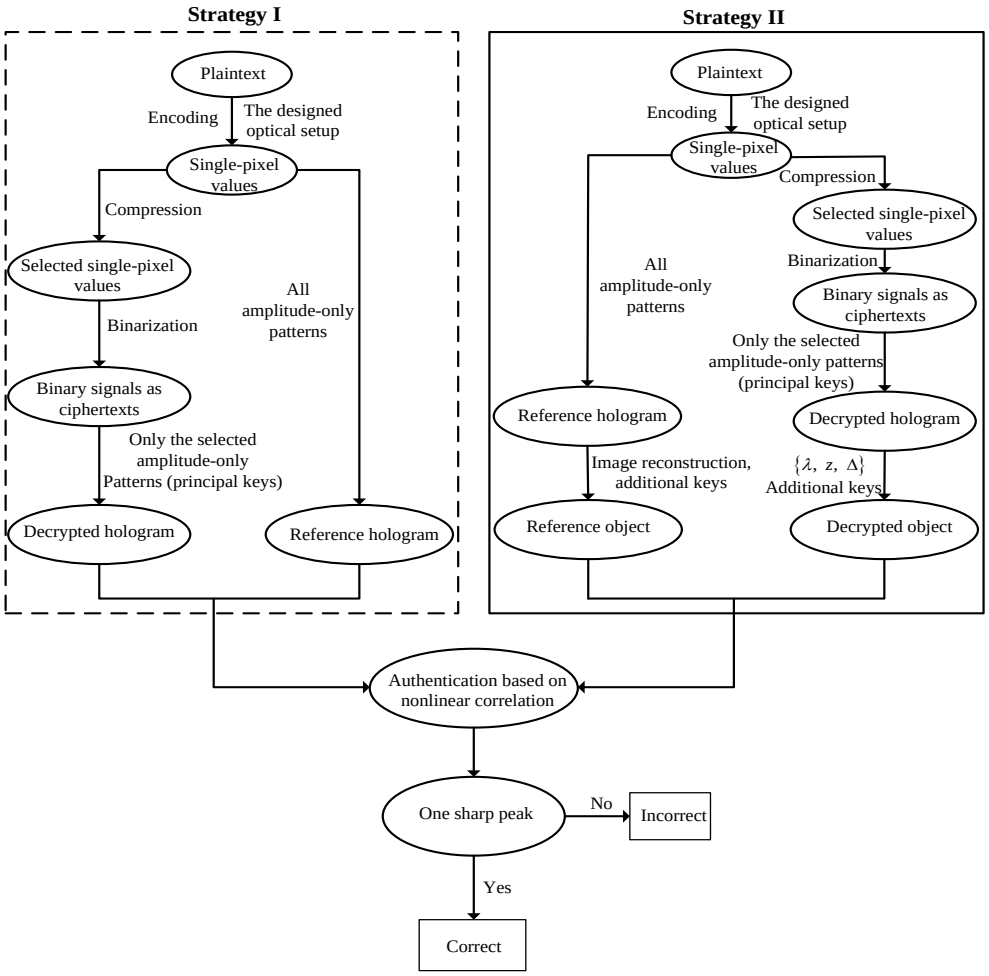

Fig. 2. Flow chart for the proposed secured single-pixel ghost holographic method.

As shown in Fig. 1, when a series of random amplitude-only patterns are sequentially embedded into the SLM, a series of single-pixel data can be correspondingly collected by a single-pixel bucket detector. Correlation algorithm [34–38] is first utilized to retrieve digital hologram just before the SLM, which is stored in a database as reference hologram, i.e., H_{ref}. Then, some recorded single-pixel data are randomly selected, and random amplitude-only patterns corresponding to these selected single-pixel data serve as principal security keys. The unselected single-pixel data and the unselected random amplitude-only patterns are discarded. Subsequently, 1-bit quantization operation is further applied to process the selected single-pixel values to generate binary signals as ciphertext. If value of the selected single-pixel data is larger than their mean value, it is set as 1. Otherwise, it is set as 0. When ciphertext and principal security keys are applied by using correlation algorithm [34–38], a decrypted hologram H_{dec} just before the SLM is obtained. Finally, the decrypted hologram is nonlinearly correlated with reference hologram for optical authentication. The above process is called "the first optical authentication strategy" in this study.

In the designed optical security system, wavelength λ, axial distance z and pixel size Δ can be used as additional security keys. In this case, optical authentication can be carried out between decrypted object and reference object. The decrypted object O_{dec} is further obtained from the decrypted hologram by using free-space wave propagation principle [43,44], and reference object can be further obtained from reference hologram stored in the database by using free-space wave propagation principle [43,44]. Finally, the decrypted object is nonlinearly correlated with reference object for optical authentication without visually observing original information. The above process is called "the second optical authentication strategy". A flow chart to clearly show the proposed method is given in Fig. 2.

3. Results and discussion

Simulations and optical experiments are carried out to verify effectiveness and flexibility of the proposed method. In the simulations and optical experiments, objects with size of 64×64 pixels are studied, and the total number of measurements used to retrieve reference hologram just before the SLM is 5000.

3.1 Nonlinearity strength and compression ratio

To choose a proper nonlinearity strength k and an appropriate number of the selected single-pixel data for the proposed optical authentication strategies, peak-to-correlation energy (PCE) is used here to analyze correlation results obtained between references and the decrypted patterns, which is defined as a ratio between the maximum intensity peak value and the total energy of correlation output. Data compression approaches are also used in the proposed method, and compression ratio is defined as the number of randomly selected single-pixel data over the total number of all recorded single-pixel data.

Figure 3(a) shows an object used as a typical example for analyzing a proper nonlinearity strength k and an appropriate number of the randomly selected single-pixel data for the proposed optical authentication strategies. Figure 3(b) shows a reference hologram retrieved just before the SLM generated from that in Fig. 3(a) by using all recorded single-pixel data.

(a) (b)

Fig. 3. (a) An object (i.e., plaintext), and (b) reference hologram retrieved just before the SLM.

3.1.1 Optical authentication between reference hologram and decrypted hologram

Using ciphertext and the corresponding random amplitude-only patterns, a decrypted hologram just before the SLM can be retrieved by using a correlation algorithm [34–38]. When different compression ratios and different nonlinearity strengths are used, the PCE values are correspondingly obtained as shown in Fig. 4(a). The higher PCE value means a better correlation. As the compression ratio increases, the PCE value increases accordingly. A larger compression ratio means that more recorded single-pixel data is selected and applied in this study, therefore more effective information is contained in the decrypted hologram and the higher PCE value can be correspondingly obtained.

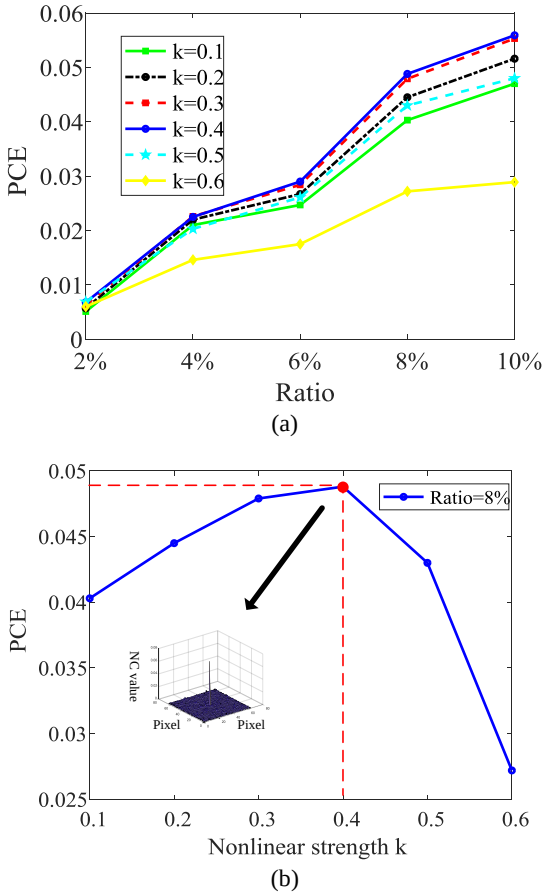

Fig. 4. (a) The PCE values versus compression ratios using different nonlinearity strengths, and (b) the PCE values versus nonlinearity strengths with a certain compression ratio. The inset in (b) shows a generated nonlinear correlation map when k is set as 0.4 and compression ratio is 8.0%.

To choose a proper nonlinearity strength, the PCE values obtained by using different nonlinearity strengths with a certain compression ratio are obtained and shown in Fig. 4(b). As can be seen in Fig. 4(b), when k is equal to 0.4, the PCE has its maximum. It is found in this study that nonlinearity strength k of 0.4 is also suitable for optically authenticating other plaintexts. Hence, the nonlinearity strength is set as 0.4 for the first optical authentication strategy. It is also found that the generated nonlinear correlation maps always contain only one single sharp peak, when compression ratio is larger than 4.0% and the nonlinearity strength is set as 0.4. Compression ratio of 8.0% is used as a typical example for numerical analyses in this study, when the first optical authentication strategy, i.e., authentication between reference hologram and the decrypted hologram, is applied.

3.1.2 Optical authentication between reference object and decrypted object

In the second optical authentication strategy, other parameters, e.g., wavelength λ, axial distance z and pixel size Δ, are used as additional security keys. Nonlinear correlation is conducted between reference object and decrypted object. In this case, the PCE values obtained by using different nonlinearity strengths and different compression ratios are shown in Fig. 5(a). It is found that when compression ratio is larger than 12.0%, only one single

remarkable peak appears in the generated nonlinear correlation maps. With a fixed compression ratio (e.g., 18.0%), the PCE values obtained by using different nonlinearity strengths are shown in Fig. 5(b), and the PCE values reach the maximum when k is equal to 0.3. Hence, compression ratio is set as 18.0% to be used as a typical example for numerical analyses and nonlinearity strength k is fixed as 0.3, when the second optical authentication strategy is applied.

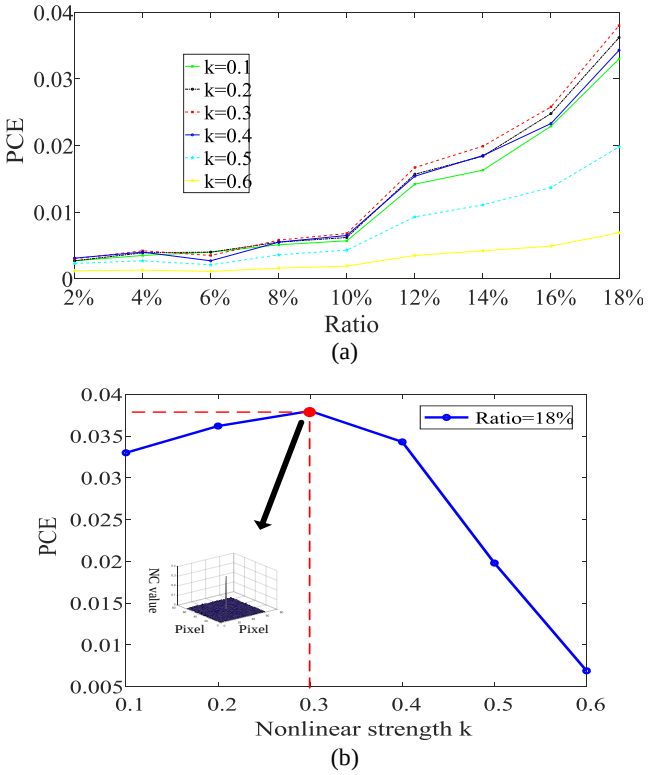

Fig. 5. (a) The PCE values versus compression ratios using different nonlinearity strengths, and (b) the PCE values versus nonlinearity strengths when a certain compression ratio is used. The inset in (b) shows a generated nonlinear correlation map when nonlinearity strength k is 0.3 and compression ratio is 18.0%.

3.2 Nonlinear correlation for optical authentication

To show feasibility and effectiveness of the proposed method, three different kinds of objects shown in Figs. 6(a)–6(c) are further tested.

(a) (b) (c)

Fig. 6. Three images as objects: (a) characters, (b) fingerprint and (c) face.

Reference holograms corresponding to the three objects in Figs. 6(a)–6(c) are first retrieved, and are respectively shown in Figs. 7(a)–7(c). Random amplitude-only patterns

corresponding to the randomly-selected single-pixel data serve as principal security keys. The randomly-selected single-pixel data is further processed by using 1-bit quantization operation to generate binary signals as ciphertext. When ciphertext and correct principal security keys are used, decrypted holograms just before the SLM are correspondingly obtained as respectively shown in Figs. 7(d)–7(f). It can be seen in Figs. 7(d)–7(f) that the decrypted holograms cannot visually render any information. Nonlinear correlations between the decrypted holograms and reference holograms are further implemented, which are shown in Figs. 7(g)–7(i). The generated correlation results mean that optical authentications are correctly carried out, and the receiver is an authorized person or has all correct security keys.

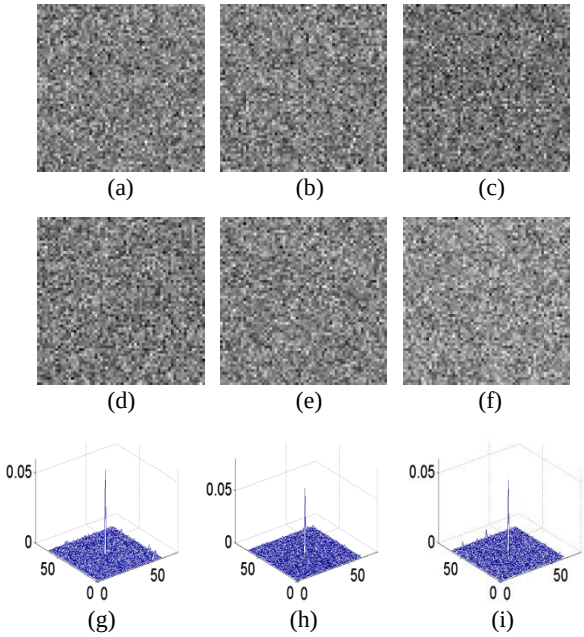

Fig. 7. (a)–(c) Reference holograms obtained just before the SLM by using correct principal security keys respectively corresponding to the three objects in Figs. 6(a)–6(c), (d)–(f) decrypted holograms obtained just before the SLM by using correct principal security keys, and (g)–(i) nonlinear correlation maps obtained between reference holograms and the decrypted holograms.

Reference objects are further obtained from the retrieved reference holograms by using free-space wave propagation principle [43,44] with additional security keys (e.g., wavelength, axial distance and pixel size), as respectively shown in Figs. 8(a)–8(c). Decrypted objects are also obtained from the retrieved decrypted holograms by using free-space wave propagation principle [43,44] with additional security keys as shown in Figs. 8(d)–8(f). In the second optical authentication strategy, nonlinear correlation maps obtained between reference objects and the decrypted objects are respectively shown in Figs. 8(g)–8(i). It can be seen in Figs. 8(g)–8(i) that when correct security keys are used, decrypted objects can be correctly authenticated. It also means that the receiver is an authorized person or has all correct security keys.

To further illustrate discrimination capability of the proposed method, another three fingerprint objects similar to that in Fig. 6(b) are used as typical examples, as respectively shown in Figs. 9(a)–9(c).

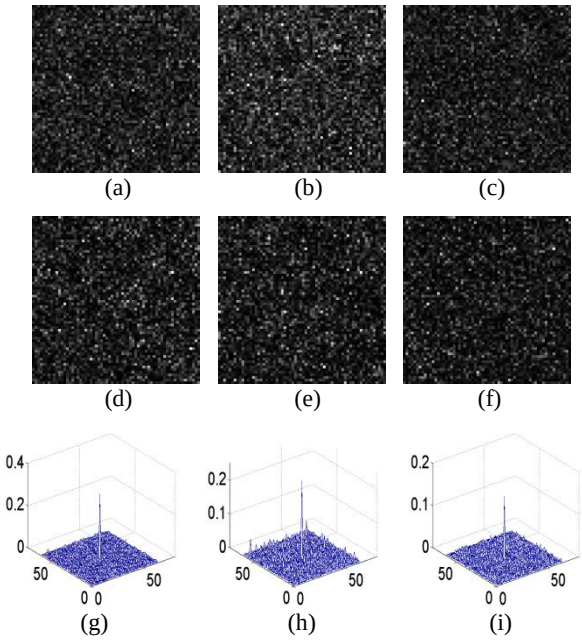

Fig. 8. (a)–(c) Reference objects obtained by using correct additional security keys respectively corresponding to the three objects in Figs. 6(a)–6(c), (d)–(f) decrypted objects obtained by using correct additional security keys, and (g)–(i) nonlinear correlation maps obtained between reference objects and the decrypted objects.

Fig. 9. (a) F1: fingerprint 1, (b) F2: fingerprint 2, and (c) F3: fingerprint 3.

Figures 10(a)–10(o) show optical decryption and authentication results using the first optical authentication strategy, in which reference holograms and the decrypted holograms are nonlinearly correlated. The reference holograms retrieved just before the SLM are shown in Figs. 10(a)–10(c) which respectively correspond to objects F1, F2 and F3 in Figs. 9(a)–9(c), and the decrypted holograms are also obtained and shown in Figs. 10(d), 10(h) and 10(l), respectively. Here, the decrypted holograms are obtained by using correct principal security keys (i.e., the corresponding random amplitude-only patterns) and ciphertext. When a decrypted hologram is correlated with its correspondingly correct reference hologram stored in a database, only one single sharp peak appears as illustrated in Figs. 10(e), 10(j) and 10(o). When incorrect reference holograms are used, the generated nonlinear correlation maps show only noisy backgrounds which can be seen in Figs. 10(f), 10(g), 10(i), 10(k), 10(m) and 10(n). Hence, it is illustrated that a decrypted hologram retrieved just before the SLM can be correctly authenticated by using only its corresponding reference hologram stored in the database, and the proposed optical authentication strategy, i.e., the authentication strategy I, possesses high discrimination capability.

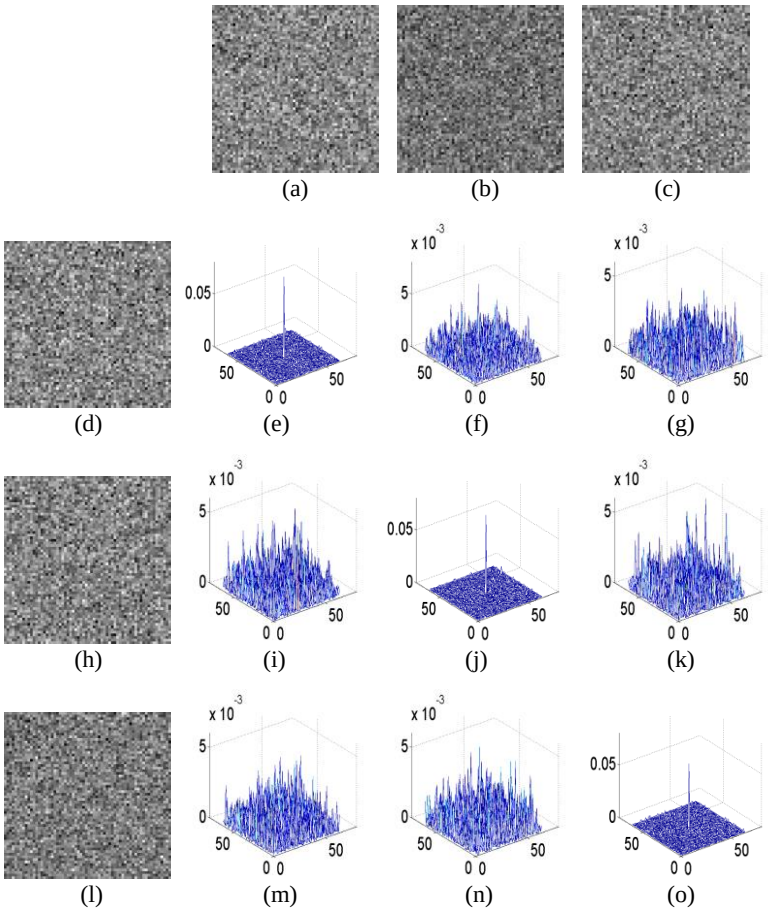

Fig. 10. (a)–(c) Reference holograms H_{ref1}, H_{ref2} and H_{ref3} respectively corresponding to objects F1, F2 and F3 in Figs. 9(a)–9(c), (d), (h), (l) decrypted holograms H_{dec1}, H_{dec2} and H_{dec3}, (e), (j) and (o) nonlinear correlation maps obtained between the decrypted holograms and their correspondingly correct reference holograms, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps obtained between the decrypted holograms and incorrect reference holograms.

In the second optical authentication strategy, reference objects are obtained from their corresponding reference holograms H_{ref1}, H_{ref2} and H_{ref3} in Figs. 10(a)–10(c) by using free-space wave propagation principle with additional security keys (e.g., wavelength, axial distance and pixel size), as respectively shown in Figs. 11(a)–11(c). Decrypted objects are obtained from the decrypted holograms by using free-space wave propagation principle with additional security keys (e.g., wavelength, axial distance and pixel size), as respectively shown in Figs. 11(d), 11(h) and 11(l). As can be seen in Figs. 11(e), 11(j) and 11(o), the decrypted objects are correctly authenticated by using their corresponding reference objects. When incorrect reference objects are used, only noisy backgrounds are generated in the nonlinear correlation maps, as shown in Figs. 11(f), 11(g), 11(i), 11(k), 11(m) and 11(n). It is illustrated that a decrypted object can be correctly authenticated by using only its corresponding reference object by using the nonlinear correlation algorithm. It is also demonstrated that the second optical authentication strategy possesses high discrimination capability.

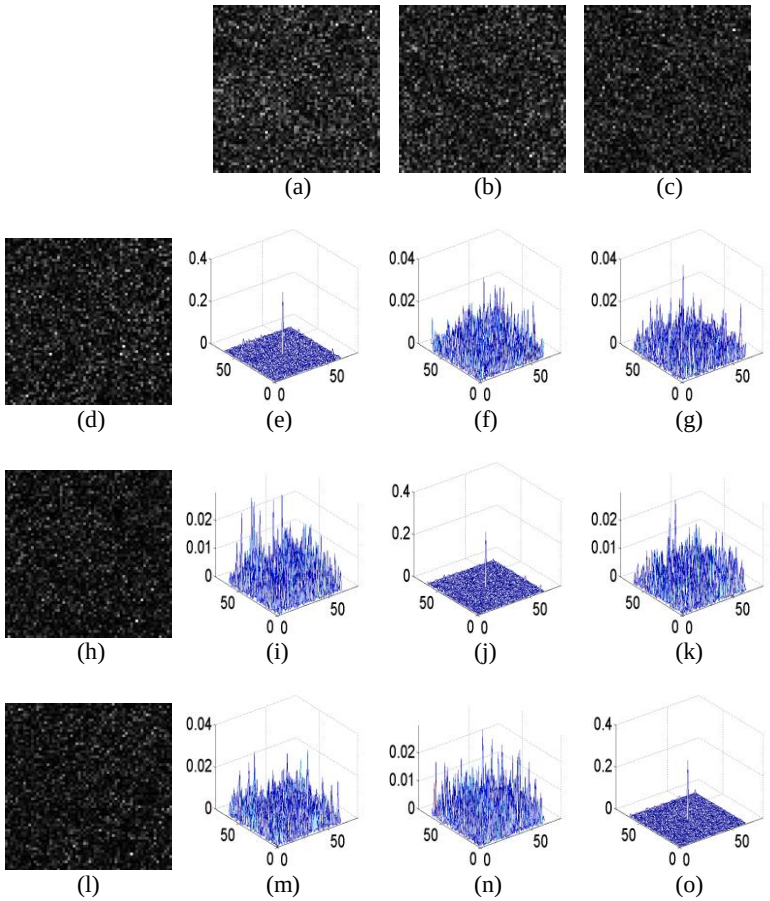

Fig. 11. (a)–(c) Reference objects O_{ref1}, O_{ref2} and O_{ref3} respectively corresponding to objects F1, F2 and F3 in Figs. 9(a)–9(c), (d), (h), (l) decrypted objects O_{dec1}, O_{dec2} and O_{dec3}, (e), (j) and (o) nonlinear correlation maps obtained between the decrypted objects and their corresponding reference objects, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps obtained between the decrypted objects and incorrect reference objects.

3.3 Optical authentication using wrong security keys for the decryption

To analyze security of the proposed secured single-pixel ghost holographic method, nonlinear correlation results are also obtained when security keys are incorrectly used for the decryption followed by optical authentication.

For the first optical authentication strategy, when wrong random amplitude-only patterns are used for the decryption, reference holograms, decrypted holograms and the corresponding optical authentication distributions are respectively shown in Figs. 12(a)–12(o). Figures 12(a)–12(c) show reference holograms H_{ref1}, H_{ref2} and H_{ref3} which respectively correspond to the objects F1, F2 and F3 in Figs. 9(a)–9(c). For the unauthorized persons who use wrong random amplitude-only patterns, decrypted holograms just before the SLM are obtained and shown in Figs. 12(d), 12(h) and 12(l). As can be seen in Figs. 12(e)–12(g), 12(i)–12(k) and 12(m)–12(o), the decrypted holograms cannot be correctly correlated with reference hologram stored in the database, and all generated nonlinear correlation maps contain only noisy backgrounds which mean unsuccessfully optical authentication. It is also demonstrated that the proposed method is of high security.

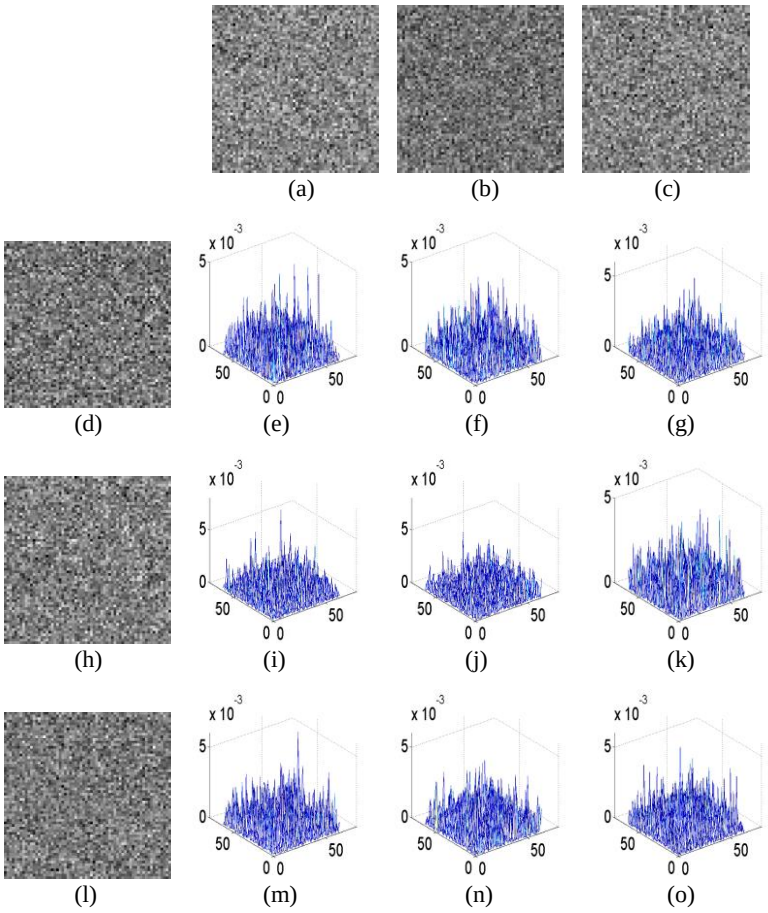

Fig. 12. (a)–(c) Reference holograms H_{ref1}, H_{ref2} and H_{ref3} respectively corresponding to F1, F2 and F3 in Figs. 9(a)–9(c), (d), (h), (l) the decrypted holograms H_{dec1}, H_{dec2} and H_{dec3} obtained by using wrong amplitude-only patterns, and (e)–(g), (i)–(k) and (m)–(o) nonlinear correlation maps obtained between reference holograms and the decrypted holograms. In this case, wrong random amplitude-only patterns are used for the decryption to generate the decrypted holograms.

In the second optical authentication strategy, it is found that nonlinear correlation results are further sensitive to additional security keys, e.g., wavelength and axial distance. An error existing in additional security keys can lead to incorrect optical information authentication. For the sake of brevity, we only show the optical authentication distributions obtained by using wrong axial distances, which are shown in Figs. 13(a)–13(o). It is found that the effect of other additional security keys is similar.

Reference objects in Figs. 13(a)–13(c) are the same as those shown in Figs. 11(a)–11(c). However, decrypted objects in Figs. 13(d), 13(h), 13(l) are obtained by using a wrong axial distance. The correct axial distance is 0.02 m in the proposed optical encryption setup, and an axial distance of 0.022 m is used to conduct the decryption here. As can be seen in Figs. 13(e), 13(j) and 13(o), although there is a small error only in the axial distance, the nonlinear correlation maps obtained between the decrypted objects and reference objects show only noisy backgrounds. Other generated nonlinear correlation maps shown in Figs. 13(f), 13(g), 13(i), 13(k), 13(m) and 13(n) also contain only noisy patterns, when incorrect reference objects are used for optical authentication.

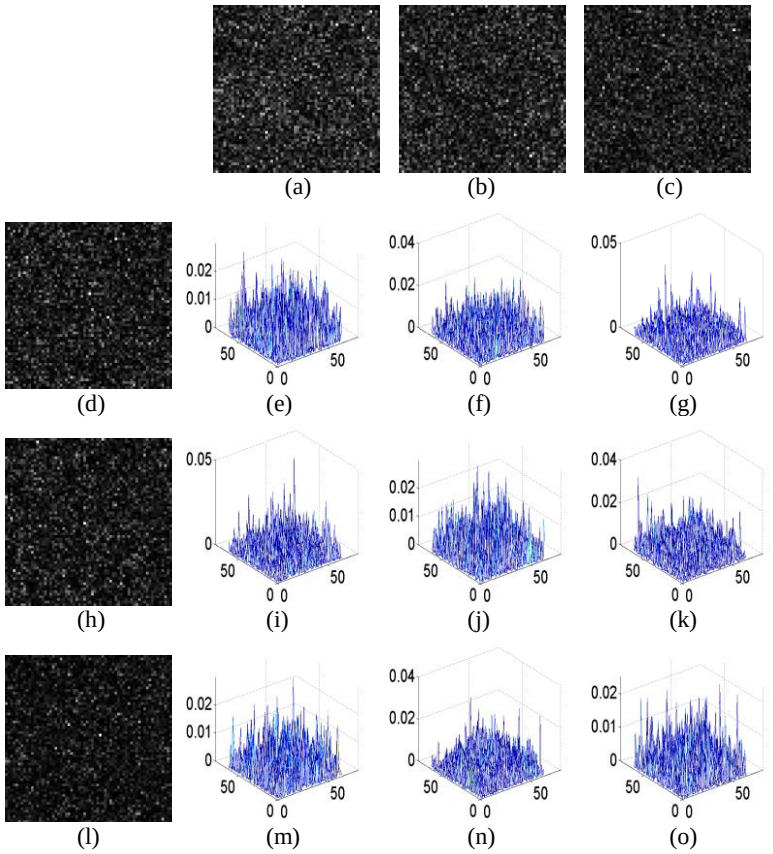

Fig. 13. (a)–(c) Reference objects O_{ref1}, O_{ref2} and O_{ref3} respectively corresponding to F1, F2 and F3 in Figs. 9(a)–9(c), (d), (h) and (l) the decrypted objects O_{dec1}, O_{dec2} and O_{dec3} obtained by using wrong axial distance, and (e)–(g), (i)–(k) and (m)–(o) nonlinear correlation maps obtained between reference objects and the decrypted objects. In this case, wrong axial distance is used for the decryption to generate the decrypted objects.

To illustrate that the second optical authentication strategy is sensitive to additional security keys, the PCE values are further obtained by using different axial distances. Here, for the sake of brevity, the correlations between reference object O_{ref1} and decrypted object O_{dec1} are implemented. As can be seen in Fig. 14, when the correct axial distance (i.e., 0.02 m) is used, the PCE value is the largest. A small error in the axial distance can lead to a dramatic decrease in the PCE values. In this case, it is assumed that all other security keys are correct.

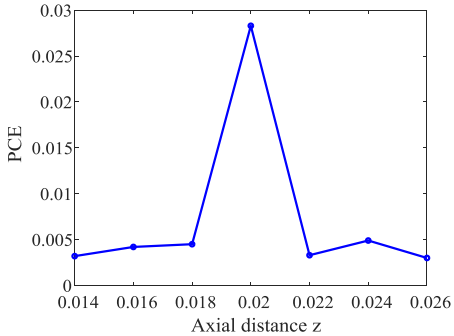

Fig. 14. The PCE values versus axial distances.

3.4 Noise and occlusion contaminations

3.4.1 Noise contamination

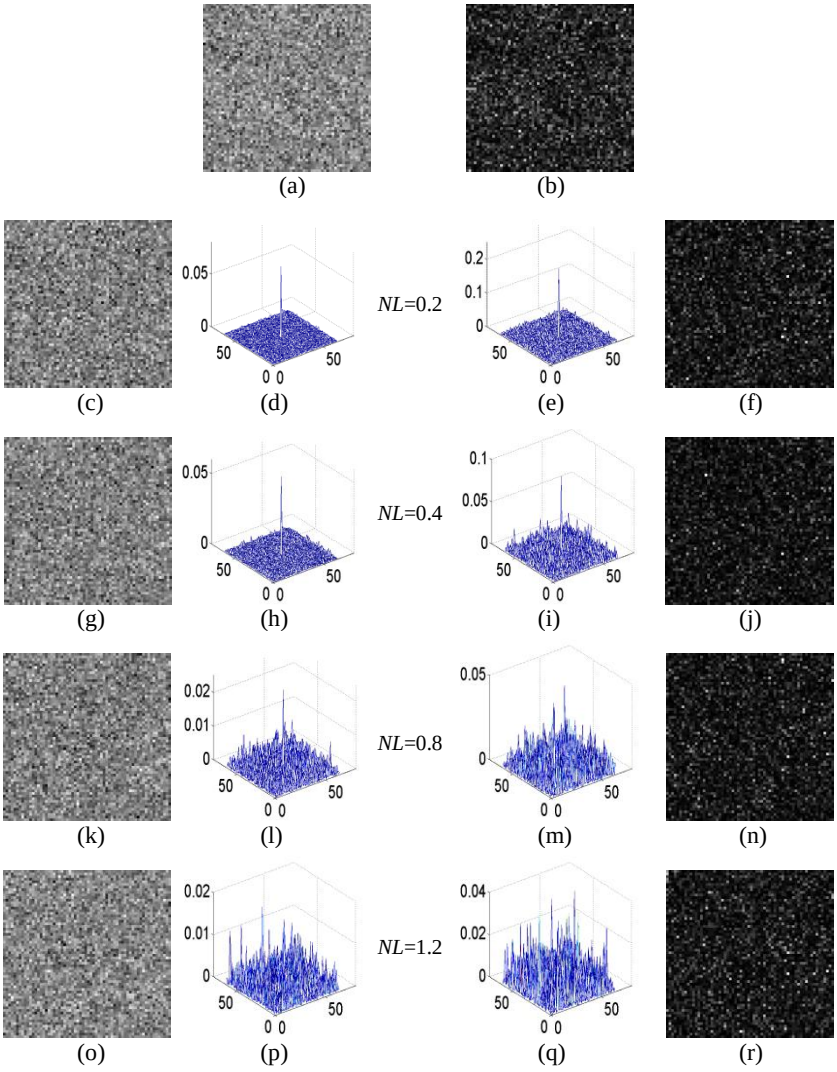

Fig. 15. (a) Reference hologram H_{ref1} corresponding to F1 in Fig. 9(a), (b) reference object O_{ref1} obtained from H_{ref1}, (c), (g), (k) and (o) decrypted holograms respectively obtained by using noise level of 0.2, 0.4, 0.8 and 1.2 in the ciphertext, (d), (h), (l) and (p) nonlinear correlation maps generated between reference holograms and the decrypted holograms, (f), (j), (n) and (r) decrypted objects respectively obtained by using noise levels of 0.2, 0.4, 0.8 and 1.2 in the ciphertext, and (e), (i), (m) and (q) nonlinear correlation maps obtained between reference objects and the decrypted objects.

In practice, the recorded ciphertext could be further contaminated during date storage or transmission, e.g., noise and occlusion. Here, noisy ciphertext is described by $B' = B + NL \times G$, where B denotes binary signals (i.e., ciphertext), B' denotes ciphertext contaminated by noise, NL represents noise level, and G represents Gaussian noise with mean of 0 and variance of 1.0. Figure 15(a) shows a reference hologram H_{ref1} obtained from object F1 in Fig. 9(a), and Fig. 15(b) shows a reference object O_{ref1} further obtained from reference hologram H_{ref1}.

When noise level is respectively set as 0.2, 0.4, 0.8 and 1.2, four decrypted holograms are correspondingly retrieved and shown in Figs. 15(c), 15(g), 15(k) and 15(o), respectively. Four decrypted objects are further obtained from the decrypted holograms as respectively shown in Figs. 15(f), 15(j), 15(n) and 15(r). Nonlinear correlation maps obtained between reference hologram H_{ref1} and the four decrypted holograms are shown in Figs. 15(d), 15(h), 15(l) and 15(p), respectively. Nonlinear correlation maps obtained between reference object O_{ref1} and the four decrypted objects are shown in Figs. 15(e), 15(i), 15(m) and 15(q), respectively. For nonlinear correlation obtained between reference hologram and the decrypted holograms, it can be seen that when the noise level is smaller than 0.4, the generated nonlinear correlation map has only one sharp peak. For nonlinear correlation maps obtained between reference object and the decrypted objects, the sharp peak appears when the noise level is close to 0.2. Hence, it is illustrated that the first optical authentication strategy is more robust to noise contamination compared with the second strategy. When the noise is large (e.g., NL=1.2), the two optical authentication strategies cannot work and there is only noisy background in the generated nonlinear correlation maps.

The trend of PCE values corresponding to different noise levels is further studied and shown in Fig. 16. For the first optical authentication strategy, the PCE values can keep to be above 0.02 when the noise level reaches 0.4. For the second optical authentication strategy, the PCE values are larger than 0.02, when noise levels are smaller than 0.2.

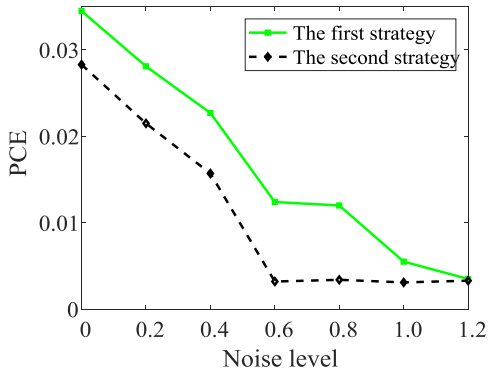

Fig. 16. The PCE values versus noise levels.

3.4.2 Occlusion contamination

During the transmission or storage, data loss or occlusion contamination could also happen. Here, it is assumed that some single-pixel data from the ciphertext are further considered to be lost or occluded. The loss percentage is defined as a ratio between the number of lost single-pixel data in the ciphertext and the total number of elements in the ciphertext.

Figures 17(a) and 17(b) respectively show reference hologram H_{ref1} and reference object O_{ref1} corresponding to object F1 in Fig. 9(a). When loss level is respectively set as 20.0%, 40.0%, 60.0% and 80.0%, four decrypted holograms are correspondingly retrieved and shown in Figs. 17(c), 17(g), 17(k) and 17(o), respectively. Four decrypted objects are further obtained from the decrypted holograms as respectively shown in Figs. 17(f), 17(j), 17(n) and 17(r). Nonlinear correlation maps obtained between reference hologram H_{ref1} and the four decrypted holograms are shown in Figs. 17(d), 17(h), 17(l) and 17(p), respectively. Nonlinear correlation maps obtained between decrypted objects O_{ref1} and the four decrypted objects are shown in Figs. 17(e), 17(i), 17(m) and 17(q), respectively. As can be seen in Figs. 17(a)–17(r), the proposed method is also robust to occlusion contamination. The first optical authentication strategy is feasible when the information loss achieves 40.0%. In the case of a

small loss (e.g., 20.0%), the two authentication strategies show high robustness against occlusions. When the loss is large (e.g., 80.0%), no much information is available for correct authentication and nonlinear correlation maps render only noisy backgrounds.

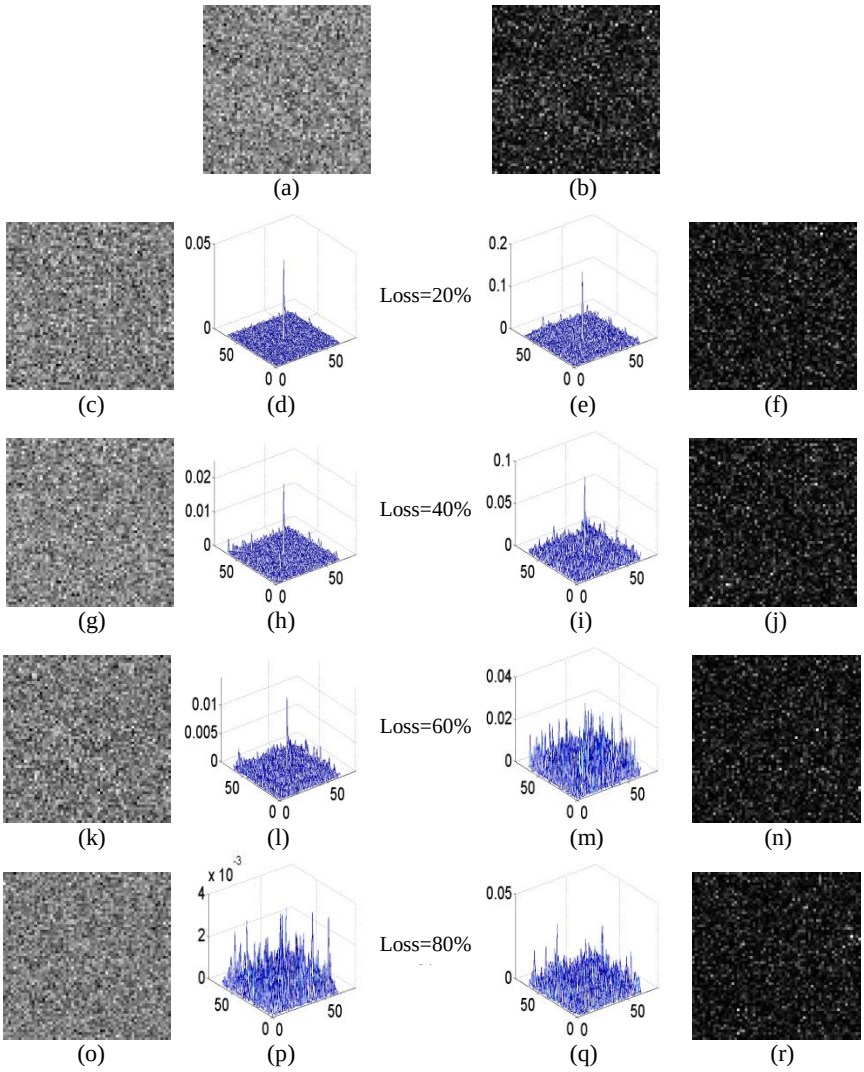

Fig. 17. (a) Reference hologram H_{ref1} corresponding to F1 in Fig. 9(a), (b) reference object O_{ref1} obtained from H_{ref1}, (c), (g), (k) and (o) decrypted holograms respectively obtained by using loss levels of 20.0%, 40.0%, 60.0% and 80.0% in the ciphertext, (d), (h), (l) and (p) nonlinear correlation maps obtained between reference hologram and the decrypted holograms, (f), (j), (n) and (r) decrypted objects respectively obtained by using loss levels of 20.0%, 40.0%, 60.0% and 80.0% in the ciphertext, and (e), (i), (m) and (q) nonlinear correlation maps obtained between reference object and the decrypted objects.

Figure 18 shows a relationship between different loss levels and the PCE values. It is found that the first authentication strategy performs better in the case of ciphertext loss, since its maximum loss level can achieve 40.0%. Although the loss level with around 20.0% in the second optical authentication strategy is allowed, it is still feasible for practical applications. These results and discussion demonstrate that the proposed method possesses high robustness

against ciphertext loss or occlusions. The first optical authentication strategy performs better when there is a contamination, and the second optical authentication strategy can achieve the higher security since additional security keys are requested for the decryption before the authentication.

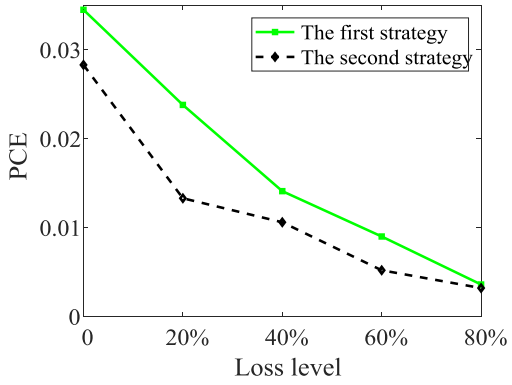

Fig. 18. The PCE values versus ciphertext loss levels.

3.5 Optical experiments

Optical experimental setup shown in Fig. 1 is further conducted to verify feasibility and effectiveness of the proposed method. The illumination source used in our experiment is a He-Ne laser beam with wavelength of 633.0 nm. Axial distance from the object to the SLM is 2.0cm. The SLM (Holoeye, LC-R720) is used to sequentially modulate the interference pattern, and pixel size of the SLM is $20.0\mu m$. It is worth noting that a series of random amplitude-only patterns are generated and sequentially embedded into the SLM, and the SLM performs amplitude modulation in optical experiments. A single-pixel bucket detector (Newport, 918D-UV-OD3R) without spatial resolution is used, which is connected to a power meter (Newport, 1936-R) to obtain experimental data, i.e., single-pixel sequence.

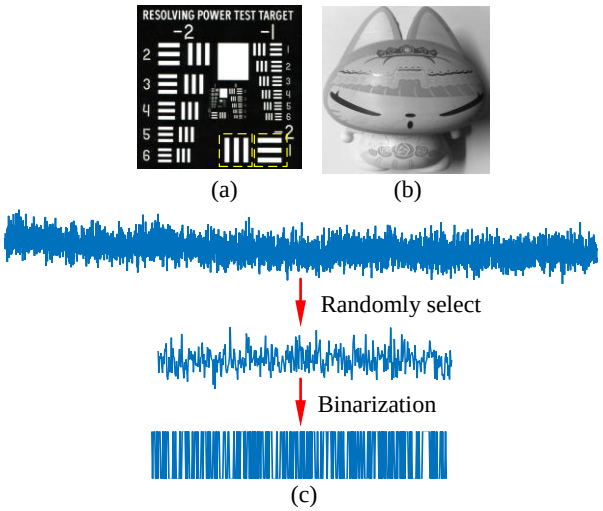

Fig. 19. (a) Transmission patterns used in the experiments (the regions inside the dashed boxes respectively act as two objects in optical experiments), i.e., the left one: object 1; the right one: object 2, (b) a reflective object (used in optical experiment) called as object 3, and (c) a typical ciphertext-generation procedure for the proposed method.

In optical experiments, an USAF1951 resolution target is used and placed in the optical path, and two parts of the target are chosen to respectively serve as two transmission objects (i.e., object 1 and object 2) as indicated in Fig. 19(a). In addition, a reflective object, called object 3, is also used, which is shown in Fig. 19(b). A typical ciphertext-generation procedure for the proposed method is illustrated in Fig. 19(c).

Using the proposed method, three reference holograms just before the SLM are correspondingly retrieved and stored in a database as respectively shown in Figs. 20(a)–20(c), which cannot be directly viewed by the receivers. Ciphertext and principal security keys are used to retrieve the decrypted holograms just before the SLM, which are shown in Figs. 20(d), 20(h) and 20(l). Nonlinear correlation maps obtained between reference holograms and the decrypted holograms are shown in Figs. 20(e)–20(g), 20(i)–20(k) and 20(m)–20(o). It can be seen that only the correlation maps obtained between the decrypted holograms and the correspondingly correct reference holograms can generate correct authentication results, as respectively shown in Figs. 20(e), 20(j) and 20(o). When incorrect reference holograms are used for the authentication, there are only noisy backgrounds in the generated nonlinear correlation maps, as shown in Figs. 20(f), 20(g), 20(i), 20(k), 20(m) and 20(n). The experimental results are in accordance with the aforementioned numerical analyses.

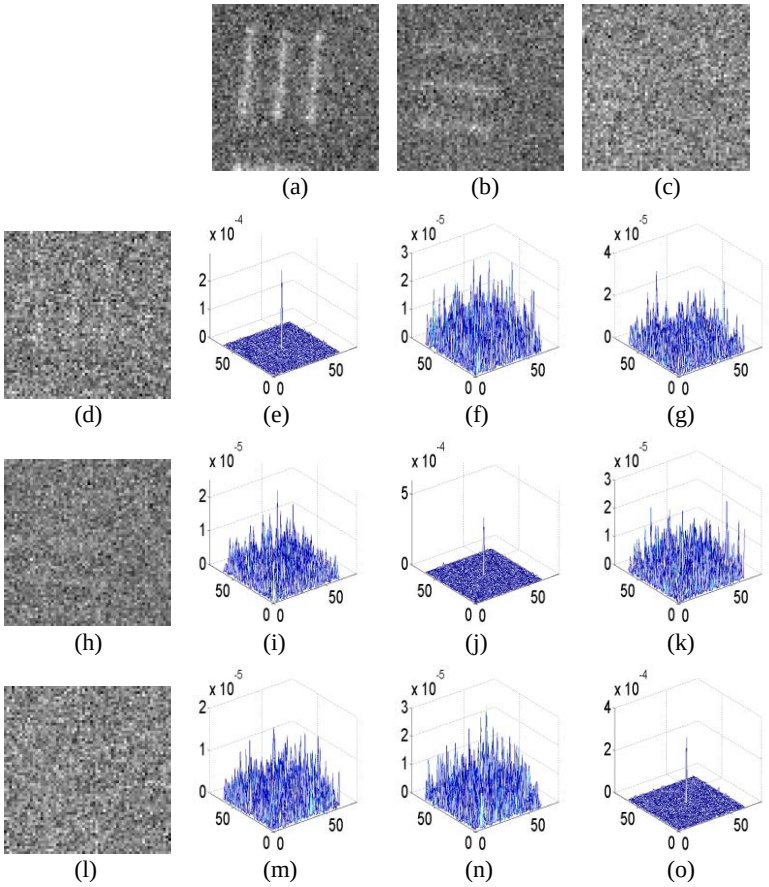

Fig. 20. (a)–(c) Reference holograms H_{ref1}, H_{ref2} and H_{ref3} respectively corresponding to object 1, object 2 and object 3 in Fig. 19, (d), (h) and (l) decrypted holograms H_{dec1}, H_{dec2} and H_{dec3} by using correct security keys, (e), (j) and (o) nonlinear correlation maps obtained between decrypted holograms and the corresponding reference holograms, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps obtained between the decrypted holograms and incorrect reference holograms.

In the second optical authentication strategy, reference objects shown in Figs. 21(a)–21(c) are further obtained respectively from reference holograms H_{ref1}, H_{ref2} and H_{ref3} in Figs. 20(a)–20(c) by using free-space wave propagation principle [43,44] with additional security keys. Decrypted objects shown in Figs. 21(d), 21(h) and 21(l) are further obtained from the decrypted holograms H_{dec1}, H_{dec2} and H_{dec3} in Figs. 20(d), 20(h) and 20(l), respectively. Correct optical authentication maps are obtained when the decrypted objects are correlated with their correspondingly correct reference objects, as shown in Figs. 21(e), 21(j) and 21(o). Optical authentication results are also obtained as shown in Figs. 21(f), 21(g), 21(i), 21(k), 21(m) and 21(n), when the decrypted objects are correlated with incorrect reference objects. The experimental results are also in accordance with the aforementioned numerical analyses. Numerical analyses and optical experimental results systematically demonstrate that the proposed method is feasible and effective.

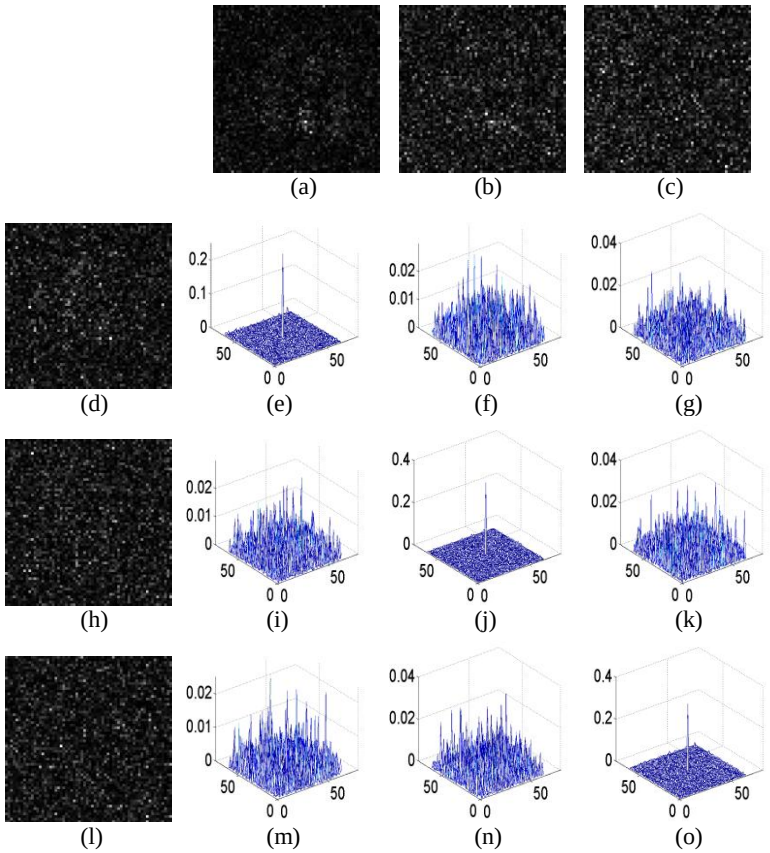

Fig. 21. (a)–(c) Reference objects O_{ref1}, O_{ref2} and O_{ref3} respectively corresponding to object 1, object 2 and object 3 in Fig. 19, (d), (h) and (l) decrypted objects O_{dec1}, O_{dec2} and O_{dec3} obtained by using correct security keys, (e), (j) and (o) nonlinear correlation maps obtained between the decrypted objects and their corresponding reference objects, and (f), (g), (i), (k), (m) and (n) nonlinear correlation maps obtained between the decrypted objects and incorrect reference objects. In this case, compression ratio is set as 20.0% to be used as a typical example, and nonlinearity strength k is set as 0.3.

Here, robustness against the contaminations is also studied for the proposed method by using optical experimental data. The proposed method is first tested when there is noise contamination to the ciphertext, i.e., respectively with noise levels of 0.1, 0.2, 0.3 and 0.4.

Figures 22(a) and 22(b) show reference hologram and reference object corresponding to object 1 in Fig. 19(a), respectively. Figures 22(c), 22(g), 22(k) and 22(o) show four decrypted holograms retrieved just before the SLM respectively corresponding to noise levels of 0.1, 0.2, 0.3 and 0.4. As can be seen in Figs. 22(d), 22(h), 22(l) and 22(p), nonlinear correlation maps generated between reference hologram and the decrypted holograms contain only one sharp peak and flat background. Four decrypted objects are further obtained from the decrypted holograms as respectively shown in Figs. 22(f), 22(j), 22(n) and 22(r). Nonlinear correlation maps obtained between reference object and the decrypted objects are shown in Figs. 22(e), 22(i), 22(m) and 22(q). It is also experimentally demonstrated that the proposed method possesses high robustness against noise contaminations to the ciphertext.

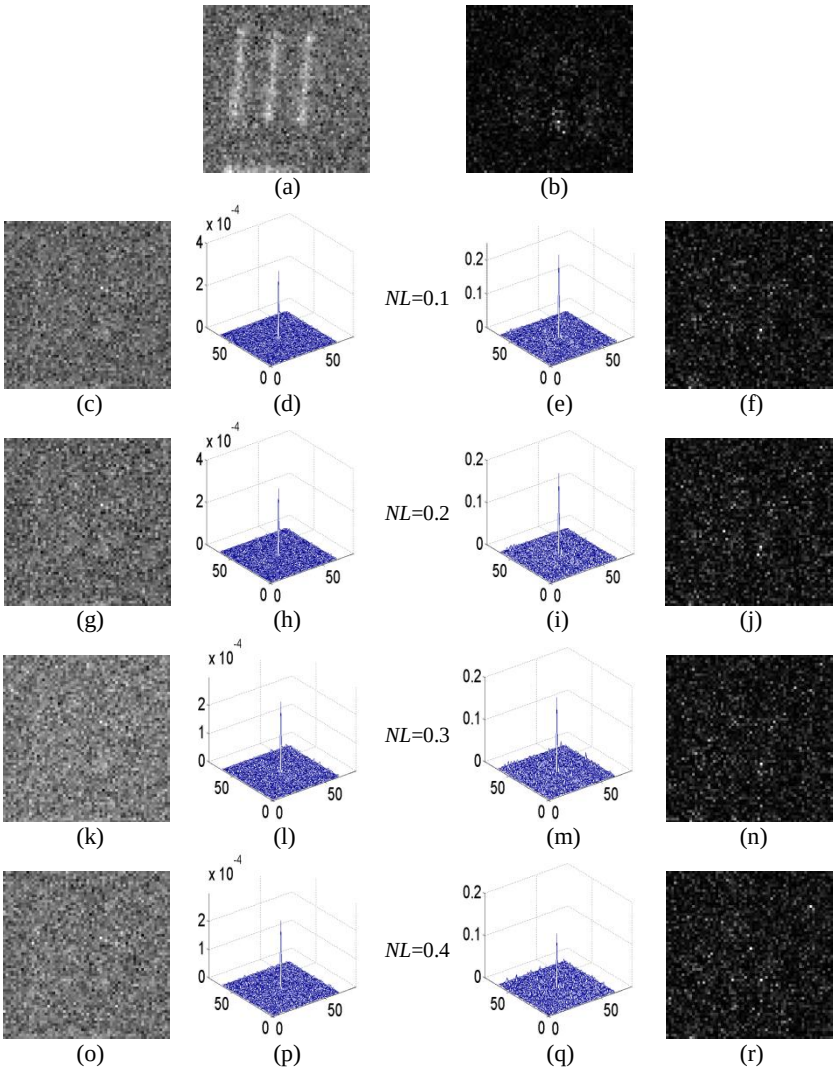

Fig. 22. (a) Reference hologram H_{ref1} corresponding to object 1 in Fig. 19(a), (b) reference object O_{ref1} further obtained from H_{ref1}, (c), (g), (k) and (o) the decrypted holograms obtained respectively corresponding to noise levels of 0.1, 0.2, 0.3 and 0.4 in the ciphertext, (d), (h), (l) and (p) nonlinear correlation maps generated between reference hologram and the decrypted holograms, (f), (j), (n) and (r) the decrypted objects respectively further obtained from the decrypted holograms, and (e), (i), (m) and (q) nonlinear correlation maps obtained between reference object and the decrypted objects.

Robustness against occlusion contamination is also evaluated for the proposed method by using the experimental data. Figures 23(a) and 23(b) show reference hologram and reference object corresponding to object 1 in Fig. 19(a), respectively. When there is a loss level of 10.0%, 20.0%, 30.0% and 40.0% respectively in the ciphertext, four decrypted holograms are obtained as respectively shown in Figs. 23(c), 23(g), 23(k) and 23(o). Four decrypted objects are further retrieved as respectively shown in Figs. 23(f), 23(j), 23(n) and 23(r). Nonlinear correlation maps generated between reference hologram and the decrypted holograms are respectively shown in Figs. 23(d), 23(h), 23(l) and 23(p), and nonlinear correlation maps generated between reference object and the decrypted objects are respectively shown in Figs. 23(e), 23(i), 23(m) and 23(q). It is experimentally demonstrated that the proposed method also possesses high robustness against occlusion contaminations to the ciphertext.

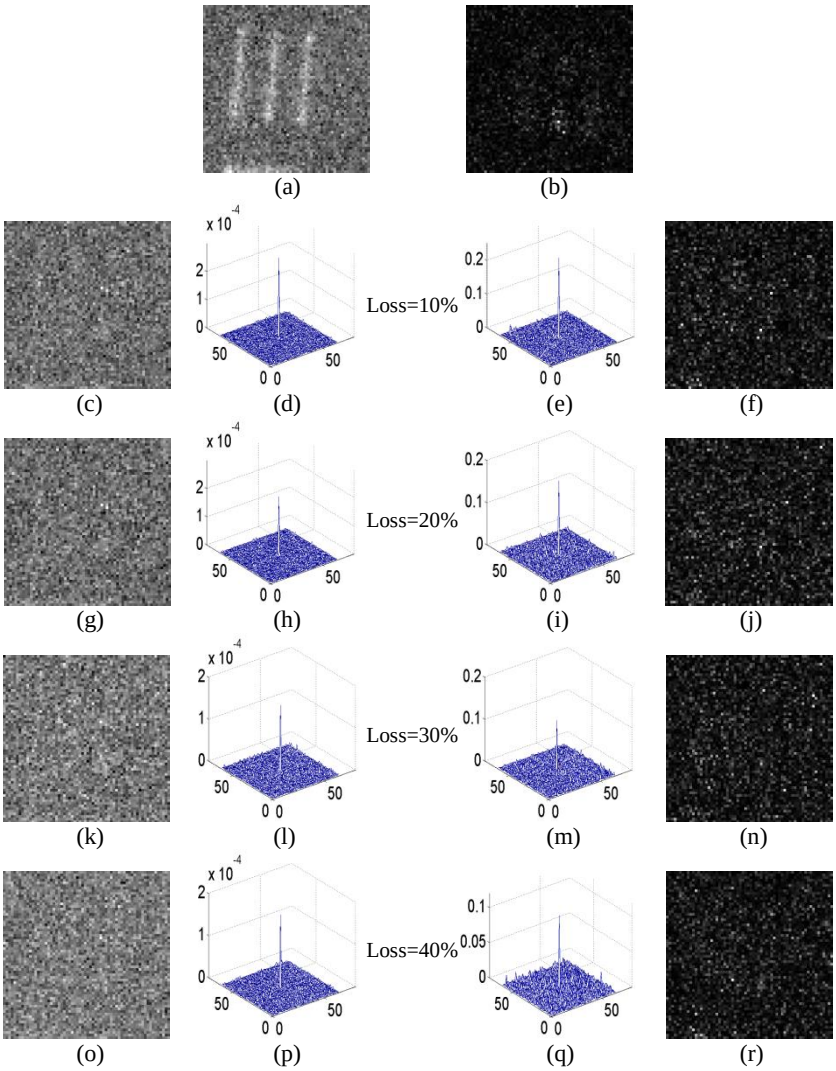

Fig. 23. (a) Reference hologram H_{ref1} corresponding to object 1 in Fig. 19(a), (b) reference object O_{ref1} further obtained from H_{ref1}, (c), (g), (k) and (o) decrypted holograms obtained respectively corresponding to a loss level of 10.0%, 20.0%, 30.0% and 40.0% in the ciphertext, (d), (h), (l) and (p) nonlinear correlation maps generated between reference hologram and the decrypted holograms, (f), (j), (n) and (r) decrypted objects respectively obtained from the decrypted holograms, and (e), (i), (m) and (q) nonlinear correlation maps obtained between reference object and the decrypted objects.

4. Conclusions

In this paper, single-pixel ghost holography has been proposed for optical authentication-based security. Numerical analyses and optical experimental results systematically demonstrate that the proposed method is feasible and effective, and can effectively resolve the problems existing in conventional holography-based optical security systems. The designed optical setup is promising for securing information, and the proposed method could open up a different research perspective for optical security. Although in-line digital holographic principle is studied and integrated with single-pixel structured detection architecture, it could be straightforward to flexibly apply other holographic setups and integrate them with the designed single-pixel structured detection architecture for optical encryption and authentication. Different optical authentication strategies have been further developed and applied for effectively verifying the decrypted information, which can also enhance system flexibility. It is believed that the proposed method can be flexibly applied in practice for securing information, and can provide a promising approach for greatly enriching single-pixel optical security.

Acknowledgements

This work was financially supported by National Natural Science Foundation of China (NSFC) (61605165), Hong Kong Research Grants Council (25201416), and Shenzhen Science and Technology Innovation Commission through Basic Research Program (JCYJ20160531184426473).

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] 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).

[4] 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).

[5] 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).

[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] M. H. Liao, W. Q. He, D. J. Lu and X. Peng, "Ciphertext-only attack on optical cryptosystem with spatially incoherent illumination: from the view of imaging through scattering medium," Sci. Rep. 7, 41789 (2017).

[8] 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).

[9] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. 6(2), 120–155 (2014).

[10] 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).

[11] W. Chen and X. D. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL 110(4), 44002 (2015).

[12] 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).

[13] S. Lai and M. A. Neifeld, "Digital wavefront reconstruction and its application to image encryption," Opt. Commun. 178(4–6), 283–289 (2000).

[14] T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng. 43(10), 2233–2238 (2004).

[15] 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).

[16] 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).

[17] 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).
[18] B. Kemper and G. von Bally, "Digital holographic microscopy for live cell applications and technical inspection," Appl. Opt. 47(4), A52– A61 (2008).
[19] 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).
[20] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. 1(3), 589–636 (2009).
[21] G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. 30(11), 1306–1308 (2005).
[22] A. Nelleri, U. Gopinathan, J. Joseph, and K. Singh, "Three dimensional object recognition from digital Fresnel hologram by wavelength matched filtering," Opt. Commun. 259(2), 499–506 (2006).
[23] J. H. Shapiro, "Computational ghost imaging," Phys. Rev. A 78(6), 061802R (2008).
[24] Y. Bromberg, O. Katz, and Y. Silberberg, "Ghost imaging with a single detector," Phys. Rev. A 79(5), 053840 (2009).
[25] 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).
[26] W. Chen and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," Opt. Lasers Eng.73, 123–127 (2015).
[27] W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. 103(22), 221106 (2013).
[28] 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).
[29] M. F. Duarte, M. A. Davenport, D. Takhar, J. N. Laska, T. Sun, K. F. Kelly, R. G. Baraniuk, "Single-pixel imaging via compressive sampling," IEEE Signal Process Mag. 25(2), 83–91 (2008).
[30] 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).
[31] Z. B. Zhang, X. Ma, and J. G. Zhong, "Single-pixel imaging by means of Fourier spectrum acquisition," Nat. Commun. 6, 6225 (2015).
[32] S. S. Welsh, M. P. Edgar, R. Bowman, P. Jonathan, B. Q. Sun, and M. J. Padgett, "Fast full-color computational imaging with single-pixel detectors," Opt. Express 21(20), 23068–23074 (2013).
[33] M. J. Sun, M. P. Edgar, D. B. Phillips, G. M. Gibson, and M. J. Padgett, "Improving the signal-to-noise ratio of single-pixel imaging using digital microscanning," Opt. Express 24(10), 10476–10485 (2016).
[34] 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).
[35] P. L. Zhang, W. L. Gong, X. Shen, and S. S. Han, "Correlated imaging through atmospheric turbulence," Phys. Rev. A 82(3), 033817 (2010).
[36] 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).
[37] F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, "Differential ghost imaging," Phys. Rev. Lett. 104(25), 253603 (2010).
[38] B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, "Normalized ghost imaging," Opt. Express 20(15), 16892–16901 (2012).
[39] B. Javidi, "Nonlinear joint power spectrum based optical correlation," Appl. Opt. 28(12), 2358–2367 (1989).
[40] 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).
[41] W. Chen, "Hierarchically optical double-image correlation using 3D phase retrieval algorithm in fractional Fourier transform domain," Opt. Commun. 427, 374–381 (2018).
[42] W. Chen, "3D Gerchberg-Saxton optical correlation," IEEE Photon. J. 10(2), 7800409 (2018).
[43] J. W. Goodman, *Introduction to Fourier Optics* (McGraw–Hill, 1996).
[44] X. D. Chen, Computational Methods for Electromagnetic Inverse Scattering (Wiley-IEEE, 2018).