The following publication Wen Chen, "Optical cryptosystem based on single-pixel encoding using the modified Gerchberg–Saxton algorithm with a cascaded structure," J. Opt. Soc. Am. A 33, 2305-2311 (2016) is available at https://doi.org/10.1364/JOSAA.35.001074.

Optical cryptosystem based on single-pixel encoding using the modified Gerchberg-Saxton algorithm with a cascaded structure

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, an optical cryptosystem is developed based on single-pixel encoding using the modified Gerchberg-Saxton algorithm with a cascaded structure. A series of random intensity-only patterns are pre-generated as principal security keys, and phase-only masks for optical encoding and decoding are generated by the modified Gerchberg-Saxton algorithm with a cascaded structure. Subsequently, a series of 1D intensity points, i.e., ciphertexts, are recorded by single-pixel detector, which may provide a potential for establishing low-cost and compact security systems. The phase-mask generation process can be flexibly designed by modifying Gerchberg-Saxton algorithm with a cascaded structure, hence high sensitivity and the large indirect space for phase can be guaranteed. It is also illustrated that compared with previous works, the higher eavesdropping percentage is requested to the attackers in the proposed single-pixel optical cryptosystem. The proposed method using a cascaded structure provides a novel strategy for single-pixel intensity-modulated optical security. © 2016 Optical Society of America

OCIS codes: *(200.4740) Optical processing; (110.1758) Computational imaging; (200.4560) Optical data processing.*

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

1. INTRODUCTION

Optical encryption approaches [1–9] have attracted more and more current attention for information security due to their remarkable advantages, such as multiple dimensions and parallel processing. The optical encryption approach, i.e., double random phase encoding, was first proposed by Refregier and Javidi [1]. It has been demonstrated that the input image can be converted into stationary white noise by using two statistically-independent random phase-only maps respectively placed in the input plane and spatial frequency domain [1]. Different domains have been continuously integrated for enriching optical security, such as Fresnel [10,11]. A number of infrastructures [12–21], such as holography [2,12], joint transform correlator [14], diffractive imaging [16] and asymmetry [18,20,21], have been designed and applied for optical encoding and decoding. Some recent advances on optical security can be further found in Ref. [6].

In conventional optical security systems, two-dimensional (2D) detectors are usually applied for recording the ciphertexts. In recent years, it has been found that imaging with single-pixel detector provides an effective alternative for optical encryption [22–24]. In single-pixel optical encryption systems, a series of random phase-only masks (or the simply-converted forms), such as 20000, are directly applied as principal security keys, and system flexibility is limited to some extent. In addition, each pixel value in phase-only masks is distributed in the range of $[0, 2\pi]$, and does not possess high data space, i.e., usually smaller than 3 bits. Although intensity modulation strategies [25,26] have been applied in single-pixel secured imaging system, it is still desirable that more alternatives can be continuously developed. As indicated in Refs. [25,26], new alternatives can be further designed to enrich or improve single-pixel intensity-modulated optical security approach, such as to achieve the higher eavesdropping percentage.

In this paper, inspired by the work in Refs. [25,26], an optical cryptosystem is further presented based on single-pixel encoding using the modified Gerchberg-Saxton algorithm with a cascaded structure. Different from conventional approaches [22–24,27], a series of random intensity-only patterns are pre-generated as principal security keys, and phase-only masks for optical encoding and decoding are generated by the modified Gerchberg-Saxton algorithms with a cascaded structure. Phase-mask generation process can be flexibly designed by modifying the Gerchberg-Saxton algorithm [28] with a cascaded structure, hence the large indirect space for phase can be guaranteed. Subsequently, a series of 1D intensity points are recorded as ciphertexts by using single-pixel detector (without spatial resolution). It will be illustrated that compared with previous works, the higher eavesdropping percentage is requested to the attackers in the proposed single-pixel optical cryptosystem.

2. THEORETICAL ANALYSIS

Figure 1(a) shows a schematic setup for embedding the pre-generated random intensity patterns [i.e., $I_e(i,j)$, e=1,2,3,...N] into noisy phase-only masks. Different from those in Refs. [25,26] another alternative is presented here, and three phase-only masks are cascaded as a typical example to illustrate the proposed method. It is straightforward to apply more or fewer phase-only masks in practice, and is also straightforward to design more complicated cascaded structures. Among the three cascaded phase-only masks two phase-only masks (i.e., M_{f1} and M_{f2}) are fixed, and another one is iteratively extracted by using a modified Gerchberg-Saxton algorithm.

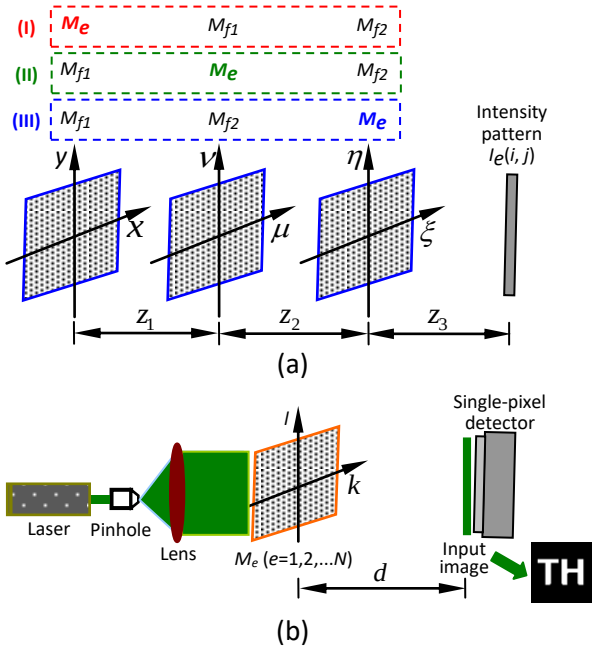

Fig. 1. (a) A schematic setup for embedding each pre-generated random intensity pattern [i.e., $I_e(i,j)$, e=1,2,3,...N] into one noisy phase-only mask M_e, and (b) a schematic setup [13,25–27] for optical image encryption. In practice, a collecting lens can be placed between the input image and single-pixel detector.

As seen in Fig. 1(a), when principal security keys, i.e., pre-generated random intensity patterns $I_e(i,j)$, are used, any one of the three embedding strategies can be arbitrarily selected for phase-mask generation and the sender can define which plane is used for the extracted phase-only mask (i.e., M_e). The embedding objective is to find correct or approximated phase-only mask M_e under the given constraints, such as wavelength, axial distances, fixed phase-only masks (M_{f1} and M_{f2}) and the pre-generated random intensity pattern [i.e, $I_e(i,j)$].

When the first embedding strategy [see (I) in Fig. 1(a)] is selected and applied, phase retrieval process based on a modified Gerchberg-Saxton algorithm can be described as follows:

(I-a) Propagate back to phase-only mask $M_e(x,y)$ plane:

$$O^{(n)}(x,y)=\mathrm{FrT}_{\lambda,-z_1}\left\{\left[\mathrm{FrT}_{\lambda,-z_2}\left(\left\{\mathrm{FrT}_{\lambda,-z_3}\left[I_e(i,j)\right]\right\}_{ij}\left[M_{f2}(\xi,\eta)\right]^{*}\right)\right]\left[M_{f1}(\mu,\nu)\right]^{*}\right\}, \quad (1)$$

where $\mathrm{FrT}_{\lambda,-z}$ denotes free-space wave back-propagation [10,11,29], λ denotes laser wavelength, z_1, z_2 and z_3 denote axial distances, asterisk denotes complex conjugate, $M_{f1}(\mu,\nu)$ and $M_{f2}(\xi,\eta)$ denote the fixed random phase-only masks.

(I-b) Apply constraint [2,26,30,31] to the generated complex-valued wavefront $O^{(n)}(x,y)$ in the phase-only mask $M_e(x,y)$ plane:

$$M_e^{(n)}(x,y)=O^{(n)}(x,y)\Big/\left|O^{(n)}(x,y)\right|, \quad (2)$$

where | | denotes the modulus operation.

(I-c) Propagate forward to the intensity pattern plane:

$$O^{(n)}(i,j)=\mathrm{FrT}_{\lambda,z_3}\left\{\left[\mathrm{FrT}_{\lambda,z_2}\left(\left\{\mathrm{FrT}_{\lambda,z_1}\left[M_e^{(n)}(x,y)\right]\right\}_{ij}M_{f1}(\mu,\nu)\right)\right]M_{f2}(\xi,\eta)\right\}, \quad (3)$$

where $O^{(n)}(i,j)$ denotes the complex-valued wavefront obtained in intensity pattern plane. Correlation coefficient calculated between the calculated out $\left|O^{(n)}(i,j)\right|^2$ and the desired output $I_e(i,j)$ is employed to monitor the process.

(I-d) When the calculated correlation coefficient is smaller than a preset threshold, complex-valued wavefront $O^{(n)}(i,j)$ is further updated by [2,30,31]:

$$\hat{O}^{(n)}(i,j)=\left[I_e(i,j)\right]^{1/2}O^{(n)}(i,j)\Big/\left|O^{(n)}(i,j)\right|, \quad (4)$$

where $\hat{O}^{(n)}(i,j)$ denotes the updated complex-valued wavefront which is further used for the next iteration (n=n+1), i.e., replacing $I_e(i,j)$ in Eq. (1) with $\hat{O}^{(n)}(i,j)$. If the preset threshold is satisfied, $M_e^{(n)}(x,y)$ (i.e., n=N) is used as the extracted phase-only mask M_e corresponding to the pre-generated intensity-only pattern $I_e(i,j)$.

When the second embedding strategy [see (II) in Fig. 1(a)] is selected and applied, phase retrieval process based on a modified Gerchberg-Saxton algorithm can be described as follows:

(II-a) Propagate back from the intensity pattern plane to the phase-only mask $M_e(\mu,\nu)$ plane:

$$O_1^{(n)}(\mu,\nu)=\mathrm{FrT}_{\lambda,-z_2}\left(\left\{\mathrm{FrT}_{\lambda,-z_3}\left[I_e(i,j)\right]\right\}_{ij}\left[M_{f2}(\xi,\eta)\right]^{*}\right). \quad (5)$$

(II-b) Propagate forward from the phase-only mask $M_{f1}(x,y)$ plane to phase-only mask $M_e(\mu,\nu)$ plane:

$$O_2^{(n)}(\mu,\nu)=\mathrm{FrT}_{\lambda,z_1}\left[M_{f1}(x,y)\right]. \quad (6)$$

(II-c) Generate the complex-valued wavefront and apply constraint [2,26,30,31] in the phase-only mask M_e plane:

$$O_3^{(n)}(\mu,\nu)=O_1^{(n)}(\mu,\nu)/O_2^{(n)}(\mu,\nu), \quad (7)$$

$$M_e^{(n)}(\mu,\nu)=O_3^{(n)}(\mu,\nu)\Big/\left|O_3^{(n)}(\mu,\nu)\right|. \quad (8)$$

(II-d) Propagate forward to the intensity pattern plane:

$$O^{(n)}(i,j)=\mathrm{FrT}_{\lambda,z_3}\left\{\left[\mathrm{FrT}_{\lambda,z_2}\left(\left\{\mathrm{FrT}_{\lambda,z_1}\left[M_{f1}(x,y)\right]\right\}_{ij}M_e^{(n)}(\mu,\nu)\right)\right]M_{f2}(\xi,\eta)\right\}, \quad (9)$$

where $O^{(n)}(i,j)$ denotes the complex-valued wavefront obtained in the intensity pattern plane. Correlation coefficient calculated between the calculated out $\left|O^{(n)}(i,j)\right|^2$ and the desired output $I_e(i,j)$ is employed to monitor the process.

(II-e) When the calculated correlation coefficient is smaller than a preset threshold, complex-valued wavefront $O^{(n)}(i,j)$ is further updated by:

$$\hat{O}^{(n)}(i,j)=\left[I_e(i,j)\right]^{1/2}O^{(n)}(i,j)\Big/\left|O^{(n)}(i,j)\right|, \tag{10}$$

where $\hat{O}^{(n)}(i,j)$ denotes the updated complex-valued wavefront which is further used for the next iteration (n=n+1), i.e., replacing $I_e(i,j)$ in Eq. (5) with $\hat{O}^{(n)}(i,j)$. If the preset threshold is satisfied, $M_e^{(n)}(\mu,\nu)$ (i.e., n=N) is used as the extracted phase-only mask corresponding to the pre-generated intensity pattern $I_e(i,j)$. Since the third embedding strategy [see (III) in Fig. 1(a)] is similar to the second one, its detailed process is not presented for the sake of brevity.

After each pre-generated random intensity pattern $I_e(i,j)$ (e=1,2,3,...N) is processed, a series of extracted phase-only masks (such as N=10000) are available for the encoding as shown in Fig. 1(b). When the extracted phase-only masks are sequentially embedded into spatial light modulator, a series of 1D intensity points, i.e., ciphertexts $\{B_e\}$ (e=1,2,3,...N), are recorded by single-pixel bucket detector (without spatial resolution). The process can be described by

$$B_e=\iint\left|\mathrm{FrT}_{\lambda,d}\left[M_e(k,l)\right]\right|^2|t(i,j)|^2\,didj, \tag{11}$$

where $t(i,j)$ denotes the input image [64×64 pixels, see inset in Fig. 1(b)], d denotes the axial distance, and $M_e(k,l)$ denotes the series of phase-only masks extracted by using the modified Gerchberg-Saxton algorithm with a cascaded structure. To clearly illustrate the encoding process aforementioned, a flow chart is further shown in Fig. 2(a).

For the decryption, the series of random intensity-only patterns $I_e(i,j)$ (e=1,2,3,...N) is stored or transmitted as principal security keys, and other parameters (such as wavelength, distances, two fixed phase-only masks, and threshold for the modified Gerchberg-Saxton algorithms) are applied as complementary security keys. The decoding process is described as follows:

(1) The authorized receiver applies correct parameters to extract the series of phase-only masks $\hat{M}_e(k,l)$ (e=1,2,3,...N) from principal security keys based on the modified Gerchberg-Saxton algorithm with a cascaded structure. In this case, a sequence of embedding strategies [i.e., (I) or (II) or (III) in Fig. 1(a)] should also be available to the authorized receiver for processing each principal security key, i.e., each intensity pattern.

(2) A series of intensity patterns at reference beam arm $P_e(i,j)$ (e=1,2,3,...N) are calculated based on free-space wave propagation principle [10,11,29], and the process is described by

$$P_e(i,j)=\left|\mathrm{FrT}_{\lambda,d}\left[\hat{M}_e(k,l)\right]\right|^2. \tag{12}$$

(3) When the ciphertexts $\{B_e\}$ (e=1,2,3,...N) are also available to the receiver, a decoded image $\hat{t}(i,j)$ can be obtained by using correlation function $[\langle BP(i,j)\rangle-\langle B\rangle\langle P(i,j)\rangle]$ (where $\langle,\rangle$ denotes ensemble average) [13,22–27]. In this study, peak signal-to-noise ratio (PSNR) is calculated to evaluate quality of decoded images. To clearly illustrate the decoding process aforementioned, a flow chart is shown in Fig. 2(b).

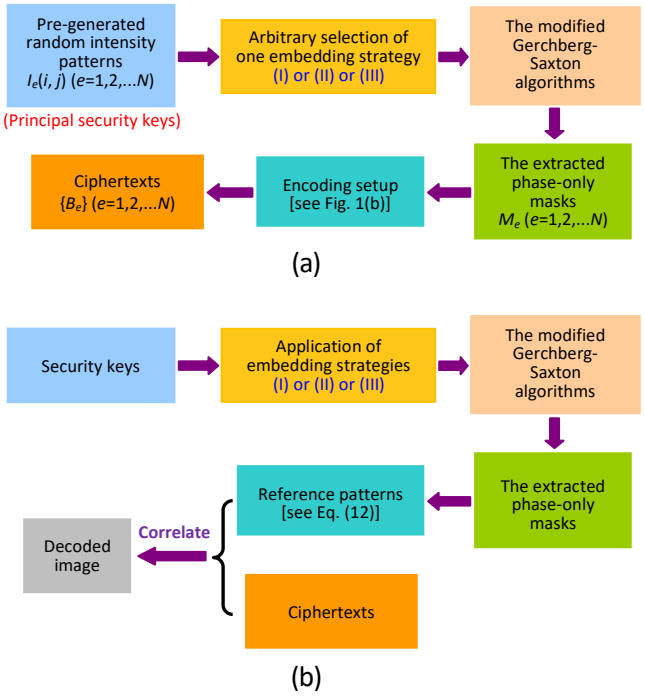

Fig. 2. Flow chart for illustrating (a) the encryption process and (b) the decryption process.

3. RESULTS AND DISCUSSION

Figures 1(a) and 1(b) show schematic setups to numerically illustrate validity of the proposed optical security system. The collimated plane wave is generated for the illumination, and laser wavelength is 630.0 nm. Free-space wave propagation [10,11,29] is applied in the optical encoding process, however it is straightforward to apply other domains in practice. Axial distances z_1, z_2, z_3 and d are 6.0 cm, 9.0 cm, 15.0 cm and 25.0 cm, respectively. In the proposed optical security system, a series of intensity patterns, i.e., N=10000, are pre-generated as principal security keys, and pixel values in each intensity pattern are randomly distributed in the range of (0,500]. The series of pre-generated random intensity patterns $I_e(i,j)$ is sequentially embedded into phase-only masks, and the threshold (here correlation coefficient used as monitoring parameter) is set as 0.90 for the modified Gerchberg-Saxton algorithms. In the modified Gerchberg-Saxton algorithms, two fixed phase-only masks M_{f1} and M_{f2} are randomly distributed in the range of $[0,2\pi]$ for processing the first two intensity patterns [i.e., $I_1(i,j)$ and $I_2(i,j)$], and subsequently are sequentially replaced by the previously extracted phase-only masks (i.e. $M_e, e=e-2$ and $e=e-1$) for processing other intensity patterns [i.e., $I_e(i,j)$, $e>2$]. When the series of extracted phase-only masks ($M_e, e=1,2,...N$) is sequentially embedded into spatial light modulator (pixel size of 20 microns and 64×64 pixels), the input image [64×64 pixels, see inset in Fig. 1(b)] can be encoded into a series of 1D intensity points (i.e., ciphertexts) by using single-pixel bucket detector (without spatial resolution).

In this study, binary input image is applied [see the inset in Fig. 1(b)], and in practice color input images and gray-scale input images can also be encoded by using the proposed method. A series of random intensity patterns are pre-generated as principal security keys in the proposed optical cryptosystem, and Figs. 3(a)–3(c) show three typical intensity patterns. Based on the modified Gerchberg-Saxton algorithm

with a cascaded structure, a series of noisy phase-only masks (M_e, e=1,2,...N) can be extracted for the subsequent encryption, and Figs. 3(d)–3(f) show three typically extracted phase-only masks. Figures 4(a)–4(c) show the typical relationships between the number of iterations and the calculated correlation coefficients, when the 1st, 2nd and 3rd embedding strategies, i.e., the modified Gerchberg-Saxton algorithm, are respectively applied for phase-mask retrieval. It can be seen in Figs. 4(a)–4(c) that only 5, 11 and 12 iterations are respectively requested, and a rapid convergence rate is achieved in the modified Gerchberg-Saxton algorithms. Although the threshold is set as 0.90 in the modified Gerchberg-Saxton algorithms in this study, the higher value (i.e., closer to one) can be arbitrarily set in practice and iteration number is slightly modified.

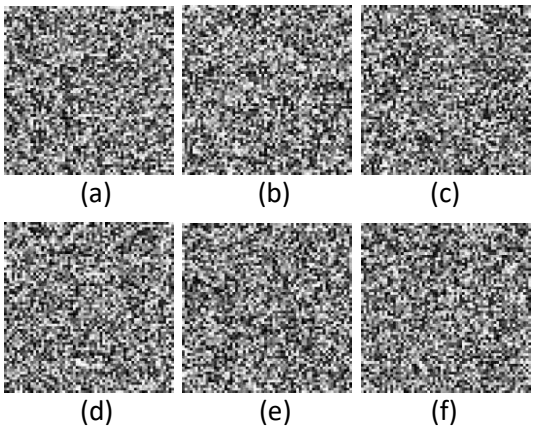

Fig. 3. (a)–(c) Three typical intensity patterns, and (d)–(f) three typically extracted phase-only masks based on the modified Gerchberg-Saxton algorithm with a cascaded structure.

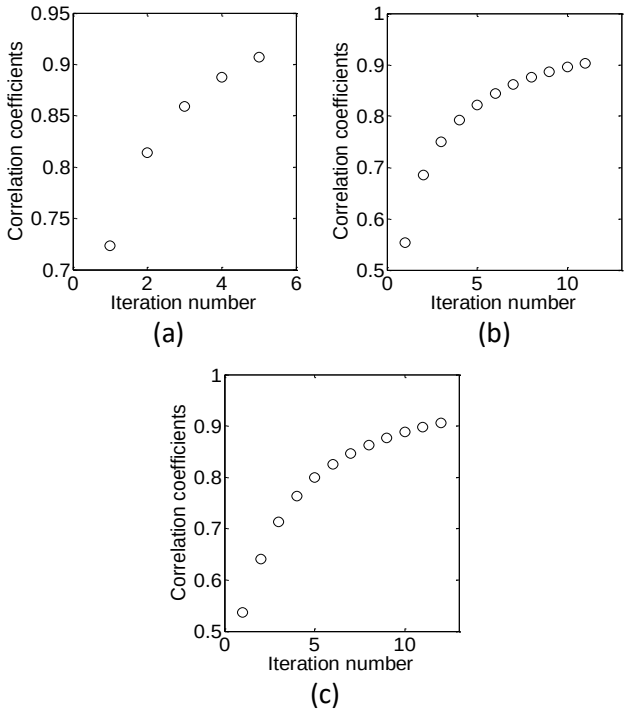

Fig. 4. The typical relationships between the number of iterations and the calculated correlation coefficients, when the (a) 1st, (b) 2nd and (c) 3rd embedding strategy, i.e., the modified Gerchberg-Saxton algorithm with a cascaded structure, is applied for phase-mask retrieval.

Using the pre-generated intensity patterns and the modified Gerchberg-Saxton algorithms with a cascaded structure, a series of phase-only masks (M_e, e=1,2,...N) can be extracted, which are sequentially embedded for image encoding. Hence, a series of 1D intensity points, i.e., ciphertexts, can be correspondingly obtained by using single-pixel bucket detector (without spatial resolution), and Fig. 5(a) shows the generated 1D ciphertexts [see Eq. (11)]. The number of measurements is 10000, i.e., N=10000. It can be seen in Fig. 5(a) that different from conventional encoding systems using 2D detectors, only 1D noisy distribution is obtained as ciphertexts after the encryption. No information related to the input image can be observed in Fig. 5(a). When all security keys are correctly applied (such as by the authorized receiver), a decoded image is obtained in Fig. 5(b). The PSNR for Fig. 5(b) is 11.39 dB. It can be seen in Fig. 5(b) that the decoded image is of high quality, and information related to the input image is fully extracted. It is worth noting that in optical cryptosystem the main objective is to clearly observe the input image during the decryption rather than to recover high-resolution images as those in conventional imaging systems [32–34].

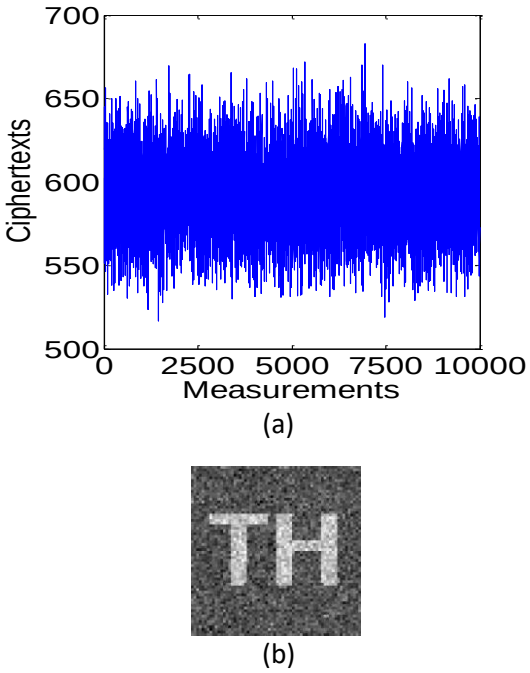

Fig. 5. (a) A series of 1D intensity points as ciphertexts, and (b) a decoded image obtained when all security keys are correctly applied (such as by authorized receivers). The number of measurements is 10000, i.e., N=10000. In practice, fewer ciphertexts can also be applicable to extract the input information, and ciphertexts and security keys can be protected by using additional strategies, such as multiple-layer distribution. Although simplified decryption with fewer measurements can still be feasible, the decryption quality can be affected. The security key distribution method should be designed. In (a), vertical axis denotes the generated 1D ciphertexts which are obtained by using Eq. (11).

Performance of principal and complementary security keys is analyzed to evaluate the proposed optical cryptosystem. Figure 6(a) shows a decoded image, when only the series of random intensity patterns $I_e(i,j)$ is wrongly used for image decoding, such as by the unauthorized receivers. The PSNR for Fig. 6(a) is 7.23 dB. Figure 6(b) shows a decoded image, when only the wavelength contains an error

of 1.0 nm during phase-mask retrieval using the modified Gerchberg-Saxton algorithms with a cascaded structure. The PSNR for Fig. 6(b) is 7.17 dB. Figure 6(c) shows a decoded image, when only the axial distance z_3 contains an error of 0.1 cm during phase-mask retrieval using the modified Gerchberg-Saxton algorithms. The PSNR for Fig. 6(c) is 7.14 dB. Figure 6(d) shows a decoded image, when only the threshold is wrong (an error of 0.01) during phase-mask retrieval using the modified Gerchberg-Saxton algorithms. The PSNR for Fig. 6(d) is 7.01 dB. Figure 6(e) shows a decoded image, when only the sequence of the selected embedding strategies is wrong during phase-mask retrieval using the modified Gerchberg-Saxton algorithms. The PSNR for Fig. 6(e) is 7.16 dB. Figure 6(f) shows a decoded image, when only the wavelength (error of 10.0 nm) and the distance *d* (an error of 1.0 cm) are incorrectly applied for generating reference intensity patterns $P_e(i,j)$ (e=1,2,3,...N) during the decoding. The PSNR for Fig. 6(f) is 7.70 dB. The results in Figs. 6(a)–6(f) illustrate that either principal or complementary security keys play an important role for the decoding. For the sake of brevity, performance of other security keys, such as the fixed phase-only masks, is not presented here.

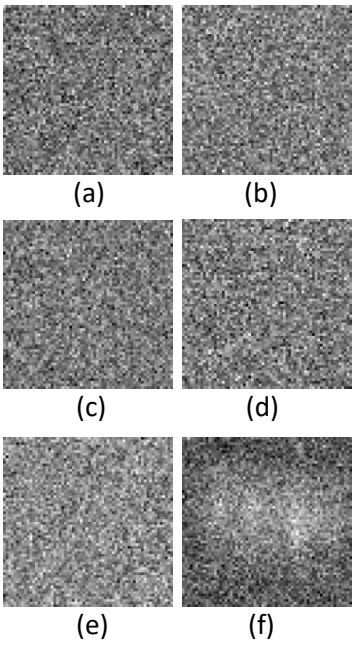

Fig. 6. Decoded images obtained (a) when only the series of random intensity patterns is wrongly used for image decoding; (b) when only the wavelength contains an error of 1.0 nm during phase-mask retrieval; (c) when only the axial distance z_3 contains an error of 0.1 cm during phase-mask retrieval; (d) when only the threshold contains an error of 0.01 during phase-mask retrieval; (e) when only the sequence of the selected embedding strategies is wrong during phase-mask retrieval; and (f) when only the wavelength (an error of 10.0 nm) and the distance *d* (an error of 1.0 cm) are incorrectly applied for generating reference intensity patterns $P_e(i,j)$ (e=1,2,3,...N). The number of measurements is 10000, i.e., N=10000.

The decryption is also conducted under different percentages of eavesdropping to further evaluate the developed cryptosystem, when the unauthorized receiver has obtained partial data related to principal security keys, i.e., the series of random intensity patterns $[I_e(i,j), e=1,2,...N]$. Here, it is assumed that the unauthorized receiver has known all other security keys, such as wavelength, distances, threshold, the sequence of embedding strategies, and the fixed phase-only masks for processing the first two principal intensity patterns. Figures 7(a)–7(d) show the decoded images, when 85.0%, 90.0%, 95.0% and 99.0% pixels of each principal security key (i.e., each random intensity pattern) are eavesdropped, respectively. It can be seen in Figs. 7(a)–7(d) that even when 99.0% pixels in each principal security key are eavesdropped, the input image is still not slightly observed. The high security and sensitivity are effectively guaranteed for the proposed single-pixel optical cryptosystem. In addition to the designed strategies, another reason is that in the modified Gerchberg-Saxton algorithm with a cascaded structure, the previously two extracted phase masks are applied and fixed for the next phase-only mask retrieval [i.e., when $e>2$].

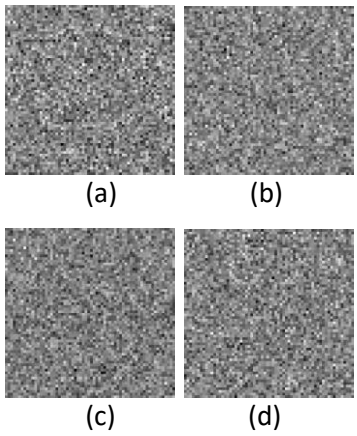

Fig. 7. Eavesdropping cases: the decoded images obtained when (a) 85.0%, (b) 90.0%, (c) 95.0% and (d) 99.0% pixels of each principal security key [i.e., $I_e(i,j)$, e=1,2,3,...N] are eavesdropped. Here, it has been assumed that no any complete intensity pattern (i.e., any one principal key) is fully eavesdropped.

Advantages of the proposed method and its comparisons to previous works are briefly discussed as follows:

(1) The series of random intensity-only patterns is pre-generated as principal security keys rather than phase-only masks (or the simply-converted forms) in conventional optical cryptosystems [22–24,27]. This modification provides high flexibility and enlarges the indirect space for phase in the developed single-pixel optical cryptosystem, since Gerchberg-Saxton algorithm [28] can be flexibly modified to extract the phase-only masks. Different from previous work [25,26], the different number of phase-only masks can be arbitrarily cascaded to generate the different embedding strategies. The proposed optical encryption method using a cascaded structure provides an alternative for single-pixel intensity-modulated optical security approaches [25,26], which is also consistent with the descriptions in Refs. [25,26] .

(2) In conventional single-pixel optical security systems [22–24,27], a series of phase-only masks are usually applied for the encoding, and are distributed in the range of $[0, 2\pi]$. Hence, high data space for each pixel cannot be guaranteed, i.e., smaller than 3 bits. To illustrate the proposed method, pixel values in each intensity pattern are randomly distributed in the range of (0,500]. In practice, the larger pixel values can be arbitrarily used in the pre-generated random intensity patterns $[I_e(i,j), e=1,2,...N]$, and data space is effectively enlarged in the proposed optical cryptosystem.

(3) In conventional optical cryptosystems [1–5], 2D detectors are usually applied to record the ciphertexts. In this study, single-pixel

detector is employed for optical encryption, hence there is a potential to establish lower-cost and more compact security systems.

(4) The modified Gerchberg-Saxton algorithm with a cascaded structure is developed for phase-mask retrieval, and the higher system sensitivity can be guaranteed compared with previous works [22,23]. As illustrated in Figs. 6 and 7, only slight modification of system parameters (especially principal security keys) leads to the wrong extraction of phase-only masks (M_e, $e=1,2,...N$), and the decoded images cannot render information related to the input image. Compared with previous works in Refs. [25,26], the proposed method using a cascaded structure requests the higher eavesdropping percentage, see Figs. 7(a)–7(d). In practice, more complicated cascaded structures can be arbitrarily designed and applied, since the generation of noisy phase-only masks is computationally implemented.

(5) There may be system vulnerability in conventional double random phase encoding methods, and the attack algorithms [35–39] could be applied to extract or estimate principal security keys. This is mainly due to the linearity property in some optical security systems. In the proposed optical encryption method, indirect phase space has been successfully established, and a linear relationship between principal security keys (i.e., a series of random intensity patterns) and 1D ciphertexts does not exist. Hence, the attack algorithms, such as known-plaintext attack [36], cannot be applied to extract or estimate principal security keys, i.e., a series of random intensity patterns. The proposed method provides high flexibility and enlarges the indirect space for phase, since Gerchberg-Saxton algorithm can be flexibly modified to extract phase-only masks. Compared with previous works in Refs. [25,26], the proposed method requests much higher eavesdropping percentage, see the results in Figs. 7(a)–7(d). Hence, when principal security keys are occluded, the decoding process can be sensitive.

4. CONCLUSIONS

An optical cryptosystem has been presented by using single-pixel encoding and the modified Gerchberg-Saxton algorithm with a cascaded structure. A series of random intensity patterns are pre-generated as principal security keys, and phase-only masks for optical encoding and decoding are generated by the modified Gerchberg-Saxton algorithm with a cascaded structure. It is illustrated that high security with a large key space is achieved for the proposed single-pixel optical cryptosystem. The phase-mask generation process can be flexibly designed by modifying Gerchberg-Saxton algorithm with a cascaded structure, hence high sensitivity and the large indirect space for phase can be guaranteed for the proposed single-pixel optical cryptosystem. Compared with previous work (such as those in Refs. [25,26]), the proposed method requests the higher eavesdropping percentage. In addition, it is numerically demonstrated that the proposed method using the cascaded structure provides a novel strategy for single-pixel intensity-modulated optical security approaches.

Funding. Science and Technology Innovation Commission of Shenzhen Municipality through Basic Research Program (JCYJ20160531184426473); The Hong Kong Polytechnic University (1-ZE5F).

References

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
2. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120–155 (2014).
3. D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, and B. Javidi, "Optical encryption using photon-counting polarimetric imaging," Opt. Express **23**, 655–666 (2015).
4. O. Matoba and B. Javidi, "Secure holographic memory by double-random polarization encryption," Appl. Opt. **43**, 2915–2919 (2004).
5. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253–10265 (2007).
6. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S Millán, N. K Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A Alfalou, C Brosseau, C. Guo, J. T Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W H Pinkse, A. P Mosk, and A. Markman, "Roadmap on optical security," J. Opt. **18**, 083001 (2016).
7. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating," Appl. Opt. **50**, 5750–5757 (2011).
8. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22–24 (2011).
9. E. Pérez-Cabré, H. C. Abril, M. S. Millan, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," J. Opt. **14**, 094001 (2012).
10. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).
11. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).
12. 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**, 1414–1416 (2006).
13. W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL **110**, 44002 (2015).
14. J. F. Barrera, M. Tebaldi, C. Ríos, E. Rueda, N. Bolognini, and R. Torroba, "Experimental multiplexing of encrypted movies using a JTC architecture," Opt. Express **20**, 3388–3393 (2012).
15. Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. **33**, 2443–2445 (2008).
16. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**, 3817–3819 (2010).
17. W. Chen, G. Situ, and X. Chen, "High-flexibility optical encryption via aperture movement," Opt. Express **21**, 24680–24691 (2013).
18. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**, 118–120 (2010).
19. A. Markman, J. Wang, and B. Javidi, "Three-dimensional integral imaging displays using a quick-response encoded elemental image array," Optica **1**, 332–335 (2014).
20. L. Sui, K. Duan, J. Liang, and X. Hei, "Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps," Opt. Express **22**, 10605–10621 (2014).
21. I. Mehra and N. K. Nishchal, "Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding," Opt. Express **22**, 5474-5482 (2014).
22. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**, 2391–2393 (2010).
23. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," Appl. Phys. Lett. **101**, 101108 (2012).
24. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**, 221106 (2013).
25. W. Chen, "Optical data security system using phase extraction scheme via single-pixel detection," IEEE Photon. J. **8**, 7801507 (2016).
26. W. Chen, "Correlated-photon secured imaging by iterative phase retrieval using axially-varying distances," IEEE Photon. Technol. Lett. **28**, 1932–1935 (2016).
27. W. Chen, "Modulating phase via rotation for optical encoding based on correlated photon imaging," IEEE Photon. Technol. Lett. **28**, 540–543 (2016).

28. R. W. Gerchberg and W. O. Saxton, “A practical algorithm for the determination of phase from image and diffraction plane pictures,” Optik (Stuttgart) **35**, 237–246 (1972).
29. J. W. Goodman, *Introduction to Fourier Optics, 2nd ed.* (New York, McGraw-Hill, 1996).
30. W. Chen, X. Wang, and X. Chen, “Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase,” J. Opt. **17**, 035702 (2015).
31. W. Chen, X. Chen, A. Stern, and B. Javidi, “Phase-modulated optical system with sparse representation for information encoding and authentication,” IEEE Photon. J. **5**, 6900113 (2013).
32. B. I. Erkmen and J. H. Shapiro, “Ghost imaging: from quantum to classical to computational,” Adv. Opt. Photon. **2**, 405–450 (2010).
33. J. H. Shapiro, “Computational ghost imaging,” Phys. Rev. A **78**, 061802 (2008).
34. F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, “Differential ghost imaging,” Phys. Rev. Lett. **104**, 253603 (2010).
35. A. Carnicer, M. M. Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett. **30**, 1644–1646 (2005).
36. X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett. **31**, 1044–1046 (2006).
37. X. Peng, H. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” Opt. Lett. **31**, 3261–3263 (2006).
38. Y. Zhang, D. Xiao, W. Wen, and H. Liu, “Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding,” Opt. Lett. **38**, 4506–4509 (2013).
39. G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, “Cryptanalysis of optical security systems with significant output images,” Appl. Opt. **46**, 5257–5262 (2007).