Ghost identification based on single-pixel imaging in big data environment

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: In recent years, single-pixel imaging has become one of the most interesting and promising imaging technologies for various applications. In this paper, a big data environment, for the first time to my knowledge, is designed and introduced into single-pixel ghost imaging for securing information. Many series of one-dimensional ciphertexts are recorded by single-pixel bucket detector to form a big data environment. Several hidden inputs are further encoded based on ghost imaging by using hierarchical structure, and their corresponding ciphertexts are synthesized into the big data environment for verifying the hidden ghosts and identifying the targeted ghosts. This new finding could open up a different research perspective for exploring more applications based on single-pixel imaging.

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

References and links

1. B. I. Erkmen and J. H. Shapiro, "Ghost imaging: from quantum to classical to computational," Adv. Opt. Photon. **2**, 405–450 (2010).
2. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," Phys. Rev. A **52**, R3429–R3432 (1995).
3. D. V. Strekalov, A. V. Sergienko, D. N. Klyshko, and Y. H. Shih, "Observation of two-photon "ghost" interference and diffraction," Phys. Rev. Lett. **74**, 3600–3603 (1995).
4. R. S. Bennink, S. J. Bentley, and R. W. Boyd, ""Two-photon" coincidence imaging with a classical source," Phys. Rev. Lett. **89**, 113601 (2002).
5. A. Gatti, E. Brambilla, M. Bache, and L. A. Lugiato, "Ghost imaging with thermal light: comparing entanglement and classical correlation," Phys. Rev. Lett. **93**, 093602 (2004).
6. R. E. Meyers, K. S. Deacon, and Y. Shih, "Turbulence-free ghost imaging," Appl. Phys. Lett. **98**, 111115 (2011).
7. R. E. Meyers, K. S. Deacon, A. D. Tunick, and Y. Shih, "Virtual ghost imaging through turbulence and obscurants using Bessel beam illumination," Appl. Phys. Lett. **100**, 061126 (2012).
8. B. I. Erkmen, "Computational ghost imaging for remote sensing," J. Opt. Soc. Am. A **29**, 782–789 (2012).
9. K. W. C. Chan, M. N. O'Sullivan, and R. W. Boyd, "High-order thermal ghost imaging," Opt. Lett. **34**, 3343–3345 (2009).
10. O. Katz, Y. Bromberg, and Y. Silberberg, "Compressive ghost imaging," Appl. Phys. Lett. **95**, 131110 (2009).
11. F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, "Differential ghost imaging," Phys. Rev. Lett. **104**, 253603 (2010).
12. J. H. Shapiro, "Computational ghost imaging," Phys. Rev. A **78**, 061802(R) (2008).
13. 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).
14. W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett. **38**, 546–548 (2013).
15. W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," Appl. Phys. Lett. **103**, 221106 (2013).
16. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
17. B. Javidi, "Securing information with optical technologies," Phys. Today **50**, 27–32 (1997).
18. B. L. Volodin, B. Kippelen, K. Meerholz, B. Javidi, and N. Peyghambarian, "A polymeric optical pattern-recognition system for security verification," Nature **383**, 58–60 (1996).
19. W. Chen, "Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation," IEEE Photon. J. **8**, 6900209 (2016).

20. L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: privacy and data mining," IEEE Access **2**, 1149–1176 (2014).
21. R. K. Vasudevan, A. Belianinov, A. G. Gianfrancesco, A. P. Baddorf, A. Tselev, S. V. Kalinin, and S. Jesse, "Big data in reciprocal space: Sliding fast Fourier transforms for determining periodicity," Appl. Phys. Lett. **106**, 091601 (2015).
22. J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. (McGraw-Hill, 1996).
23. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120–155 (2014).
24. W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," EPL **110**, 44002 (2015).
25. B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, "Normalized ghost imaging," Opt. Express **20**, 16892–16901 (2012).
26. L. J. Kong, Y. Li, S. X. Qian, S. M. Li, C. Tu, and H. T. Wang, "Encryption of ghost imaging," Phys. Rev. A **88**, 013852 (2013).
27. W. Chen and X. Chen, "Marked ghost imaging," Appl. Phys. Lett. **104**, 251109 (2014).
28. 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).

1. Introduction

Ghost imaging [1–5] has attracted much current attention, and its corresponding applications have been continually explored. Fundamental principle of single-pixel ghost imaging is established based on intensity correlation between object signals and reference signals [1–5]. Both quantum and classical ghost imaging can be applicable, and remarkable characteristics of ghost imaging, such as high capability against turbulence [6,7], are useful for some applications, such as remote sensing [8]. A number of algorithms and infrastructures, such as high-order [9], compressed sensing [10] and differential [11], have been developed and applied to improve the performance of ghost imaging, and computational ghost imaging [1,12] has also been proposed to simplify the experimental setup.

In recent years, ghost imaging [13–15] has been applied as a promising approach for optical security [16–19]. Random phase-only profiles can be applied as security keys, and one-dimensional signals recorded at object beam arm are used as ciphertexts. However, conventional ghost-secured imaging systems seem to be simple without the use of a sufficiently large number of varied strategies, and the encoding strategies may be estimated by attackers. In this paper, a big data environment [20,21], for the first time to my knowledge, is designed and introduced into single-pixel ghost imaging to significantly enhance system security. Many series of one-dimensional ciphertexts are recorded by single-pixel bucket detector to form a big data environment. Several hidden inputs are further encoded based on single-pixel ghost imaging by using hierarchical structure, and their corresponding ciphertexts are synthesized into the big data environment for verifying the hidden ghosts and identifying the targeted ghosts.

2. Ghost identification analysis

Figure 1 shows a schematic for the generation of many series of one-dimensional ciphertexts to establish a big data environment. As shown in Fig. 1, a large number of different inputs are sequentially encoded, and among them only four inputs are employed as target inputs. A series of random phase-only masks M_h (h=1,2,3,...,30000) are repeatedly applied for encoding each input, hence many series of one-dimensional ciphertexts can be generated as shown in Fig. 2. Each series of the ciphertexts is defined as T_h (h=1,2,3,...,30000). These ciphertexts form a big data environment, and this strategy can effectively confuse the unauthorized receivers. However, it is also important to design an effective approach to identify the targeted ciphertexts in the big data environment for authorized receivers.

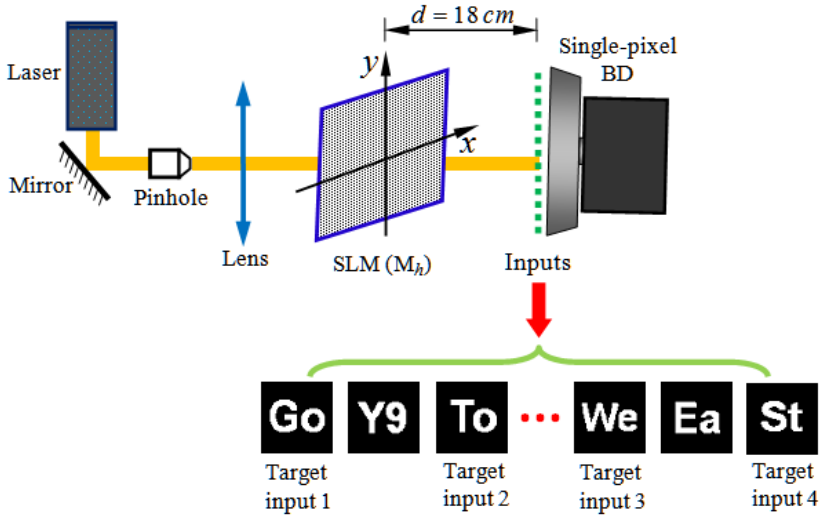

Fig. 1. Schematic for illustrating the generation of many series of one-dimensional ciphertexts to form a big data environment: SLM, phase-only spatial light modulator; BD, bucket detector; h=1,2,3,...,30000. A collecting lens can be placed between the input and bucket detector.

In this study, only four series of one-dimensional ciphertexts in Fig. 2 are the targeted ciphertexts corresponding to the four different target inputs. In the proposed optical security system, four hidden inputs are further encoded based on single-pixel ghost imaging using a hierarchical structure as shown in Fig. 3. At each hierarchical level, a hidden input is encoded, and a series of one-dimensional ciphertexts are correspondingly generated. For instance, at the first hierarchical level, random phase-only masks M_i (i=1,2,3,...,650) are arbitrarily selected from the sequence M_h (h=1,2,3,...,30000) as schematically illustrated in Fig. 4, and a series of one-dimensional ciphertexts [i.e., C_i (i=1,2,3,...,650)] can be obtained. Similarly, random phase-only masks M_j (j=1,2,3,...,650), M_k (k=1,2,3,...,650) and M_l (l=1,2,3,...,650) are arbitrarily selected from the sequence M_h (h=1,2,3,...,30000), and other three series of one-dimensional ciphertexts, i.e., C_j (j=1,2,3,...,650), C_k (k=1,2,3,...,650) and C_l (l=1,2,3,...,650), are obtained at the second, third and fourth hierarchical level, respectively.

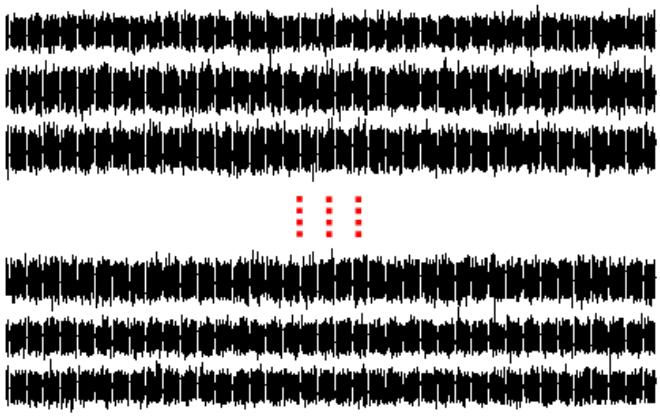

Fig. 2. Data big environment established by using the recorded ciphertexts.

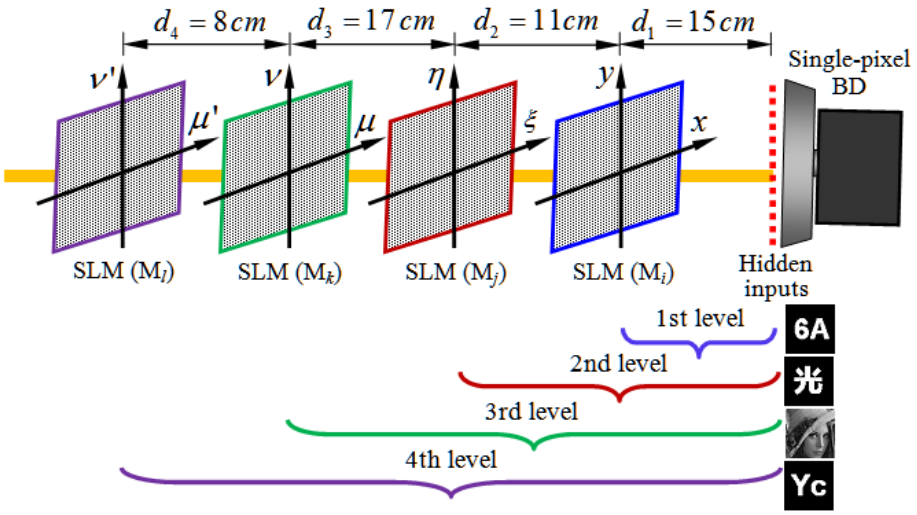

Fig. 3. Schematic setup for computationally encoding the hidden inputs based on single-pixel imaging using a hierarchical structure: *i*, *j*, *k*, *l*=1,2,3,...,650. For hierarchically encoding the hidden inputs, computational approach is applied based on single-pixel ghost imaging. In practice, different architectures can be flexibly designed and computationally applied for encoding the hidden inputs.

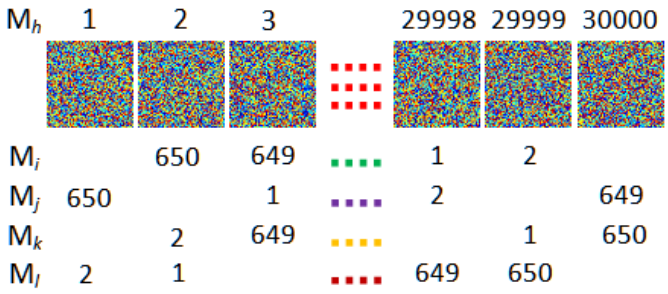

Fig. 4. Schematic for illustrating the arbitrary selection of phase-only masks (M_i, M_j, M_k and M_l) from the phase-mask sequence M_h. The maximum value for *i*, *j*, *k* and *l* is 650, and the maximum value for *h* is 30000.

After the four series of ciphertexts C_i, C_j, C_k and C_l (*i*, *j*, *k* and *l*=1,2,3,...,650) are obtained, each series is further embedded into one specific series of ciphertexts T_h (*h*=1,2,3,...,30000) corresponding to a target input. For instance, as shown in Fig. 5, each pixel in C_i (*i*=1,2,3,...,650) can randomly replace a pixel in the series T_h (*h*=1,2,3,...,30000). After all pixels in C_i are processed, a new series of synthesized ciphertexts T'_h (*h*=1,2,3,...,30000) are generated and hidden in the big data environment. Figure 6(a) shows a series of targeted ciphertext T_h (*h*=1,2,3,...,30000) before the replacement, and Fig. 6(b)

shows the series of synthesized ciphertexts T'_h (h=1,2,3,...,30000) after ciphertexts C_i (i=1,2,3,...,650) generated for a hidden input are embedded for the replacement. It can be seen in Figs. 6(a) and 6(b) that the ciphertexts generated for a hidden input are fully hidden into the designed big data environment. Here, only four series of one-dimensional ciphertexts in Fig. 2 contain the hidden ciphertexts, and other series of ciphertexts in Fig. 2 also play an important role to form the big data environment and confuse the unauthorized receivers.

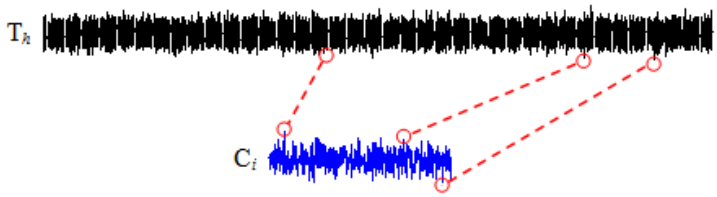

Fig. 5. Schematic for illustrating the embedding and replacement process to generate the synthesized ciphertexts: one-dimensional ciphertexts C_i (generated for a hidden input) randomly replace the pixels in a series of ciphertexts T_h (generated for a target input).

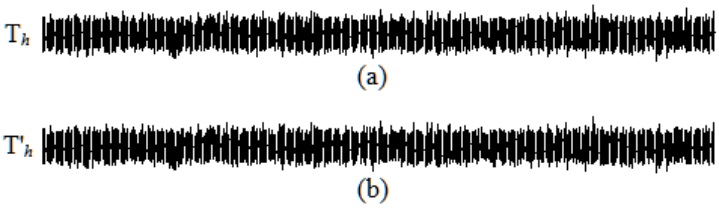

Fig. 6. (a) Typical one-dimensional ciphertexts T_h generated for a target input, and (b) typical one-dimensional synthesized ciphertexts T'_h after the ciphertexts generated for a hidden input are embedded for the replacements.

When the big data, i.e., ciphertexts, are transmitted to authorized receivers, the steps as follows are implemented to extract the target inputs: (1) Embedding positions of the ciphertexts C_i (i=1,2,3,...,650) should be available to the receiver. According to the embedding positions, a series of the hidden ciphertexts are sequentially chosen from each series of cipherexts in Fig. 2 for the verification. For instance, one series of ciphertexts C'_i (i=1,2,3,...,650) is sequentially extracted from each series of cipherexts in the big data environment. (2) Reference intensity patterns, calculated at the first hierarchical level using phase keys M_i (i=1,2,3,...,650), are obtained through the function $\left|\mathrm{FrT}_{\lambda,d_1}\left[M_i(x,y)\right]\right|^2$ (where λ denotes the wavelength and FrT denotes free-space wave propagation [22]), which are correlated with each series of extracted ciphertexts C'_i (i=1,2,3,...,650). Hence, a series of recovered inputs can be obtained, which are sequentially correlated with the original hidden input for data verification [15,19,23,24]. In practice, the original hidden inputs can be stored in a remote database, and only one interface is given for data authentication without direct observation. (3) Only when one remarkable peak is obtained in a generated correlation distribution, one series of ciphertexts in the big data environment can be correspondingly

determined as targeted ciphertexts. (4) Similarly to steps (1)-(3), other three series of targeted ciphertexts can also be extensively searched in the big data environment and determined according to the phase keys at the higher hierarchical levels and the embedding positions of the hidden ciphertexts C_j, C_k and C_l (j, k and l=1,2,3,...,650). (5) After all four series of targeted ciphertexts are identified, each target input can be decoded by using correlation function $\left[\langle BR_h(m,n)\rangle - \langle B\rangle\langle R_h(m,n)\rangle\right]$, where $\langle\cdot\rangle$ denotes ensemble average, $\{B\}$ denotes each series of the targeted ciphertexts identified by the aforementioned method, and $R_h(m,n)$ denotes reference intensity patterns for the target inputs. Other reconstruction methods, such as differential [11], normalized [25], high-order [9] and compressed sensing [10], may also be employed in order to reduce the number of measurements during the encoding. In practice, the decoded target inputs can be combined to visually render the complete information to authorized receivers.

3. Results and discussion

Validity of the proposed method is further illustrated. As shown in Fig. 1, plane wave, with a waist of 740 μm and wavelength of 600.0 nm, is applied. Each phase-only mask M_h (h=1,2,3,...,30000) is randomly distributed in the range of $[0, 2\pi]$. As seen in Fig. 1, when the series of random phase-only masks M_h (h=1,2,3,...,30000) is repeatedly applied and sequentially embedded into spatial light modulator (pixel pitch of 18 μm and pixel number of 64×64) for encoding each input, many series of ciphertexts can be correspondingly recorded by using single-pixel bucket detector (without spatial resolution) to form the big data environment (see Fig. 2). The proposed method can be implemented by using either optical approach or virtual-optics (computational) approach in practical applications, and computational single-pixel (ghost) imaging is considered and applied, such as for the encoding using the designed hierarchical structure. In addition, chaotic functions can also be used to generate the series of random phase-only masks, which will facilitate data transmission (such as the security keys) and generate the consistent authentication and decoding results.

Each series of hidden ciphertexts should be extensively searched and verified in the big data environment, when accurate keys, such as the embedding positions and phase-mask keys, are available. Figure 7(a) shows a recovered hidden input, and its corresponding authentication distribution is shown in Fig. 7(b). As seen in Fig. 7(b), only one remarkable peak is generated to confirm that the series of ciphertexts in the big data environment containing these hidden ciphertexts [used for the recovery in Fig. 7(a)] is the targeted ciphertexts. Hence, one target input can be correspondingly recovered as shown in Fig. 7(c). Peak signal-to-noise ratio (PSNR) for Fig. 7(c) is 13.37 dB. Similarly, other three target inputs can also be recovered as shown in Figs. 7(f), 7(i) and 7(l), when their hidden inputs are correspondingly identified and verified in the big data environment as illustrated in Figs. 7(d) and 7(e), 7(g) and 7(h), and 7(j) and 7(k), respectively. The PSNRs for Figs. 7(f), 7(i) and 7(l) are 11.59 dB, 12.17 dB and 14.36 dB, respectively. Here, the series of random phase-only masks, arbitrarily-selected positions for random phase-only masks M_i, M_j, M_k and M_l, and ciphertext embedding positions can be considered as security keys. It is worth noting that since only 650 measurements (for the hidden input) are embedded into the targeted ciphertexts (each sequence of 30000), the influence due to cross-talk term can be ignored during the decoding of target inputs.

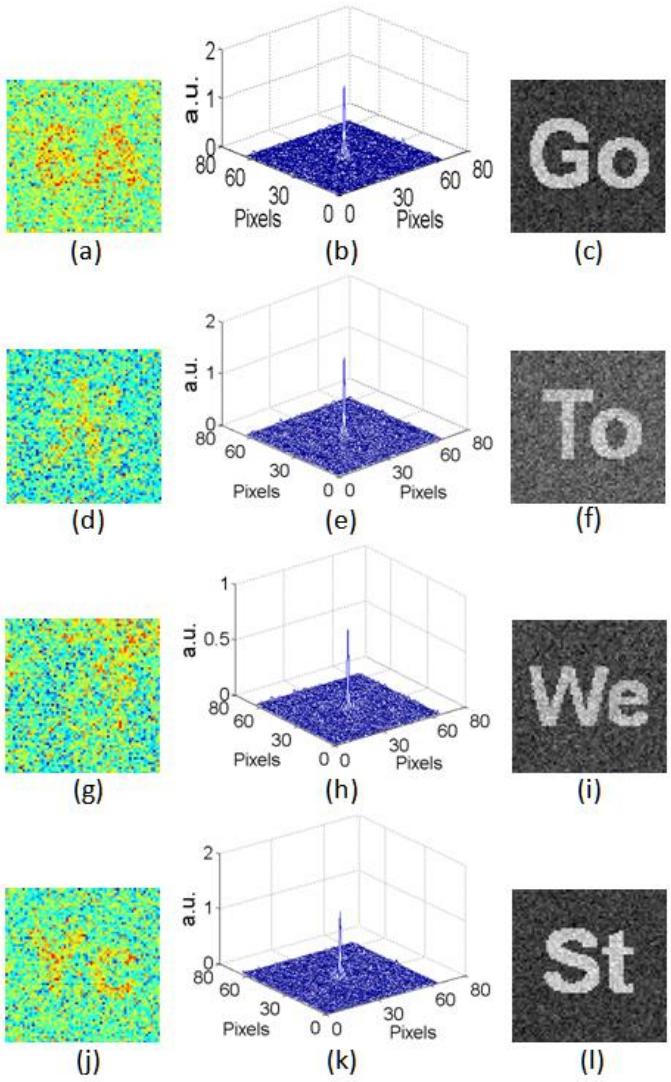

Fig. 7. (a) A recovered hidden input, (b) data authentication corresponding to (a), and (c) the correspondingly recovered target input; (d) A recovered hidden input, (e) data authentication corresponding to (d), and (f) the correspondingly recovered target input; (g) A recovered hidden input, (h) data authentication corresponding to (g), and (i) the correspondingly recovered target input; (j) A recovered hidden input, (k) data authentication corresponding to (j), and (l) the correspondingly recovered target input.

In the proposed optical security system, an extensive search is conducted in the big data environment to find out a series of hidden ciphertexts for recovering the hidden input. When the series of hidden ciphertexts is not extracted from the series of targeted ciphertexts, typical authentication distributions are shown in Figs. 8(a)-8(h). It can be seen that only noisy correlation distributions are obtained, which are largely different from those in Figs. 7(b), 7(e), 7(h) and 7(k). Through this design using hidden ciphertexts in the big data environment, the target inputs can be effectively identified and extracted without implementation of a complex procedure. Here, each hidden input is individually encoded, and its series of one-

dimensional ciphertexts replaces some pixels in one specific series of one-dimensional targeted ciphertexts for ghost verification. In practice, several series of hidden ciphertexts corresponding to multiple hidden inputs can be simultaneously hidden into one specific series of targeted ciphertexts for verifying one specific target input. Only when these hidden inputs are correctly decoded and simultaneously authenticated, the recovered input can be confirmed as a target input in the designed big data environment. Hence, high flexibility is guaranteed in the proposed optical system.

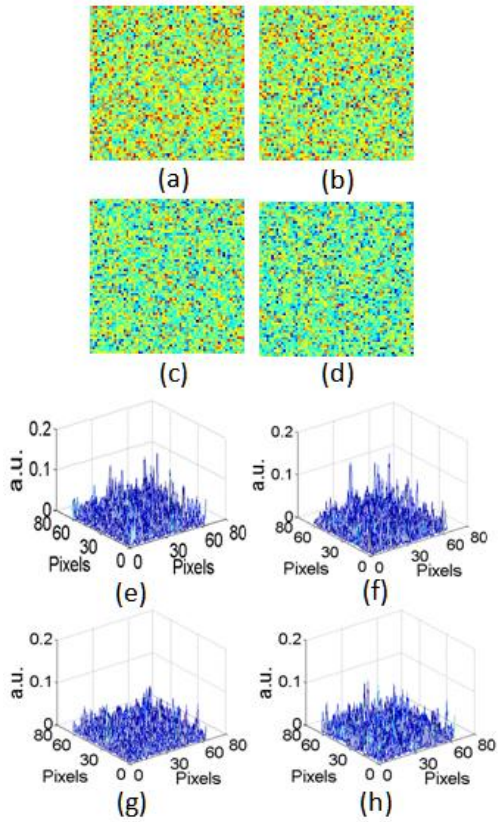

Fig. 8. (a)-(d) Four recovered inputs when the hidden ciphertexts are respectively selected from a wrong series of ciphertexts in the big data environment for the decoding and verification, and (e)-(h) authentication distributions respectively corresponding to (a)-(d).

4. Conclusions

A big data environment, for the first time to my knowledge, has been successfully designed and integrated into single-pixel imaging for securing information. It has been effectively demonstrated that many series of one-dimensional ciphertexts can be recorded by single-pixel bucket detector to form the big data environment. In addition, several hidden inputs are further encoded based on single-pixel ghost imaging by using a hierarchical structure, and their corresponding ciphertexts are synthesized into the big data environment for effectively verifying the hidden ghosts and correctly identifying the targeted ghosts. This new approach using big data environment could open up a different research perspective for single-pixel imaging [1–5,25–28] and optical security [16,23]. Either virtual-optics (computational)

approach or optical approach can be flexibly designed and implemented for the proposed system. It is expected that different big-data concepts can be continuously explored and applied to enrich single-pixel ghost-secured imaging area.

Funding

National Natural Science Foundation of China (NSFC) (61605165); Hong Kong Research Grants Council Early Career Scheme (25201416); Shenzhen Science and Technology Innovation Commission through Basic Research Program (JCYJ20160531184426473); The Hong Kong Polytechnic University (1-ZE5F).