The following publication W. Chen, "Correlated-Photon Secured Imaging by Iterative Phase Retrieval Using Axially-Varying Distances," in IEEE Photonics Technology Letters, vol. 28, no. 18, pp. 1932-1935, 15 Sept.15, 2016 is available at https://doi.org/10.1109/LPT.2016.2577596.

Correlated-Photon Secured Imaging by Iterative Phase Retrieval using Axially-Varying Distances

Wen Chen

***Abstract*—Correlated-photon imaging (also called ghost imaging) has attracted much attention in various fields, and its characteristics, such as single-pixel detection, have been extensively explored. In this letter, correlated-photon imaging is presented by using iterative phase retrieval with axially-varying distances for optical encryption. A series of phase-only masks are iteratively extracted by modulating the pre-generated random intensity-only maps, and propagation distances are axially varied in a random manner. It is illustrated that setup parameter can be applied as one of significant keys rather than just complementary one, and the iterative phase retrieval algorithm is applied to flexibly generate phase-only masks for the encoding.**

***Index Terms*—Correlated-photon secured imaging, iterative phase retrieval, optical encryption, axially-varying distances.**

I. INTRODUCTION

CORRELATED-photon imaging, known as ghost imaging [1]–[4], has been considered as one of the most interesting imaging technologies, and its application potential has been extensively explored, such as recognition [5], remote sensing [6] and optical security [7]–[10]. The imaging setup usually consists of two correlated optical beams and spatially-separated detectors [11]–[13]. At object beam arm, light interacts with the sample, and the waves are collected by single-pixel bucket detector (without spatial resolution). At reference beam arm, the light usually propagates in free space and received by charge-coupled device (CCD) or pinhole detector [1]–[13]. In correlated-photon imaging (ghost imaging), the reconstruction is usually conducted by correlating intensity signals recorded by two detectors [6].

Ghost imaging principle was initially explained based on quantum correlations associated with entangled photons generated by parametric down-conversion [1],[2]. Later, it was found that the classically correlated light can also be applied for photon-correlated imaging [3],[4]. The classical approach has attracted much attention, since pseudo-thermal light source can be applied and some related applications have been explored. Until now, there are a number of infrastructures and algorithms which have been developed for correlated-photon imaging, such as differential [11], normalized [12], and high-order [13]. In addition, signal or image processing algorithms, such as compressive sensing [14],[15], have also been integrated into the correlated-photon imaging system to resolve some application problems.

In recent years, correlated-photon imaging is applied for optical security [16]–[23], such as optical recognition or authentication [5],[9],[20]–[22] and optical encryption [7],[8],[10]. It has been found that due to its unique characteristics, correlated-photon imaging can provide a promising alternative for optical encoding. Either random phase profiles or reference intensity patterns can be employed as principle keys, which can guarantee system security. However, conventional systems do not provide the sufficiently varied strategies to encode the input, and security-key generation strategies may be estimated by attackers. Hence, it is desirable that more alternatives with guaranteed security can be further developed.

In this letter, correlated-photon imaging (ghost imaging) is applied by using iterative phase retrieval with axially-varying distances for optical encryption. A series of phase-only masks are iteratively extracted by modulating the pre-generated random intensity-only maps, and propagation distances are axially varied in a random manner. An approach to establishing correlated-photon secured imaging system is presented in this letter, where the major contribution is as follows: setup parameter, i.e., propagation distance, is flexibly designed and applied in a random manner to enhance system security. It realizes that setup parameter can be applied as one of significant keys rather than just complementary one [18] for data decoding in the modulation-based correlated-photon secured imaging system [18]. When the series of propagation distances is incorrectly applied, it is impossible to extract accurate phase-only masks via iterative phase retrieval algorithm for the decryption.

II. PRINCIPLES

Figure 1 shows a schematic setup for illustrating the correlated-photon secured imaging system using iterative phase retrieval algorithm with axially-varying distances. In this setup, a series of random intensity-only maps $[I_1(\mu,\nu)\ .....\ I_N(\mu,\nu)]$ are pre-generated as principal keys for extracting the series of phase-only masks $[M_1(\xi,\eta)\ .....\ M_N(\xi,\eta)]$ using an iterative phase retrieval algorithm.

This work was supported by the startup grant (1-ZE5F) from The Hong Kong Polytechnic University.

Wen Chen is with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China (e-mail: owen.chen@polyu.edu.hk).

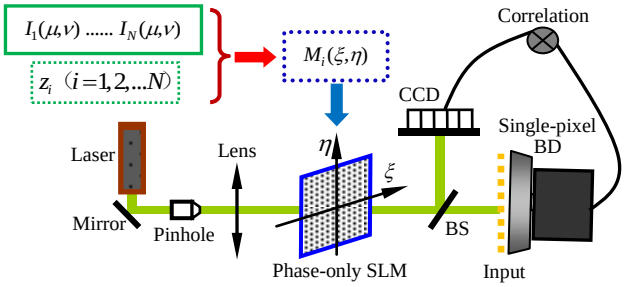


Fig. 1. Schematic setup for correlated-photon secured imaging (ghost-secured imaging) using iterative phase retrieval with axially-varying distances: SLM, spatial light modulator; BS, beam splitter; BD, bucket detector. Two-dimensional (2D) input is placed just before bucket detector, and is used as a plaintext. The 2D intensity patterns at reference beam arm can be computationally calculated [24], hence the use of CCD camera at reference beam arm can be further avoided to enhance acquisition efficiency in practice. A collecting lens may be placed between the input and bucket detector.

A. Optical Encoding

Here, the series of phase-only masks $[M_1(\xi,\eta)$ ..... $M_N(\xi,\eta)]$ is extracted by modulating a series of pre-generated random intensity-only maps $[I_1(\mu,\nu)$ ..... $I_N(\mu,\nu)]$, and these intensity-only maps act as principal keys for the proposed optical system. Iterative phase-mask retrieval procedure is described as follows, and extraction of phase-only mask $M_1(\xi,\eta)$ is illustrated as a typical example:

1) Wave back-propagation between the intensity $[I_1(\mu,\nu)]$ plane and phase-only mask (M1) plane is described by

$$O^{(n)}(\xi,\eta)=\mathrm{FrT}_{-z_1,\lambda}\left[I_1(\mu,\nu)\right], \tag{1}$$

where z_1 denotes axial distance between the intensity $[I_1(\mu,\nu)]$ plane and phase-only mask (M1) plane, n denotes iteration number (n=1,2,3.....N), λ denotes light wavelength, and FrT_{-z_1} denotes free-space back propagation [25],[26].

2) Unity-amplitude constraint is applied to update the complex-valued wavefront $O^{(n)}(\xi,\eta)$:

$$M_1^{(n)}(\xi,\eta)=O^{(n)}(\xi,\eta)\Big/\left|O^{(n)}(\xi,\eta)\right|, \tag{2}$$

where $|\ |$ denotes a modulus operation.

3) Propagate forward to the intensity $[I_1(\mu,\nu)]$ plane:

$$O^{(n)}(\mu,\nu)=\mathrm{FrT}_{z_1,\lambda}\left[M_1^{(n)}(\xi,\eta)\right]. \tag{3}$$

4) A constraint is applied to update the complex-valued wavefront $O^{(n)}(\mu,\nu)$:

$$\hat{O}^{(n)}(\mu,\nu)=\sqrt{I_1(\mu,\nu)}\,O^{(n)}(\mu,\nu)\Big/\left|O^{(n)}(\mu,\nu)\right|. \tag{4}$$

5) Correlation coefficient between the estimated output $\left|O^{(n)}(\mu,\nu)\right|^2$ and the desired output $I_1(\mu,\nu)$ is calculated to judge whether iterative process can be stopped. If the threshold is satisfied, the updated phase-only mask $M_1^{(n)}(\xi,\eta)$ is considered as phase-only mask M1, i.e., $M_1(\xi,\eta)$. Otherwise, the updated complex-valued wavefront $\hat{O}^{(n)}(\mu,\nu)$ in Eq. (4) is used in Eq. (1) for the next iteration (i.e., n=n+1).

Similarly, other phase-only masks $[M_2(\xi,\eta)$ .....$M_N(\xi,\eta)]$ can be iteratively extracted by using the correspondingly pre-generated random intensity-only maps $[I_2(\mu,\nu)$ ..... $I_N(\mu,\nu)]$, respectively. Here, axial distance z_i $(i=1,2,...N)$ is randomly generated for extracting each phase-only mask, i.e., $M_i(\xi,\eta)$.

After all phase-only masks $[M_1(\xi,\eta)$ ..... $M_N(\xi,\eta)]$ are extracted, they can be sequentially embedded into phase-only spatial light modulator (SLM) in practical applications, as shown in Fig. 1. As shown in Fig. 1, ciphertexts $\{B_i\}$ $(i=1,2,3,....N)$ are obtained by using single-pixel bucket detector (without spatial resolution), which can be described by [9],[10],[18],[20]

$$B_i=\iint\left|\left\{\mathrm{FrT}_{d,\lambda}\left[M_i(\xi,\eta)\right]\right\}O(\mu,\nu)\right|^2 d\mu d\nu, \tag{5}$$

where $O(\mu,\nu)$ denotes the input (i.e., plaintext), and d denotes axial distance between the phase-mask plane and detector plane. In practice, the series of 1D intensity points recorded can be sequentially transmitted via various communication channels, such as internet. A flow chart is given in Fig. 2 to clearly illustrate the optical encoding procedure aforementioned.

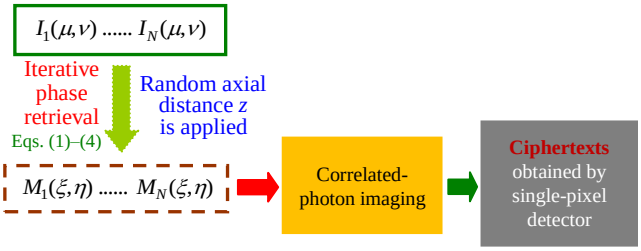


Fig. 2. Flow chart for schematically illustrating optical encryption process. N is equivalent to 30000.

B. Optical Decoding

The series of pre-generated random intensity-only maps $[I_1(\mu,\nu)$ .....$I_N(\mu,\nu)]$ and the series of axial distances z_i $(i=1,2,...N)$ are transmitted as principal keys. Flow chart for the decoding process is shown in Fig. 3, and the detailed procedure consists of the following steps:

1) When the series of pre-generated random intensity-only maps $[I_1(\mu,\nu)$ .....$I_N(\mu,\nu)]$ and the series of random distances z_i $(i=1,2,...N)$ are available to authorized receiver, a series of phase-only masks $[M_1(\xi,\eta)$ .....$M_N(\xi,\eta)]$ can be extracted by using the iterative phase retrieval algorithm, i.e., Eqs. (1)–(4).

2) A series of reference intensity patterns can be obtained by

$$R_i(\mu,\nu)=\left|\mathrm{FrT}_{d,\lambda}\left[M_i(\xi,\eta)\right]\right|^2, \tag{6}$$

where $R_i(\mu,\nu)$ $(i=1,2,...N)$ denotes a series of intensity patterns obtained at reference beam arm.

3) The calculated reference intensity patterns are correlated with ciphertexts $\{B_i\}$ $(i=1,2,...N)$ for information retrieval, which can be described by [6]–[10], [20]–[22]

$$\hat{O}(\mu,\nu)=\langle BR(\mu,\nu)\rangle-\langle B\rangle\langle R(\mu,\nu)\rangle, \tag{7}$$

where $\hat{O}(\mu,\nu)$ denotes a decoded image, and $\langle\cdot\rangle$ denotes ensemble average. Note that different from previous work [9], the series of pre-generated random intensity maps is used as principal keys in the proposed optical system, and the decoding objective of this study is to extract the input data rather than for the authentication. In this investigation, previous work in Ref. [18] has been effectively studied by using an iterative phase retrieval with axially-varying distances to enhance system security, and system parameters or phase-only masks can be flexibly generated.

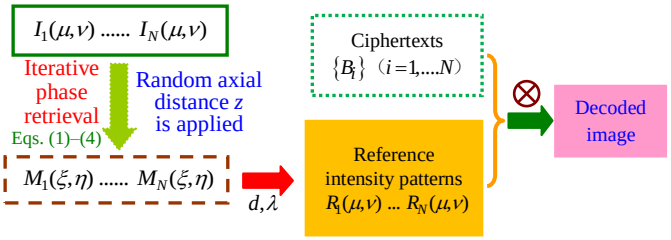


Fig. 3. Flow chart for schematically illustrating the decryption process. Symbol ⊗ denotes correlation. Simplified decryption with less measurements is also applicable, hence strategy to distribute the keys should be further designed.

III. System Results

A schematic setup for correlated-photon secured imaging system shown in Fig. 1 is computationally conducted. The series of extracted phase-only masks can be sequentially embedded into a device, such as phase-only SLM (64×64 pixels). In the setup, plane wave can be generated by the combination of pinhole and a lens for the illumination. Light wavelength is 630.0 nm, and the waist is 740.0 μm. Each pre-generated intensity-only map $[I_1(\mu,\nu)$ ..... $I_N(\mu,\nu)]$ is randomly distributed in the range of (0, 800], and the series of axial distances z_i $(i=1,2,...N)$ is randomly distributed in the range of [2.0 cm, 70.0 cm]. In the encoding setup, axial distance d is 35.0 cm. When the series of extracted phase-only masks, i.e., N=30000, is sequentially embedded, one-dimensional (1D) ciphertexts are recorded by using bucket detector.

Figure 4(a) shows a typical pre-generated random intensity map $I_i(\mu,\nu)$, and its corresponding phase-only mask $M_i(\xi,\eta)$ is extracted in Fig. 4(b). The iterative operation is requested during phase extraction, and a relationship between the number of iterations and correlation coefficients is shown in Fig. 4(c). It can be seen that a rapid convergence rate is achieved, and only 10 iterations are requested. Here, the threshold is set as 0.95 for the iterations. In correlated-photon imaging (ghost imaging), it is important that the extracted phase-only masks are not strongly correlated. Figure 5 shows the correlations among the extracted phase-only masks $[M_1(\xi,\eta)$ ..... $M_N(\xi,\eta)]$. It is illustrated that the extracted phase-only masks are strongly uncorrelated, which satisfies the system requirement.

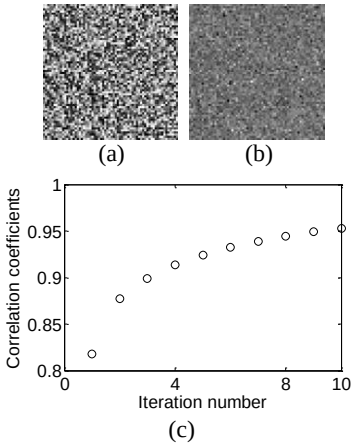


Fig. 4. (a) A typical pre-generated random intensity map $I_i(\mu,\nu)$, (b) the correspondingly extracted phase-only mask $M_i(\xi,\eta)$, and (c) a relationship between the number of iterations and correlation coefficients during the phase-mask extraction.

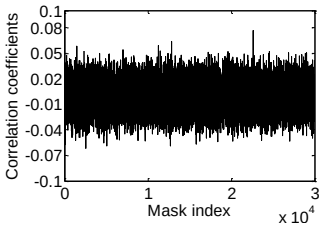


Fig. 5. Correlations among the extracted phase-only masks $[M_1(\xi,\eta)$ ..... $M_N(\xi,\eta)]$. As an example, the first extracted phase-only mask $M_1(\xi,\eta)$ is used as a base for the calculations.

When the series of extracted phase-only masks $[M_1(\xi,\eta)$ ..... $M_N(\xi,\eta)]$ is sequentially embedded, 1D ciphertexts, as shown in Fig. 6(a), are obtained by using single-pixel bucket detector. It can be seen in Fig. 6(a) that information related to the input cannot be observed, and the 2D input is fully encoded. In the proposed optical security system, the series of pre-generated random intensity-only maps $[I_1(\mu,\nu)$ ..... $I_N(\mu,\nu)]$ and the series of random distances z_i $(i=1,2,...N)$ are considered as principal keys. When these keys are correctly applied (such as by authorized receivers), a decoded input image is obtained as shown in Fig. 6(b). Correlation coefficient and peak signal-to-noise ratio (PSNR) for Fig. 6(b) are 0.88 and 10.56 dB, respectively. It can be seen in Fig. 6(b) that the decoding quality is satisfactory, since significant information related to the input (i.e., Chinese character "North") can be clearly observed.

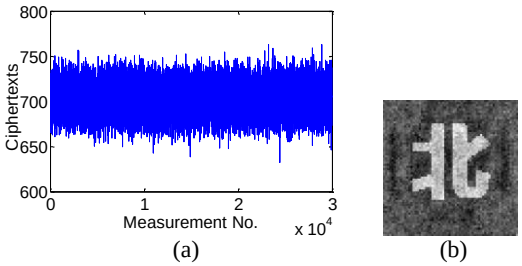
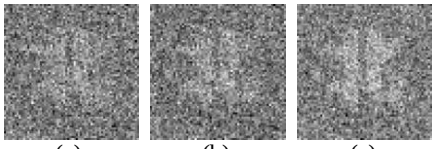


Fig. 6. (a) The 1D ciphertexts, and (b) a decoded input image obtained when all keys are correctly applied. Here, the total measurements are 30000, i.e., N=30000. Note that the measurements may be redundant, and ciphertexts and security keys may be distributed by additional protection approaches, such as multi-layer.

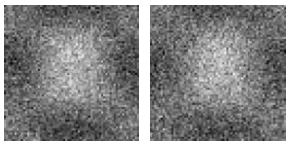
In optical security system, it is important to conduct the eavesdropping test. Here, it is assumed that unauthorized receiver knows the encoding infrastructure, and security keys are partially eavesdropped. Figures 7(a)–7(c) show the decoded images, when 30.0%, 35.0% and 45.0% of security keys are eavesdropped for the decoding, respectively. For instance, 30.0 % pixels of each pre-generated intensity map $[I_1(\mu,\nu)$ ..... $I_N(\mu,\nu)]$ are eavesdropped in Fig. 7(a). It has also been assumed that other principal security keys, i.e., the series of random distances z_i $(i=1,2,...N)$, are fully eavesdropped. Correlation coefficients for Figs. 7(a)–7(c) are 0.28, 0.32 and 0.40, respectively. The PSNRs for Figs. 7(a)–7(c) are 7.94 dB, 8.02 dB and 8.19 dB, respectively. It is illustrated that only when a number of security keys (such as larger than 30.0%) are eavesdropped, unauthorized receiver can slightly retrieve the input information. It is worth noting that when the series of random distances z_i $(i=1,2,...N)$ is not assumed to be fully eavesdropped, the higher eavesdropping percentage may be requested to slightly observe the input.



(a) (b) (c)

Fig. 7. Decoded images obtained when (a) 30.0%, (b) 35.0% and (c) 45.0% of security keys are eavesdropped by unauthorized receiver. Here, it is assumed that no any whole intensity-only map has been eavesdropped.

Different from previous work [7],[8],[18], a series of axial distances z_i $(i=1,2,...N)$ are generated in a random manner during the iterative phase-mask retrieval. Performance of this principal key is further analyzed. Figure 8(a) shows a decoded input, when a fixedly axial distance (i.e., 20.0 cm) is employed for the extraction of all phase-only masks during optical decoding. Figure 8(b) shows a decoded image, when only the series of axial distances z_i $(i=1,2,...N)$ is wrongly used. It can be seen in Figs. 8(a) and 8(b) that when principal keys are wrongly used (such as by unauthorized receivers), no information related to the input can be obtained. For brevity, performance of complementary setup parameters, such as wavelength λ and distance d, is not presented. In the future work, more detailed statistical analyses [27] can be further conducted. The proposed method is also different from previous work in Ref. [28], since modulation-based correlated-photon secured imaging is presented by using an iterative phase retrieval algorithm with axially-varying distances. In the proposed optical security system, iterative phase retrieval algorithm is applied to flexibly generate phase-only masks from the pre-generated intensity patterns, and computational approach can be applied at reference beam arm without increasing system complexity. In the proposed optical security system, setup parameter, i.e., propagation distance, is flexibly designed and applied in a random manner to enhance system security. It realizes that setup parameter can be applied as one of significant keys rather than just complementary one [18] in the modulation-based correlated-photon secured imaging system [18].



(a) (b)

Fig. 8. A decoded input image obtained (a) when only one fixedly axial distance is employed for extraction of all phase-only masks during the decryption, and (b) when only the series of axial distances z_i $(i=1,2,...N)$ is wrongly used.

IV. CONCLUSIONS

Iterative phase retrieval with axially-varying distances has been presented for correlated-photon secured imaging (i.e., ghost-secured imaging). A series of phase-only masks are iteratively retrieved by modulating the pre-generated random intensity-only maps, and propagation distances are axially varied in a random manner. It has been illustrated that optical security is effectively guaranteed due to the application of iterative phase retrieval with axially-varying distances in correlated-photon imaging. The numerical results demonstrate that setup parameter can be applied as one of significant keys rather than just complementary one.

REFERENCES

[1] D. V. Strekalov, A. V. Sergienko, D. N. Klyshko, and Y. H. Shih, "Observation of two-photon "ghost" interference and diffraction," *Phys. Rev. Lett.*, vol. 74, no. 18, pp. 3600–3603, May 1995.

[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*, vol. 52, no. 5, pp. R3429–R3432, Nov. 1995.

[3] A. Gatti, E. Brambilla, M. Bache, and L. A. Lugiato, "Ghost imaging with thermal light: comparing entanglement and classical correlation," *Phys. Rev. Lett.*, vol. 93, no. 9, pp. 093602, Aug. 2004.

[4] A. Valencia, G. Scarcelli, M. D'Angelo, and Y. H. Shih, "Two-photon imaging with thermal light," *Phys. Rev. Lett.*, vol. 94, no. 6, pp. 063601, Feb. 2005.

[5] Y. K. Liu, Y. Wang, D. Z. Cao, and S. H. Zhang, "Pattern recognition based on the correlated intensity fluctuations of thermal light," *J. Opt. Soc. Am. A*, vol. 31, no. 7, pp. 1547–1551, Jun. 2014.

[6] B. I. Erkmen, "Computational ghost imaging for remote sensing," *J. Opt. Soc. Am. A*, vol. 29, no. 5, pp. 782–789, Apr. 2012.

[7] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," *Opt. Lett.*, vol. 35, no. 14, pp. 2391–2393, Jul. 2010.

[8] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," *Appl. Phys. Lett.*, vol. 101, no. 10, pp. 101108, Sep. 2012.

[9] W. Chen and X. Chen, "Ghost imaging for three-dimensional optical security," *Appl. Phys. Lett.*, vol. 103, no. 22, pp. 221106, Nov. 2013.

[10] W. Chen and X. Chen, "Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption," *EPL,* vol. 109, no. 1, pp. 14001, Jan. 2015.

[11] F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, "Differential ghost imaging," *Phys. Rev. Lett.*, vol. 104, no. 25, pp. 253603, Jun. 2010.

[12] B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, "Normalized ghost imaging," *Opt. Express*, vol. 20, no. 15, pp. 16892–16901, Jul. 2012.

[13] K. W. C. Chan, M. N. O'Sullivan, and R. W. Boyd, "High-order thermal ghost imaging," *Opt. Lett.*, vol. 34, no. 21, pp. 3343–3345, Nov. 2009.

[14] O. Katz, Y. Bromberg, and Y. Silberberg, "Compressive ghost imaging," *Appl. Phys. Lett.*, vol. 95, no. 13, pp. 131110, Sep. 2009.

[15] W. K. Yu, M. F. Li, X. R. Yao, X. F. Liu, L. A. Wu, and G. J. Zhai, "Adaptive compressive ghost imaging based on wavelet trees and sparse representation," *Opt. Express*, vol. 22, no. 6, pp. 7133–7144, Mar.2014.

[16] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.

[17] J. Liu, X. Xu, Q. Wu, J. T. Sheridan, and G. Situ, "Information encryption in phase space," *Opt. Lett.*, vol. 40, no. 6, pp. 859–862, Mar. 2015.

[18] W. Chen, "Optical data security system using phase extraction scheme via single-pixel detection," *IEEE Photon. J.*, vol. 8, no. 1, pp. 7801507 (7pp), Feb. 2016.

[19] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.*, vol. 36, no.1, pp. 22–24, Jan. 2011.

[20] W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," *Opt. Lett.*, vol. 38, no. 4, pp.546–548, Feb. 2013.

[21] W. Chen and X. Chen, "Grayscale object authentication based on ghost imaging using binary signals," *EPL*, vol. 110, no. 4, pp. 44002, May 2015.

[22] W. Chen and X. Chen, "Optical authentication via photon-synthesized ghost imaging using optical nonlinear correlation," *Opt. Lasers Eng.*, vol. 73, pp. 123–127, Oct. 2015.

[23] W. Chen, X. Chen, A. Anand, and B. Javidi, "Optical encryption using multiple intensity samplings in the axial domain," *J. Opt. Soc. Am. A*, vol. 30, no. 5, pp. 806–812, Apr. 2013.

[24] J. H. Shapiro, "Computational ghost imaging," *Phys. Rev. A*, vol. 78, no. 6, pp. 061802(R), Dec. 2008.

[25] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762–764, Jun. 1999.

[26] J. W. Goodman, *Introduction to Fourier Optics, 2nd ed.* (New York, McGraw-Hill, 1996).

[27] A. Markman and B. Javidi, "Full-phase photon-counting double-random-phase encryption," *J. Opt. Soc. Am. A*, vol. 31, no. 2, pp. 394–403, Jan. 2014.

[28] I. Moon and B. Javidi, "Three-dimensional recognition of photon-starved events using computational integral imaging and statistical sampling," *Opt. Lett.*, vol. 34, no. 6, pp. 731–733, Mar. 2009.