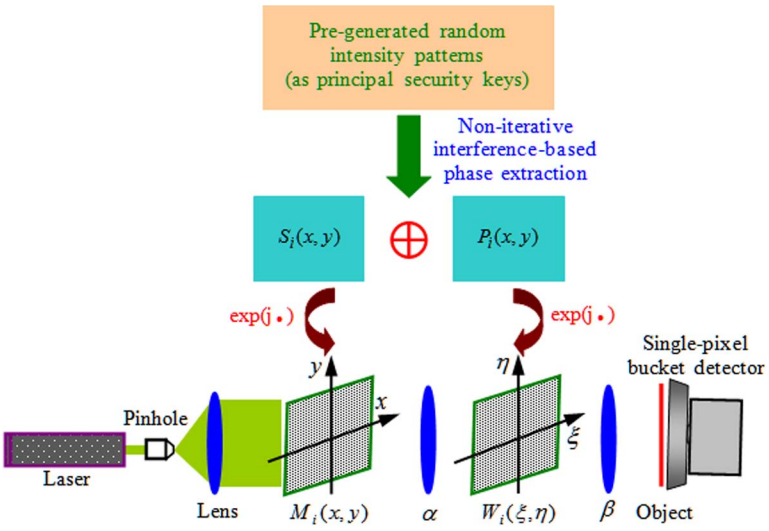
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Optical Data Security System Using Phase Extraction Scheme via Single-Pixel Detection

Volume 8, Number 1, February 2016

Wen Chen



DOI: 10.1109/JPHOT.2016.2523994
1943-0655 © 2016 IEEE

Optical Data Security System Using Phase Extraction Scheme via Single-Pixel Detection

Wen Chen

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China

DOI: 10.1109/JPHOT.2016.2523994

Manuscript received January 2, 2016; revised January 27, 2016; accepted January 27, 2016. Date of publication February 3, 2016; date of current version February 15, 2016. This work was supported by the Startup Grant (1-ZE5F) from The Hong Kong Polytechnic University. Corresponding author: W. Chen (e-mail: owen.chen@polyu.edu.hk).

Abstract: Single-pixel imaging via phase extraction is presented for optical security and flexibility enhancement. A series of random intensity patterns are pregenerated as principal security keys and are sequentially encoded into phase-only masks. Since different optical sensing infrastructures can be arbitrarily designed for the extraction of phase-only masks and object encoding, high flexibility and high security with a largely indirect space for phase are achieved in the proposed optical security system. This finding may advance single-pixel correlated imaging as a quantum or classical technology with potential for significantly enriching the security field.

Index Terms: Optical imaging system, single-pixel photon detection, optical data security, phase extraction.

1. Introduction

Single-pixel correlated imaging, widely known as ghost imaging [1], has been one of the most interesting topics in many application fields due to its remarkable characteristics. In single-pixel correlated imaging, the sample can be reconstructed by scanning the camera at reference beam arm, in which the sample is not located [1]. Since the characteristics obtained with entangled photons are also found to be realized by using classical pseudo-thermal light source [2], single-pixel correlated imaging has been explored in classical domain, such as optical sensing [1] and optical encryption [3], [4]. It has also been illustrated that correlated-photon image is formed intrinsically due to classical coherence propagation [1], [5].

Since a series of random phase-only masks are applied, single-pixel correlated imaging [3], [4] has attracted much attention in optical data security field and effectively enriches conventional optical security field [6]–[16]. It is illustrated that single-pixel imaging has a potential to prevent some attacks [15], [16] when the keys can be continuously modified. However, conventional single-pixel correlated imaging systems are usually established based on direct use or simple modulation of phase-only masks [3], [4], and system flexibility is limited. It is also desirable that the indirect space for phase can be large to make single-pixel correlated imaging system difficult for unauthorized receivers.

In this paper, single-pixel imaging via phase extraction is presented for optical security and flexibility enhancement. A series of random intensity patterns are pre-generated as principal

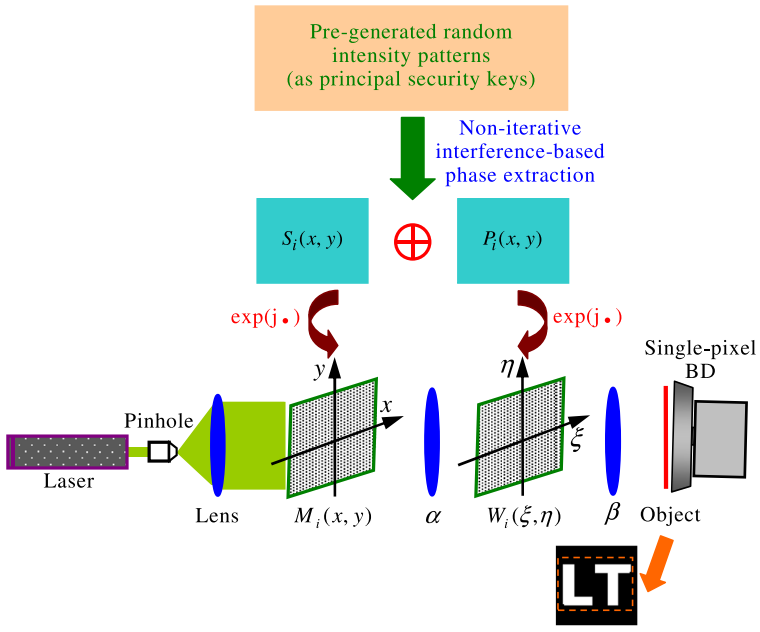


Fig. 1. Schematic setup for illustrating the object encoding process in the proposed optical system: BD, bucket detector. The dashed box denotes region of interest. Since the wavefront at reference beam arm can be computationally calculated, it is not shown here. In practice, a collecting lens can also be placed between the object and bucket detector.

security keys and are sequentially encoded into phase-only masks. Since different optical sensing infrastructures can be arbitrarily designed, respectively, for the extraction of phase-only masks and object encoding, high flexibility and high security with a largely indirect (or virtual) space for phase are achieved in the proposed system.

2. Principles

Fig. 1 shows a schematic setup for the proposed optical security system. A series of random intensity patterns $I_i(\mu,\nu)$ $[i = 1, 2, 3, \ldots N]$ are pre-generated as principal security keys, and various phase extraction algorithms, such as computer-generated hologram [17], can be applied to encode each pre-generated random intensity pattern into phase-only masks. Here, non-iterative interference-based phase extraction algorithm [18], [19] is applied as one typical example to encode each pre-generated random intensity pattern $I_i(\mu,\nu)$ $[i = 1, 2, 3, \ldots, N]$ into two noisy phase-only masks. The objective is to ensure that interference intensity $|\mathrm{IFT}[(\mathrm{FT}\{\exp[jS_i(x,y)]\})\Im(f_x, f_y; d)] + \mathrm{IFT}[(\mathrm{FT}\{\exp[jP_i(x,y)]\})\Im(f_x, f_y; d)]|^2$ is close to each pre-generated random intensity pattern $I_i(\mu,\nu)$, where FT and IFT respectively denote Fourier transform and inverse Fourier transform, $\exp[jS_i(x,y)]$ and $\exp[jP_i(x,y)]$ denote the extracted phase-only masks, $j = \sqrt{-1}$, d denotes axial distance, and $\Im(f_x, f_y; d)$ denotes transfer function [5]. Non-iterative interference-based phase extraction algorithm is analytically conducted, and two phase-only masks are, respectively, extracted by

$$S_i(x,y) = \mathrm{ang}\left[\mathrm{IFT}\left(\frac{\left\{\mathrm{FT}\left[\hat{O}_i(\mu,\nu)\right]\right\}}{\Im(f_x, f_y; d)}\right)\right] - \arccos\left(\frac{\left\{\mathrm{abs}\left[\mathrm{IFT}\left(\frac{\{\mathrm{FT}[\hat{O}_i(\mu,\nu)]\}}{\Im(f_x,f_y;d)}\right)\right]\right\}}{2}\right) \quad (1)$$

$$P_i(x,y) = \mathrm{ang}\left\{\mathrm{IFT}\left(\frac{\left\{\mathrm{FT}\left[\hat{O}_i(\mu,\nu)\right]\right\}}{\Im(f_x, f_y; d)}\right) - \exp[jS_i(x,y)]\right\} \quad (2)$$

where $\hat{O}_i(\mu,\nu) = \sqrt{I_i(\mu,\nu)}\exp[j\Re(\mu,\nu)]$, $\Re(\mu,\nu)$ denotes a 2-D map randomly distributed in the range of $[0, 2\pi]$, and ang and abs, respectively, denote the extraction of argument and magnitude of a complex number.

As seen in Fig. 1, during object encoding, each pair of the extracted phase-only masks $M_i(x,y)$ {i.e., $\exp[jS_i(x,y)]$} and $W_i(\xi,\eta)$ {i.e., $\exp[jP_i(x,y)]$} is sequentially displayed in phase-only spatial light modulators (SLMs) using another optical sensing infrastructure, i.e., cascaded. Since cascaded structure is applied during object encoding, coordinate of $\exp[jP_i(x,y)]$ is re-defined as (ξ,η). A series of intensity points $\{B_i\}[i = 1,2,3,\ldots,N]$, acting as ciphertexts, can be obtained by using single-pixel bucket detector (without spatial resolution), which are described by

$$B_i = \int\int \left|\left[\mathrm{FrFT}_{\beta,\beta}\left(\left\{\mathrm{FrFT}_{\alpha,\alpha}[M_i(x,y)]\right\}W_i(\xi,\eta)\right)\right]O(\mu,\nu)\right|^2 d\mu\, d\nu \tag{3}$$

where $O(\mu,\nu)$ denotes amplitude transmittance of the object, FrFT denotes fractional Fourier transform [20], and α and β denote FrFT function orders. The 1-D FrFT with order α is described by [20]

$$\mathrm{FrFT}_\alpha[M_i(x)] = \int_{-\infty}^{+\infty} M_i(x)H_\alpha(\xi_\alpha,x)dx \tag{4}$$

where $H_\alpha(\xi_\alpha,x) = \begin{cases} Q\exp\{j\pi[\xi_\alpha^2\cot(\alpha\pi/2) + x^2\cot(\alpha\pi/2) - 2\xi_\alpha x\csc(\alpha\pi/2)]\}, & (\text{if } \alpha \neq 2m) \\ \delta(\xi_\alpha - x), & (\text{if } \alpha = 4m) \\ \delta(\xi_\alpha + x), & (\text{if } \alpha = 4m \pm 2) \end{cases}$

m denotes an integer, and $Q = \sqrt{1 - j\cot(\alpha\pi/2)}$. The description of 2-D FrFT is straightforward.

Only one series of the pre-generated random intensity patterns $I_i(\mu,\nu)$ $[i = 1,2,3,\ldots,N]$ should be stored or transmitted as principal security keys. For object decoding, the interference-based infrastructure with accurate parameters is first applied for extracting phase-only masks [i.e., $M_i(x,y)$ and $W_i(\xi,\eta)$] from principal security keys [i.e., $I_i(\mu,\nu)$], and subsequently, a cascaded infrastructure with the extracted phase-only masks is employed for generating each intensity pattern at reference beam arm $k_i(\mu,\nu)$ $[i = 1,2,3,\ldots,N]$ which can be described by function $|\mathrm{FrFT}_{\beta,\beta}(\{\mathrm{FrFT}_{\alpha,\alpha}[M_i(x,y)]\}W_i(\xi,\eta))|^2$. Finally, the series of calculated reference intensity patterns $k_i(\mu,\nu)$ $[i = 1,2,3,\ldots,N]$ is correlated with the ciphertexts $\{B_i\}$ $[i = 1,2,3,\ldots,N]$ for extracting the decoded object using correlation function $[\langle Bk(\mu,\nu)\rangle - \langle B\rangle\langle k(\mu,\nu)\rangle]$. It is worth noting that when the less number of measurements is used, the object can also be recovered and is of the lower quality. Hence, security key management or distribution is an important topic in practical applications.

3. Results and Discussion

In Fig. 1, the plane wave (wavelength of 630.0 nm and waist of 740.0 μm) is simulated and applied for the illumination to illustrate validity of the proposed method. During the generation of phase-only masks and object encoding, the axial distance d is 20.0 cm, and FrFT function orders α and β are 0.40 and 0.80, respectively. By using the proposed method, a series of phase-only masks $M_i(x,y)$ and $W_i(\xi,\eta)$ $(i = 1,2,3,\ldots,N)$ (i.e., $N = 25000$) are generated and are cascaded and sequentially embedded into phase-only SLMs (64×64 pixels and pixel pitch of 15 μm) during object encoding. Fig. 2(a) and (b) show two typical pre-generated random intensity patterns, and Fig. 2(c) and (d) show the typically extracted phase-only masks $M_i(x,y)$ and $W_i(\xi,\eta)$, respectively. When the extracted phase-only masks $M_i(x,y)$ and $W_i(\xi,\eta)$ are sequentially cascaded at object beam arm, a series of intensity points $\{B_i\}$, acting as ciphertexts, are obtained by using single-pixel bucket detector (without spatial resolution) as shown in Fig. 2(e). It is illustrated in Fig. 2(e) that only 1-D noisy map is obtained as ciphertexts after object encoding. Fig. 2(f) shows the correlations between each pair of $M_i(x,y)$ and $W_i(\xi,\eta)$.

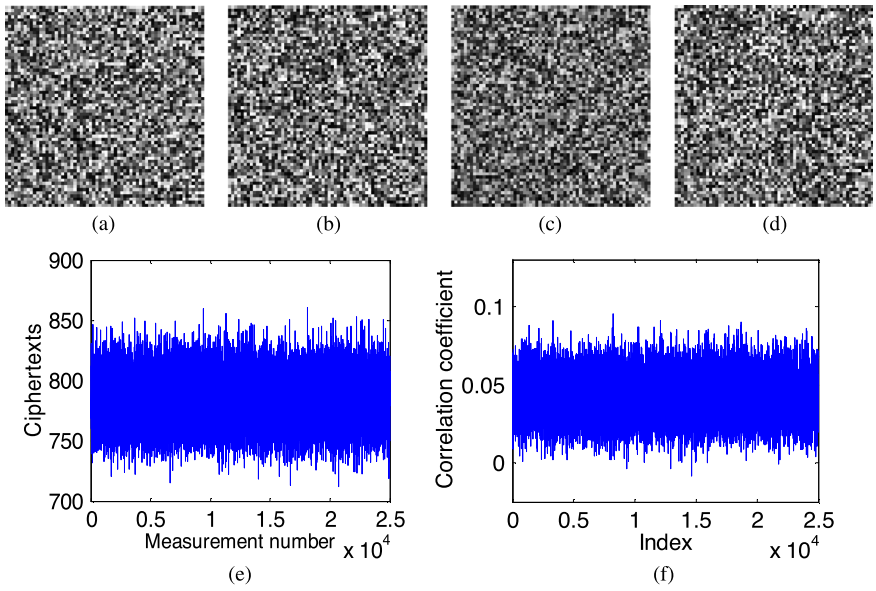


Fig. 2. (a) and (b) Two typical pre-generated random intensity patterns, typically extracted phase-only mask (c) $M_i(x, y)$ and (d) $W_i(\xi, \eta)$. (e) Ciphertexts obtained by single-pixel bucket detector (without spatial resolution). (f) Correlation between each pair of $M_i(x, y)$ and $W_i(\xi, \eta)$.

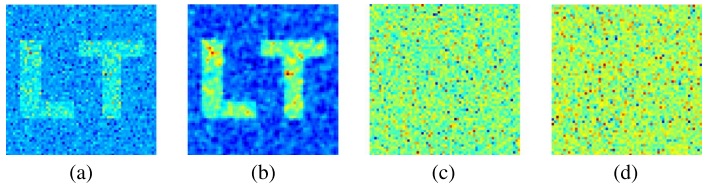


Fig. 3. (a) Decoded object obtained when principal keys and imaging infrastructures with setup parameters are correctly applied for the decoding, (b) a recovered object obtained after filtering the image in (a) using Gaussian low-pass filter, (c) a decoded object obtained when a series of wrong pre-generated random intensity patterns are applied for the decoding, and (d) a decoded object obtained when only wavelength and axial distance are incorrectly applied during phase-mask retrieval for the decoding.

The object shown in inset of Fig. 1 is encoded in the developed optical security system. Fig. 3(a) shows a decoded object, when principal security keys and imaging infrastructures with setup parameters are correctly applied for the decoding. Peak signal-to-noise ratio (PSNR) for Fig. 3(a) is 6.66 dB. In this study, the PSNR is calculated to evaluate quality of the decoded objects within the region of interest (indicated in Fig. 1). It can be seen in Fig. 3(a) that when security keys are available to authorized receivers, object information can be effectively retrieved. Quality of the decoded object in Fig. 3(a) can be further enhanced by using various post-processing algorithms, and Fig. 3(b) shows a recovered object obtained by using Gaussian low-pass filter to the image in Fig. 3(a). The PSNR for Fig. 3(b) is 8.24 dB. In the proposed system, the series of pre-generated random intensity patterns $I_i(\mu, \nu)$ $(i = 1, 2, 3, \ldots, N)$ is used as principal security keys. Fig. 3(c) shows a decoded object, when a series of wrong pre-generated random intensity patterns are employed to generate phase-only masks during the decoding, such as by unauthorized receivers. The PSNR for Fig. 3(c) is 4.15 dB. Fig. 3(d) shows a decoded object, when only the wavelength (an error of 10.0 nm) and axial distance (an error of 1.0 cm) are wrongly used during the generation of phase-only masks for the decoding. The PSNR for Fig. 3(d) is 3.96 dB. It can be seen in Fig. 3(c) and (d) that when the keys are wrong, only noisy distributions can be obtained. It should be emphasized that different imaging infrastructures can

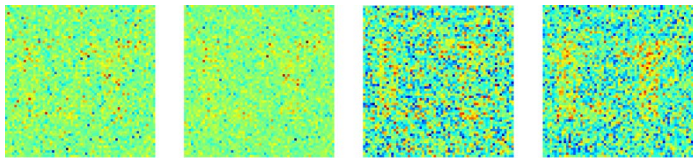


Fig. 4. Eavesdropping attacks: decoded objects obtained when (a) 60.0% and (b) 65.0% pixels of each pre-generated random intensity pattern $I_i(\mu,\nu)$ $(i = 1,2,3,\ldots,N)$ are eavesdropped for the decoding. Eavesdropping attacks to conventional method: decoded objects obtained when (c) 8.0% and (d) 13.0% pixels of each random phase-only mask are eavesdropped for the decoding. Here, it has been assumed that no any whole or complete principal key is eavesdropped.

be arbitrarily applied, respectively, for the generation of phase-only masks and object encoding, and without proper applications of imaging infrastructures, it is impossible to extract the object. For the sake of brevity, performance of other parameters, such as FrFT function orders, is not presented here.

Attack analyses using different percentages of eavesdropping are conducted to further evaluate the proposed approach, when an unauthorized receiver has got some information related to principal security keys, i.e., $I_i(\mu,\nu)$ $(i = 1,2,3,\ldots,N)$. It is assumed that unauthorized receiver knows the designed imaging infrastructures, i.e., non-iterative interference for phase-mask generation and cascaded phase-only masks for object encoding. Fig. 4(a) and (b) show the decoded objects, when 60.0% and 65.0% pixels of each pre-generated random intensity pattern are eavesdropped for the decoding, respectively. The PSNRs for Fig. 4(a) and (b) are 4.44 dB and 4.56 dB, respectively. For a comparison, conventional approach directly using a series of random phase-only masks is also conducted, and the eavesdropping attacking results are shown in Fig. 4(c) and (d). The PSNRs for Fig. 4(c) and (d) are 4.27 dB and 4.35 dB, respectively. As seen in Fig. 4(a)–(d), a much larger number of pixels in principal keys should be eavesdropped (or attacked) to slightly observe the object in the proposed method compared to previous work.

The proposed method can also be applied to multiple-object encoding and decoding, and the whole process can be carried out as follows: 1) Each object can be individually encoded; hence, several series of 1-D photons [i.e., ciphertexts like those in Fig. 2(e)] can be sequentially recorded. For instance, three objects [i.e., $c(\mu,\nu)$, $d(\mu,\nu)$, and $e(\mu,\nu)$] are independently encoded, and three series of recorded photons are respectively denoted as $\{C_i\}$, $\{D_i\}$ and $\{E_i\}$ $(i = 1,2,3,\ldots,N)$. The same series of $M_i(x,y)$ and $W_i(\xi,\eta)$ is used for each object encoding. 2) Photon synthesis is conducted by using $\{C_i\} \times \{D_i\} \times \{E_i\}$ or $\{C_i\} + \{D_i\} + \{E_i\}$, and the synthesized photons are used as final ciphertexts. 3) To avoid cross-talk term, other series of photons, such as $\{C_i\} \times \{D_i\}$ or $\{C_i\} + \{D_i\}$, can be considered as additional parameters for extracting one specific series of photons (such as $\{E_i\}$) for decoding the object, i.e., $e(\mu,\nu)$. Similarly, other objects $c(\mu,\nu)$ and $d(\mu,\nu)$ can also be extracted without cross-talk term during the decoding.

Some discussions and explanations related to the proposed approach are briefly described as follows.

1) Since a series of random intensity patterns $I_i(\mu,\nu)$ $(i = 1,2,3,\ldots,N)$ are pre-generated, either non-iterative or iterative phase retrieval algorithms can be flexibly designed to extract phase-only masks. For instance, non-iterative interference-based phase retrieval can effectively reduce computational time without compromising system security, and analytical solutions can be generated. Various imaging infrastructures [see typical ones in Fig. 5(a)–(c)], such as cascaded, interference or mixture of cascaded and interference, can be arbitrarily applied, respectively, for phase-mask generation and object encoding; hence, high flexibility can be guaranteed.
2) Each pre-generated random intensity pattern $I_i(\mu,\nu)$ $(i = 1,2,3,\ldots,N)$ can be flexibly encoded into a different number of phase-only masks. Although a large number of phase-only masks can be arbitrarily generated and applied during object encoding, only one

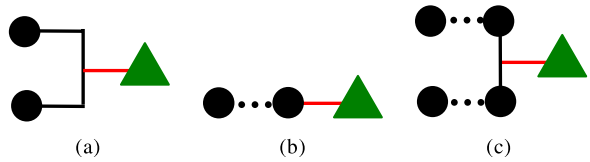


Fig. 5. Several typical imaging infrastructures for phase-mask generation and object encoding, such as (a) interference, (b) cascaded, and (c) a mixture of interference and cascaded: Triangle denotes a random intensity pattern. Circles denote the extracted phase-only masks. In practice, multiple phase-only masks can be flexibly generated rather than only two illustrated here, and different imaging infrastructures can be applied, respectively, for phase-mask generation and object encoding.

series of pre-generated random intensity patterns is requested to be transmitted as principal security keys. Alternatively, these intensity patterns $I_i(\mu, \nu)$ can be further transformed or compressed to be only 1-D vector using random intensity generator.

3) For the decoding, the pre-generated random intensity patterns, acting as principal keys, should be transformed to intensity patterns at reference beam arm by using at least two imaging infrastructures with arbitrarily-designed phase-mask arrangements, hence a largely indirect space for phase is available. It has also been illustrated that due to the designed intensity modulation strategy, security enhancement (i.e., with large eavesdropping percentage) can be achieved; see Fig. 4(a)–(d).
4) The larger data space, such as 8 or 10 bits, may be designed and applied to pre-generate random intensity patterns as principal security keys compared with those keys directly using random phase-only masks (i.e., smaller than 3 bits) in previous systems.
5) The objective of object decryption is to clearly observe the input using correct security keys, and the results in Fig. 3(a) and (b) can be satisfactory. In this study, the method can also be applied to encode grayscale image like previous work [4]. The decoding quality will be lower, since more information should be recovered during the decoding compared with binary-image encoding case. In practice, some algorithms, such as differential [21], can be applied to enhance decryption quality.

4. Conclusion

Single-pixel correlated imaging via phase extraction has been presented for optical security and flexibility enhancement. A series of random intensity patterns are pre-generated as principal security keys, and are sequentially encoded into phase-only masks. The numerical results and corresponding analyses demonstrate that since different optical sensing infrastructures can be arbitrarily designed for the extraction of phase-only masks and object encoding, high flexibility, and high security with a largely indirect (or virtual) space for phase are achieved in the proposed optical data security system. This finding may advance single-pixel correlated imaging as a quantum or classical technology with potential for significantly enriching the security field.

References

[1] B. I. Erkmen and J. H. Shapiro, "Ghost imaging: From quantum to classical to computational," *Adv. Opt. Photon.*, vol. 2, pp. 405–450, 2010.
[2] 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, 2004, Art. ID 093602.
[3] 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.
[4] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," *Appl. Phys. Lett.*, vol. 101, 2012, Art. ID 101108.
[5] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York, NY, USA: McGraw-Hill, 1996.
[6] 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.
[7] B. Javidi, "Securing information with optical technologies," *Phys. Today*, vol. 50, pp. 27–32, 1997.

[8] W. Chen, G. Situ, and X. Chen, "High-flexibility optical encryption via aperture movement," *Opt. Exp.*, vol. 21, no. 21, pp. 24680–24691, Oct. 2013.
[9] O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.
[10] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.*, vol. 36, pp. 22–24, 2011.
[11] F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," *Opt. Exp.*, vol. 19, no. 6, pp. 5706–5712, Mar. 2011.
[12] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.*, vol. 38, no. 17, pp. 3198–3201, Sep. 2013.
[13] I. Mehra, S. K. Rajput, and N. K. Nishchal, "Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification," *Opt. Eng.*, vol. 52, 2013, Art. ID 028202.
[14] Y. Shi *et al.,* "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, May 2013.
[15] T. Li and Y. Shi, "Security risk of diffractive-imaging-based optical cryptosystem," *Opt. Exp.*, vol. 23, no. 16, pp. 21384–21391, Aug. 2015.
[16] T. Li, Y. Wang, J. Zhang, and Y. Shi, "Analytic known-plaintext attack on a phase-shifting interferometry-based cryptosystem," *Appl. Opt.*, vol. 54, no. 2, pp. 306–311, Jan. 2015.
[17] A. W. Lohmann and D. P. Paris, "Binary Fraunhofer holograms, generated by computer," *Appl. Opt.*, vol. 6, no. 10, pp. 1739–1748, Oct. 1967.
[18] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol. 33, pp. 2443–2445, 2008.
[19] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, pp. 120–155, 2014.
[20] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, Jun. 2000.
[21] F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, "Differential ghost imaging," *Phys. Rev. Lett.*, vol. 104, no. 25, Jun. 2010, Art. ID 253603.