Advances in optical security systems

Wen Chen,[1] Bahram Javidi,[2,*] and Xudong Chen[1]

[1]Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117583, Singapore

[2]Department of Electrical and Computer Engineering, University of Connecticut, 371 Fairfield Road, Storrs, Connecticut 06269, USA

*Corresponding author: bahram@engr.uconn.edu

Received January 2, 2014; revised March 19, 2014; accepted March 24, 2014; published April 17, 2014 (Doc. ID 203795)

Information security with optical means, such as double random phase encoding, has been investigated by various researchers. It has been demonstrated that optical technology possesses several unique characteristics for securing information compared with its electronic counterpart, such as many degrees of freedom. In this paper, we present a review of optical technologies for information security. Optical security systems are reviewed, and theoretical principles and implementation examples are presented to illustrate each optical security system. In addition, advantages and potential weaknesses of each optical security system are analyzed and discussed. It is expected that this review not only will provide a clear picture about current developments in optical security systems but also may shed some light on future developments. © 2014 Optical Society of America

OCIS codes: (060.4785) Optical security and encryption; (070.4560) Data processing by optical means; (100.4998) Pattern recognition, optical security and encryption; (110.1650) Coherence imaging; (110.1758) Computational imaging
http://dx.doi.org/10.1364/AOP.6.000120

1943-8206/14/020120-36$15/0$15.00 © OSA

Advances in optical security systems

Wen Chen, Bahram Javidi, and Xudong Chen

1. Introduction

The popularization of computers and the internet has led to much research effort in the field of information transmission and storage security. Many commonly used products, such as video and images, are widely protected with invisible content or marks, which allow the owners to prevent unauthorized distribution and use [1]. A number of encryption technologies are also in common use, such as secure communication channels for mobile phones or even electronic mail. Although the public may not be highly aware of the importance of information security, many activities in our society, such as identification and password settings, do remind us of the use of information security technologies. Due to the rapid development of modern technologies, various identity proofs are becoming necessary, such as for online transactions. Without protection of individual or company materials, huge losses or personal attacks could be inevitable [2]. Hence, many companies and government sectors have spent much money each year for the development of cryptography technologies [2]. In particular, the military sector always seeks to confuse attackers through varied and advanced encoding technologies, since storage or transmission of confidential materials can be directly related to national security. Although a huge number of cryptography infrastructures have been established, there is still a great demand from individuals, companies, and government sectors to develop novel and advanced encoding technologies.

Since double random phase encoding (DRPE) was developed by Réfrégier and Javidi [3], optical technologies have become increasingly important for securing information. Optical encryption has attracted much attention in recent years due to its marked characteristics, such as parallel processing and multidimensional capabilities [4–11]. Much research and investigation on optical encryption have been performed based on DRPE, and a number of optical encryption infrastructures [12–32] have been established over the past decades. The main objective of these recent developments is improving the flexibility, security, and implementation convenience of optical cryptosystems. Significant advantages of optical encryption are summarized as follows. (1) Optical instruments, such as spatial light modulators and lenses, have inherent natures of parallel processing. Optical hardware can process each pixel of an input image at the same time, but electronic counterparts usually need to sequentially process data [2]. (2) Optical encryption methods possess multiple-dimensional and multiple-parameter capabilities. Many optical parameters, such as wavelength, polarization, and phase, can be employed as security keys [1–11]. Hence, system variety and security can be effectively guaranteed. (3) Optical encryption will require researchers to possess multidisciplinary knowledge, such as optical signal processing, image processing, optical theories, and computer technologies. A huge number of optical systems can be designed for securing information, and one typical optical security system could consist of some particular optical devices, such as light sources, lenses, detectors, and spatial light modulators [2]. Hence, without *prior* knowledge, attackers would have to do tedious searches or studies before they could accomplish decoding.

In this paper, we present a review of optical technologies for securing information. Optical security systems are reviewed, and theoretical principles and implementation examples are presented to illustrate each optical security system. In addition, advantages and potential weaknesses of each optical security system are analyzed and discussed. It is expected that this review will not only provide a clear picture about current developments of optical security systems, but may also shed some light on future developments. This paper is organized as follows. In Sections 2 and 3, the earliest optical encryption method, i.e., double random phase encoding (DRPE), is introduced, and the latest developments, such as DRPE with photon counting, are also analyzed and discussed. In Section 4, optical encryption with coherent diffractive imaging is analyzed and discussed, and it is illustrated that coherent diffractive imaging can provide an effective alternative for optical encoding compared to the conventional holographic technique. In Section 5, phase-retrieval algorithms, i.e., 2D, 3D, and non-iterative, are introduced for optical image encryption, and significant advantages of phase-retrieval algorithms are illustrated. In Section 6, phase-truncated optical encoding is described, and it is illustrated that phase-truncated optical cryptosystems can endure some attacks. In Section 7, the latest development using sparse constraint is described, and it is demonstrated that an additional security layer can be established for optical security systems. Finally, the conclusions and perspectives are presented in Section 8.

2. Double Random Phase Encoding

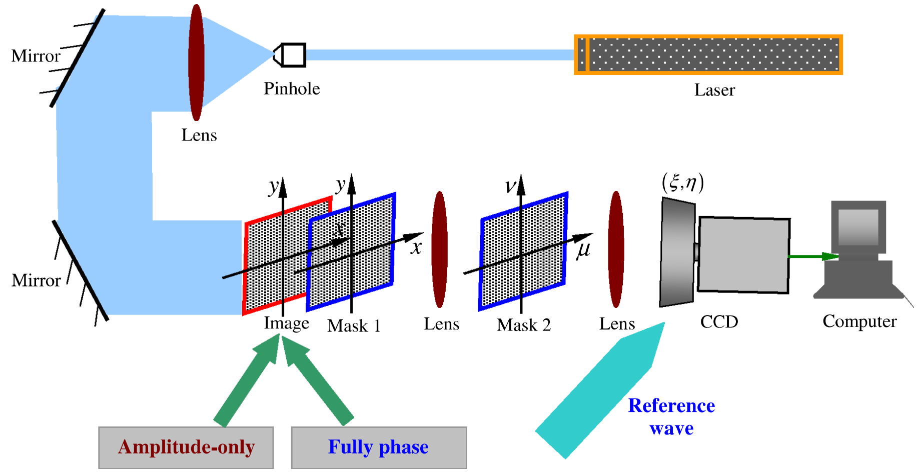
2.1. Amplitude-Only and Fully Phase Optical Encoding

DRPE [3] was the first optical security system, and it has been widely analyzed and studied. In a DRPE system, the input image can be converted into stationary white noise by using two statistically independent random phase-only masks respectively placed in the input image plane and the Fourier domain, as shown in Fig. 1. The random phase-only mask in the input image plane makes the signal white but nonstationary, and the random phase-only mask in the Fourier plane maintains whiteness but makes it stationary with signal encryption. It is also possible to show that the encrypted data are stationary white noise by using an autocorrelation function [3]. Let $\exp[j\phi(x,y)]$ and $\exp[j\varphi(\mu,\nu)]$ denote phase-only masks M1 and M2, respectively, located in the input image plane and the Fourier domain, where $j=\sqrt{-1}$, and $\phi(x,y)$ and $\varphi(\mu,\nu)$ denote 2D maps randomly distributed in the range of $[0,2\pi]$. Here, symbols (x,y) and (μ,ν) are used to denote the coordinates of the input image plane and the Fourier plane, respectively. The complex-valued wavefront just before phase-only mask M2 can be described by

$$H(\mu,\nu)=\mathrm{FT}\{P(x,y)\exp[j\phi(x,y)]\}, \tag{1}$$

where $P(x,y)$ denotes an input image (such as a non-negative gray-scale image), and FT denotes Fourier transform. The optical wavefront $H(\mu,\nu)$ is modulated by phase-only mask M2 in the Fourier domain, and, subsequently, inverse Fourier transform is conducted:

Figure 1



Schematic setup for DRPE in the Fourier domain.

$$O(\xi,\eta) = \mathrm{IFT}\{H(\mu,\nu)\exp[j\varphi(\mu,\nu)]\}, \tag{2}$$

where $O(\xi,\eta)$ denotes the complex-valued wavefront in the CCD plane, and IFT denotes inverse Fourier transform. Since no devices can directly record complex-valued information like $O(\xi,\eta)$, a CCD camera is usually used to record intensity patterns.

Some optical technologies, such as phase-shifting and off-axis digital holography [33–35], can be employed during the encoding in practical applications, so the complex-valued wavefront can be correspondingly extracted from the recorded intensity patterns. Let $\hat{O}(\xi,\eta)$ denote the complex-valued wavefront extracted in the CCD plane. During decoding, the extracted wavefront $\hat{O}(\xi,\eta)$ is Fourier transformed to the phase-only mask (M2) plane and the conjugate of phase-only mask M2 is modulated as follows:

$$\hat{H}(\mu,\nu) = \{\mathrm{FT}[\hat{O}(\xi,\eta)]\}\{\exp[j\varphi(\mu,\nu)]\}^*, \tag{3}$$

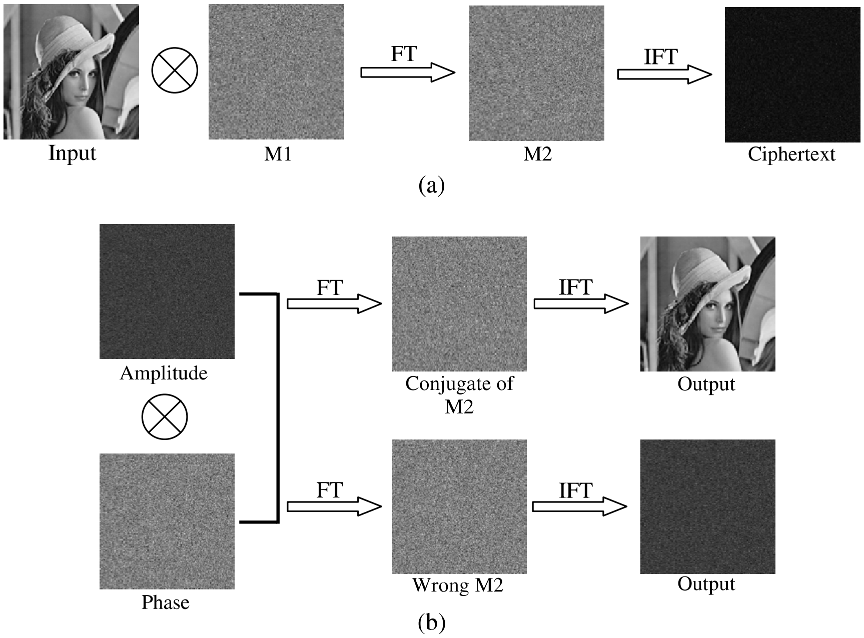
where the asterisk denotes complex conjugate. Subsequently, the generated wavefront $\hat{H}(\mu,\nu)$ is inverse Fourier transformed to the input image plane for extracting the plaintext:

$$S(x,y) = \{\mathrm{IFT}[\hat{H}(\mu,\nu)]\}\{\exp[j\phi(x,y)]\}^*, \tag{4}$$

where $S(x,y)$ denotes the decoded wavefront in the input image plane.

It can be seen in Eq. (4) that when the input image is a non-negative amplitude-only map, phase-only mask M1 can be omitted during decryption. One example is given to illustrate performance of the DRPE system. Figure 2(a) shows optical encoding based on the DRPE system, when an amplitude-only input image is encoded. The input image (selected from the USC-SIPI database: http://sipi.usc.edu/database/database.php?volume=misc) is effectively converted into a noise-like intensity distribution, and no information about the input image can be observed after the encoding. During decryption, the complex-valued wavefront in the CCD plane is first extracted according to the recording principles, such as holography. For simplicity, the wavefront $O(\xi,\eta)$ could be directly applied for

Figure 2



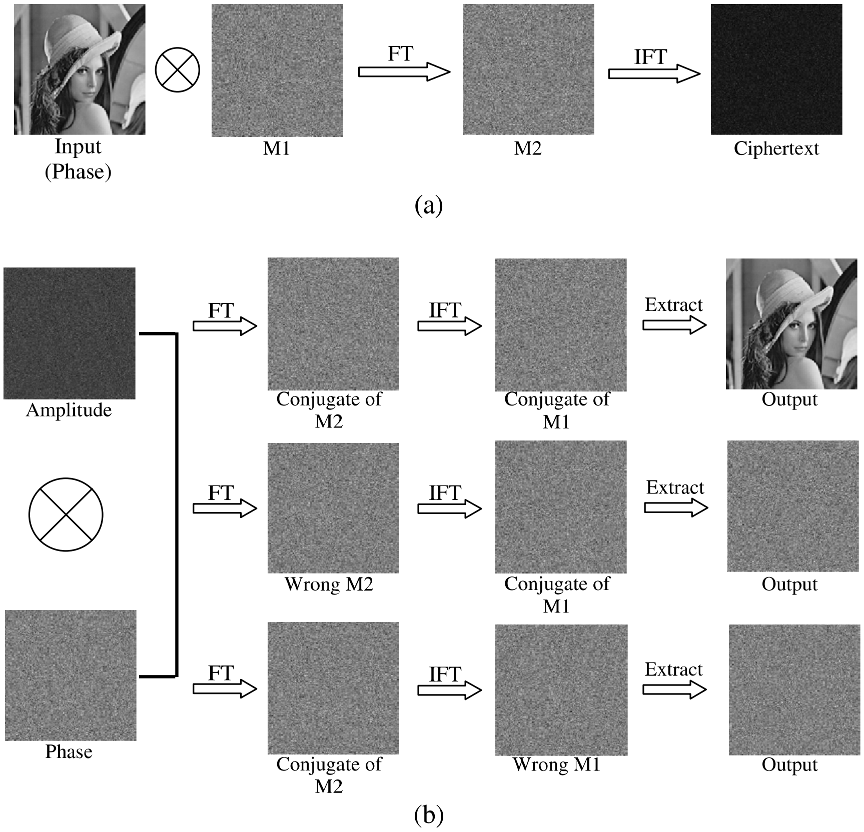
Amplitude-only DRPE: (a) encoding process and (b) decoding process.

decryption, such as in numerical examples. Figure 2(b) shows the optical decryption process. Since phase-only mask M2 can act as a security key during decryption, image decryption with the wrong phase-only mask M2 has also been illustrated in Fig. 2(b). It can be seen in Fig. 2(b) that when DRPE is implemented in the Fourier domain, the key space is relatively limited. Hence, a number of optical security systems [4–32] have been further developed based on the earliest DRPE strategy for improving system performance.

One of the most straightforward methods is to convert the input image into a fully phase map [36], and then this phase-only map is encoded based on the DRPE system. The encoding process is similar to those described for encoding amplitude-only input images, and the only difference is that the input image (such as a gray-scale image) is first normalized and converted into $\exp[jP(x,y)]$ before the encoding. In addition to phase-only mask M2, phase-only mask M1 is also considered a security key that effectively enlarges the key space of the DRPE system. Phase-only mask M1 should be applied during image decryption; otherwise, only noise-like distribution is generated. After the phase-only image is decoded, many optical technologies, such as interferometry, can be applied to extract the plaintext. Figures 3(a) and 3(b) show optical encoding and decoding processes based on fully phase DRPE, respectively. It is illustrated in Fig. 3(b) that phase-only mask M1 also plays an important role during decoding, and the larger key space is generated by using fully phase DRPE compared with amplitude-only DRPE.

Since the DRPE system was developed, attack algorithms have also been studied to illustrate DRPE vulnerability. Known-plaintext attacks, chosen-plaintext attacks, and chosen-ciphertext attacks [37,38] have been correspondingly applied to analyze the vulnerability. It is usually assumed in attack algorithms that some keys, such as the positions of phase-only masks, are known parameters. In

Figure 3



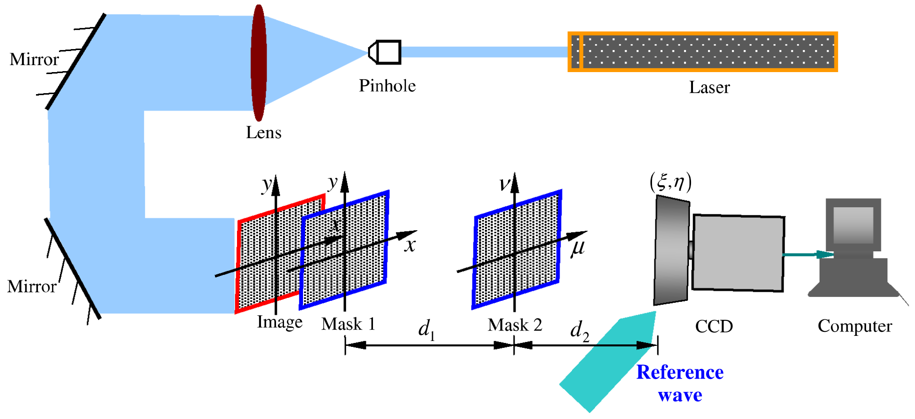
Fully phase DRPE: (a) encoding process and (b) decoding process.

addition, it is also assumed that the same phase-only masks M1 and M2 are used for encoding different input images [37]. For instance, in a known-plaintext attack [37], an iterative phase-retrieval algorithm is usually applied to extract the phase-only mask in the spatial domain at first, and then the second pair of known-plaintext and ciphertext is used to extract the phase-only mask in the Fourier domain. In a chosen-plaintext attack, impulse signals are usually assumed as the plaintexts to first extract the phase-only mask in the spatial domain, and, subsequently, the phase-only mask in the Fourier (or Fresnel) domain can be extracted by using the second pair of known-plaintext and ciphertext. Although phase-only masks can be approximately extracted under the assumptions, a simple strategy, i.e., updated phase-only masks for each input image, can fully endure these attacks [39]. In addition, many complementary algorithms [40–47], such as pixel scrambling algorithms [43–45], can also be applied to enhance the security of a DRPE system. Hence, it is believed that DRPE is highly suitable for securing information in most applications.

2.2. Lensless Optical Encryption in the Fresnel Domain

As illustrated in Section 2.1, the key space of a DRPE system is mainly dependent on phase-only masks. In practice, different transform domains [18,19,29,48–50], such as the Fresnel domain [18] and the fractional Fourier transform domain [29], can be integrated into a DRPE system, and additional security keys can be correspondingly generated. Here, we illustrate one of these

Figure 4



Schematic setup for DRPE in the Fresnel domain.

studies in which Fresnel transform is applied in a DRPE system [18]. Optical encoding and decoding processes in the Fresnel domain are similar to those described in Section 2.1; however, lenses used in Fourier-based DRPE are removed in Fresnel-transform-based DRPE, as shown in Fig. 4. The optical encoding process can be described by

$$O(\xi,\eta) = \mathrm{FrT}_{d_2,\lambda}\{(\mathrm{FrT}_{d_1,\lambda}\{P(x,y)\exp[j\phi(x,y)]\})\exp[j\varphi(\mu,\nu)]\}, \tag{5}$$

where FrT denotes wave propagation in the Fresnel domain, which can be described by diffraction theory [51,52], λ denotes the light wavelength, and d_1 and d_2 are axial distances. It can be seen in Eq. (5) that geometrical parameters, such as axial distances and wavelength, are also used as security keys. Optical technologies, such as holography [33–35], can also be applied to record intensity patterns, and complex-valued wavefront $\hat{O}(\xi,\eta)$ can be extracted in the CCD plane during decryption. Subsequently, it is straightforward to conduct image decryption, which can be described by

$$S(x,y) = [\mathrm{FrT}_{-d_1,\lambda}(\{\mathrm{FrT}_{-d_2,\lambda}[\hat{O}(\xi,\eta)]\}\{\exp[j\varphi(\mu,\nu)]\}^*)]\{\exp[j\phi(x,y)]\}^*, \tag{6}$$

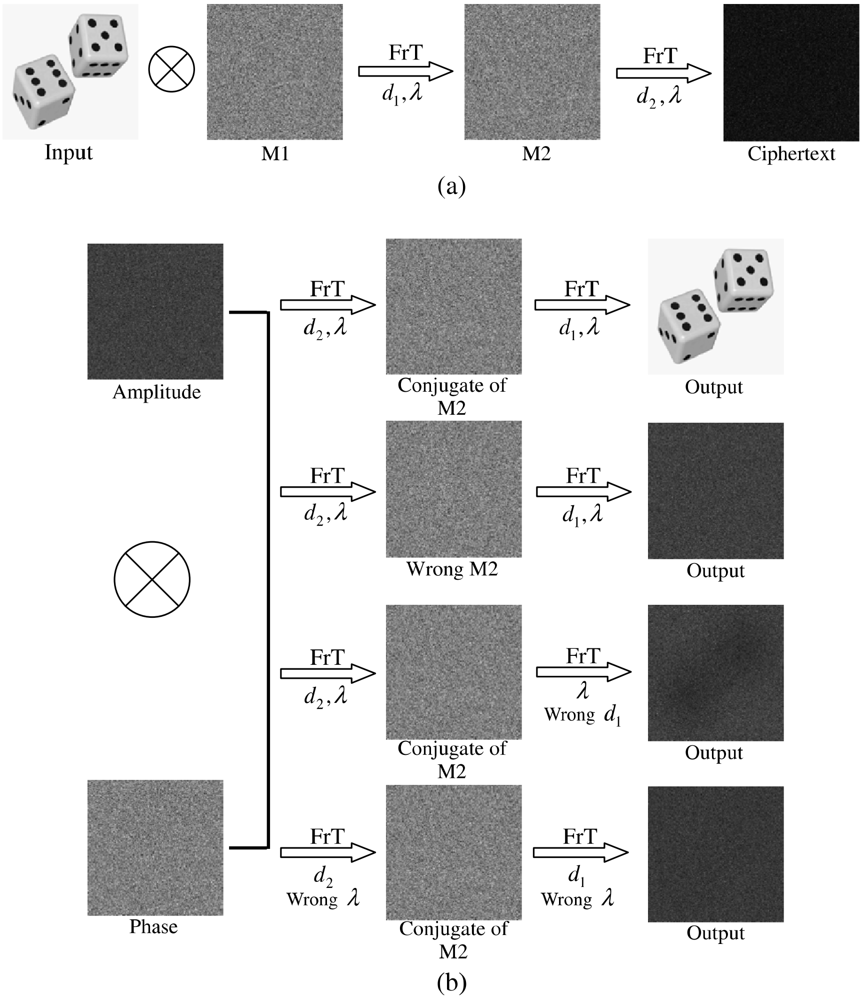
where $\mathrm{FrT}_{-d_1,\lambda}$ and $\mathrm{FrT}_{-d_2,\lambda}$ denote inverse Fresnel transform. When amplitude-only input image is encoded, phase-only mask M1 can be omitted during image decryption.

Figure 5(a) shows the optical encoding process that uses DRPE in the Fresnel domain, and Fig. 5(b) shows the corresponding optical decoding process. In this case, an amplitude-only input image is encoded. It can be seen in Fig. 5(b) that, in addition to a phase-only mask, wavelength and axial distances are also used as security keys. Without accurate information about geometrical parameters, plaintext information cannot be extracted. Compared with Fourier-based DRPE, DRPE in the Fresnel domain possesses a larger key space.

2.3. Multidimensional Random Phase Encoding

There are various degrees of freedom that can be used to improve the security of DRPE systems. In this section, we discuss how these degrees of freedom can be used in the optical encoding process to improve system performance. One

Figure 5



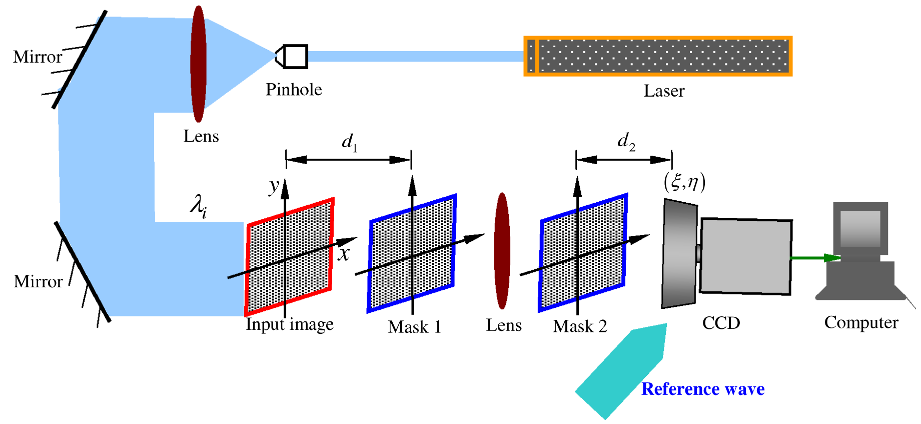
DRPE in the Fresnel domain: (a) encoding process and (b) decoding process.

potential degree of freedom to be employed is by varying the 3D positions of random phase-only masks in DRPE as developed by Matoba and Javidi [18]. For example, random phase-only masks can be located in the Fresnel domain [18], as shown in Fig. 6. Different from Sections 2.1 and 2.2, phase-only mask M1 is not bonded with the input image.

When random phase-only masks are placed in the Fresnel domain, the 3D positions of phase-only masks also need to be searched by an attacker. Hence, this can provide an additional barrier against attacks, since both phase keys and their 3D locations need to be searched. Unless the keys are placed with precision in their respective 3D lateral and longitudinal positions, the correctly decrypted image cannot be generated.

Some researchers have proposed using optical keys in other domains, such as fractional Fourier transform [29,53]. However, the basic principle is mathematically similar to Fresnel transform, since random phase-only masks can be placed anywhere in the encoding system. In practice, optical implementation of fractional Fourier transform could be more complex than that using Fresnel transform.

Figure 6



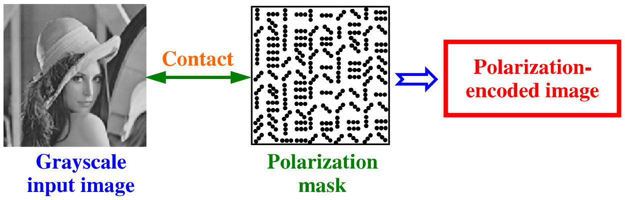
Schematic setup for optical encryption using multidimensional keys. Various degrees of freedom can be used to encrypt the data/image, and wavelength sensitivity can also be tested. Different from Sections 2.1 and 2.2, phase-only mask M1 is not bonded with the input image.

Polarization encoded keys can also be employed for enhancing the dimensionality and complexity of optical keys [7,8,54], and a schematic illustration [41] is shown in Fig. 7. In polarimetric encoding, the input image to be encoded is bonded with a polarization encoded mask. The polarimetric mask consists of randomly oriented linear polarizer rotated at various angles from 0 to 180 deg. In addition to random phase-only masks, the presence of randomly varying polarization provides an additional degree of freedom for securing information. The polarization-encoded information cannot be detected by using an intensity-sensitive device (such as a CCD camera), and a special sensor is required to measure various polarization states that are encoded into the input image.

3. Double Random Phase Encoding with Photon Counting

Recently, it has been illustrated that a photon-counting imaging approach can be integrated into an optical encryption system, especially for information authentication [55–57]. The motivation is that the combination of photon counting imaging and DRPE can generate an additional security layer against attacks. A photon-limited encrypted image is sparse compared with conventional

Figure 7



Schematic illustration of polarization encoding in an optical security system.

encrypted data. When the sparse encrypted data are used for decoding, only noisy signals will be produced. Unlike conventional optical decryption, when photon counting is used, the decrypted image is not recognizable by visual inspection. Instead, verification of the decrypted data should be further performed by means of image correlation.

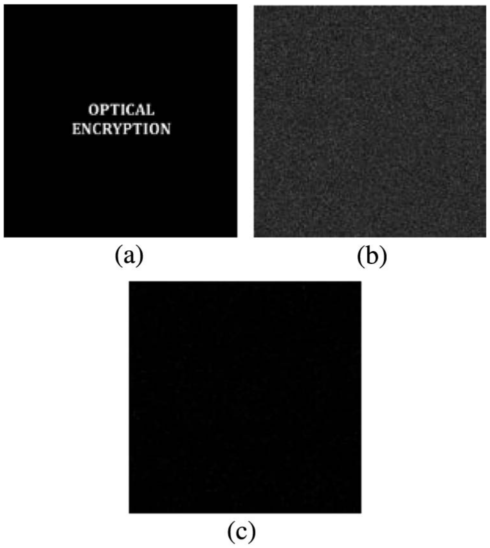
In photon-counting imaging [58], the scene has a limited number of photons. The expected number of photons (counts) in the scene is denoted as N_p. The probability of counting l_j photons at pixel x_j is shown to be Poisson distributed [55,56,58]:

$$P_d(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j!}, \qquad l_j = 0, 1, 2\ldots, \tag{7}$$

where l_j denotes the number of photons detected at pixel x_j. Poisson parameter λ_j is calculated by $\lambda_j = N_p g(x_j)$, with $g(x_j)$ being the normalized irradiance at pixel x_j such that $\sum_{j=1}^{M} g(x_j) = 1$, and M denotes the total number of pixels.

One example [55] is given to illustrate the performance of photon-counting optical encoding. Figure 8(a) shows the input image, and Fig. 8(b) shows the amplitude component of the encrypted image (without photon counting) obtained by using DRPE. Figure 8(c) shows the magnitude of the photon-counting encrypted image corresponding to Fig. 8(b). Here, the total number of photons is $N_p = 10^3$. Figure 9(a) shows the photon-counting decrypted image obtained from the encrypted data in Fig. 8(c) using the correct keys. The input image in Fig. 8(a) cannot be recognized in the decrypted image [see Fig. 9(a)]. To authenticate the photon-counting decrypted image, we can correlate it with the input image by using a kth-law nonlinear correlator [55–57,59], and the verification result is shown in Fig. 9(b) [55]. It can be seen in Figs. 9(a) and 9(b) that the decrypted image does not visually render any plaintext information;

Figure 8

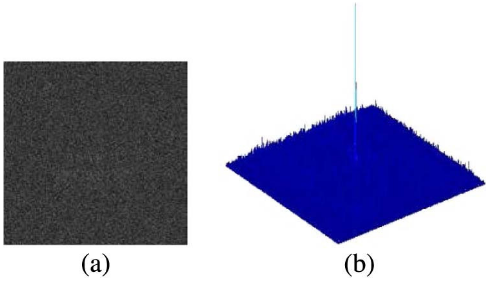


(a) (b)

(c)

(a) Input image to be encrypted, (b) amplitude of the encrypted data, and (c) photon-counting encrypted data using the number of photons $N_p = 10^3$. Reprinted from [55].

Figure 9



(a) Decrypted image corresponding to Fig. 8(c), and (b) correlation output using a kth-law nonlinear correlator with $k = 0.30$. Reprinted from [55].

however, information verification can be further conducted. Compared with conventional DRPE, photon-counting DRPE can provide an additional security layer without direct observation of input images.

4. Coherent Diffractive Imaging for Optical Encryption

In Sections 2 and 3, interferometric technology, such as holography [33–35], is usually applied for optical image encryption. However, the interferometric method requires a relatively complex optical recording system, such as reference waves and temporal coherence. Recently, coherent diffractive imaging has been developed and successfully applied for optical image encryption [13,14,60–62]. Its advantages, such as simple optical setup and insensitivity to vibration, have been illustrated. In coherent diffractive imaging, only one single optical path is applied, and a reference wave is not required. A phase-retrieval algorithm is usually applied between real and reciprocal spaces during image decryption. We take optical image encryption based on diffractive imaging with axial translation of a CCD camera [60] as an example, but it is straightforward to apply other coherent diffractive imaging systems for optical image encryption. More related information can be found in Refs. [13,14,43,52,61,62].

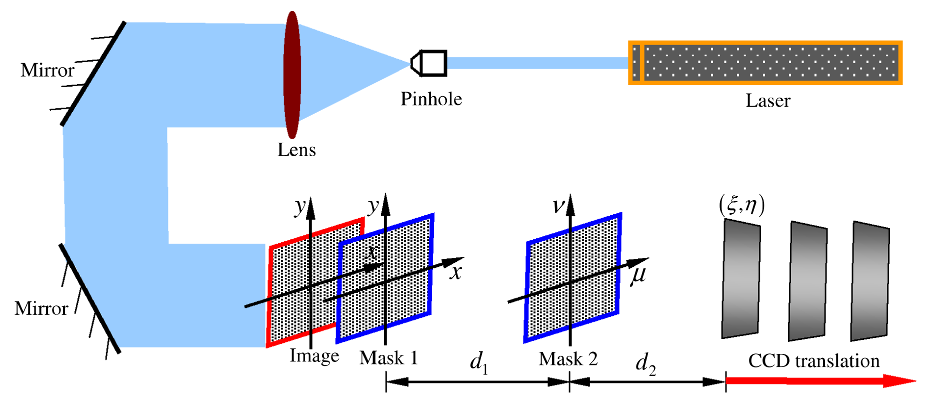
Figure 10 shows a schematic setup for optical image encryption using coherent diffractive imaging with axial translation of a CCD camera. The recorded diffraction intensity patterns (i.e., ciphertexts) can be described by

$$I^{(h)}(\xi,\eta) = |\mathrm{FrT}_{d_2+\Delta d\times(h-1)}\{(\mathrm{FrT}_{d_1}\{P(x,y)\exp[j\phi(x,y)]\})\exp[j\varphi(\mu,\nu)]\}|^2, \quad (8)$$

where $I^{(h)}(\xi,\eta)(h = 1,2,3)$ denotes the recorded diffraction intensity patterns, d_1 and d_2 denote axial distances, and Δd denotes the CCD camera translation amount. In coherent diffractive imaging, the recordings are conducted based on single-path wave diffraction, which is different from holographic-based encoding approaches [33–35].

An iterative phase-retrieval algorithm is developed for plaintext recovery during the decryption. We take three diffraction intensity recordings as examples for illustrating the principles of coherent diffractive imaging. Let $P^{(n)}(x,y)$ $(n = 1)$ denote the estimated plaintext in the initial iteration, and it is randomly distributed in the range of $[0, 2\pi]$. The iterative phase-retrieval algorithm consists of following steps.

Figure 10



Schematic setup for diffractive-imaging-based optical encoding.

(1) Wave propagation between the input image plane and the CCD plane is implemented:

$$O^{(n)}(\xi,\eta)=\mathrm{FrT}_{d_2+\Delta d\times(h-1)}\{(\mathrm{FrT}_{d_1}\{P^{(n)}(x,y)\exp[j\phi(x,y)]\})\exp[j\varphi(\mu,\nu)]\}, \tag{9}$$

where n and h are set as 1 in the initial step.

(2) The constraint with corresponding ciphertext $I^{(h)}(\xi,\eta)$ is applied to update the amplitude part of the wavefront $O^{(n)}(\xi,\eta)$:

$$\hat{O}^{(n)}(\xi,\eta)=\sqrt{I^{(h)}(\xi,\eta)}[O^{(n)}(\xi,\eta)/|O^{(n)}(\xi,\eta)|]. \tag{10}$$

(3) After the complex-valued wavefront is updated in the CCD plane, wave back-propagation is conducted between the CCD plane and the input image plane:

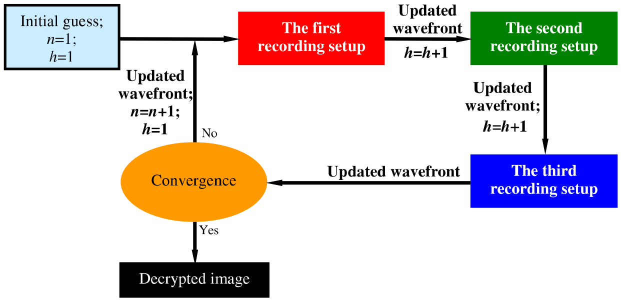
$$\begin{aligned}\hat{P}^{(n)}(x,y)=&[\mathrm{FrT}_{-d_1}(\{\mathrm{FrT}_{-[d_2+\Delta d\times(h-1)]}[\hat{O}^{(n)}(\xi,\eta)]\}\\&\times\{\exp[j\varphi(\mu,\nu)]\}^*)]\{\exp[j\phi(x,y)]\}^*,\end{aligned} \tag{11}$$

where $\hat{P}^{(n)}(x,y)$ denotes the updated complex-valued wavefront related to the plaintext. Subsequently, the amplitude part of the updated wavefront $\hat{P}^{(n)}(x,y)$ is used as a new estimate for the plaintext, and the next ciphertext (i.e., $h=h+1$) and the next CCD position [i.e., $d_2+\Delta d\times(h-1)$] are applied until $h=3$. After all three recordings are processed, one iterative operation is completed and iterative errors (IEs) [13,14,43,52,61] are calculated to judge whether the iterative process should be stopped:

$$\mathrm{IE}=\sum_{x,y}[|\hat{P}^{(n)}(x,y)|-|\hat{P}^{(n-1)}(x,y)|]^2. \tag{12}$$

If the iterative error is still larger than the preset threshold, the amplitude part of the updated complex amplitude $\hat{P}^{(n)}(x,y)$ is further used as a new guess for the next iteration (i.e., $n=n+1$), and parameter h is reset as 1. In coherent diffractive imaging with CCD translation, other decoding methods, such as transport of intensity [63,64], might also be developed and applied for plaintext recovery. In practice, simplified decryption methods, including even those with a single diffraction pattern, may be further designed and applied for image decoding.

Figure 11

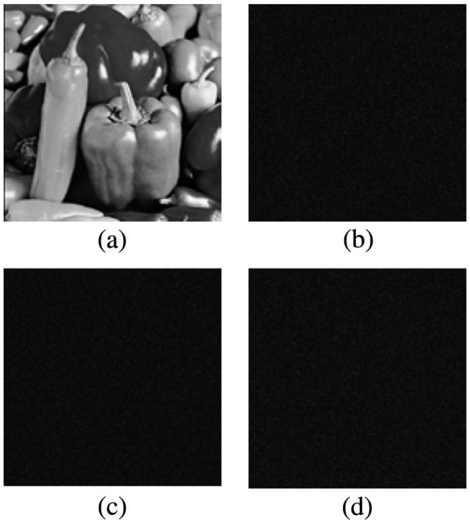


Flow chart for image decryption in a diffractive-imaging-based optical security system.

However, when there are some distortions in the ciphertexts (such as occlusions and noise), it is much better that multiple recordings be implemented and applied to guarantee algorithm convergence during decoding. To clearly illustrate the decryption process aforementioned, a flow chart is shown in Fig. 11.

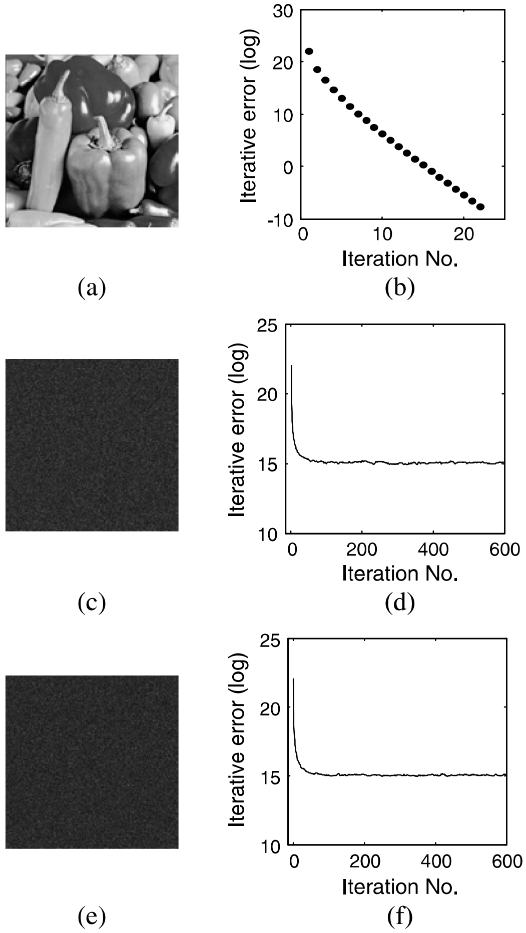
Figure 12(a) shows one gray-scale image that is encoded based on coherent diffractive imaging with axial translation of the CCD camera, and Figs. 12(b)–12(d) show three recorded diffraction intensity patterns (i.e., ciphertexts). It can be seen in Figs. 12(b)–12(d) that the input image has been fully encoded, and no plaintext information can be observed. Figures 13(a)–13(f) show some decryption results, when correct or wrong security keys are used during image decryption. In coherent diffractive imaging, both phase-only masks and geometrical parameters are used as security keys. Compared with holographic-based optical encoding systems, it possesses several advantages as follows. (1) Coherent diffractive imaging could be considered a wavefront-modification or phase-diversity approach, and various strategies can be developed for recording multiple ciphertexts. This flexibility or variety is highly desirable for establishing optical security systems. (2) Coherent diffractive imaging requires simple

Figure 12



Diffractive-imaging-based optical encoding: (a) an input image and (b)–(d) three diffraction intensity patterns (i.e., ciphertexts).

Figure 13



Diffractive-imaging-based optical encoding: (a) and (b) decryption using correct keys (22 iterations), (c) and (d) decryption using the wrong wavelength (600 iterations), and (e) and (f) decryption using the wrong phase-only mask (M2, 600 iterations).

optical setup, which can be easily implemented in practical applications. In addition, coherent diffractive imaging is not sensitive to environmental or mechanical vibrations. (3) The diffractive-imaging-based optical encryption can effectively endure attacks, since the complex-valued wavefront in the CCD plane may not be directly extracted in many diffractive imaging systems, such as a grating-modulated system [14]. However, one possible disadvantage is that a digital approach is preferred for image decryption, since an iterative phase-retrieval algorithm is usually employed.

5. Phase-Retrieval Algorithms for Optical Encryption

5.1. 2D Phase Retrieval for Optical Encryption

Different from holographic-based and diffractive-imaging-based methods, phase retrieval provides new insight for optical image encryption [65–71]. A digital approach is usually applied for embedding the input image into phase-only masks, and either a digital or optical approach can be employed for image decryption. The main objective of optical encoding is to find correct or approximate phase-only masks under the given constraints, such as the input image. Since phase-only masks can be embedded into spatial light modulators, easy and simple implementation of image decryption becomes possible. Compared with DRPE systems, a totally different encoding strategy is applied in a phase-retrieval-based optical security system.

Figure 14 shows a typical optical setup for a phase-retrieval-based encoding system. The input image is iteratively encrypted into two phase-only masks; however, it is straightforward to embed the input image into fewer or more cascaded phase-only masks. In the initial step, phase-only masks M1 and M2 should be initialized. Let $\exp[j\phi^{(n)}(\mu,\nu)]$ and $\exp[j\varphi^{(n)}(\xi,\eta)]$ $(n=1)$ denote phase-only masks M1 and M2, respectively. The collimated plane wave is generated for the illumination, and wave propagation between the phase-only mask (M1) plane and the image plane can be described by

$$O^{(n)}(x,y) = \mathrm{FrT}_{d_2}\{(\mathrm{FrT}_{d_1}\{\exp[j\phi^{(n)}(\mu,\nu)]\})\exp[j\varphi^{(n)}(\xi,\eta)]\}. \tag{13}$$

Subsequently, the square root of the input image is used as a constraint for the updating:

$$\hat{O}^{(n)}(x,y) = \sqrt{P(x,y)}O^{(n)}(x,y)/|O^{(n)}(x,y)|, \tag{14}$$

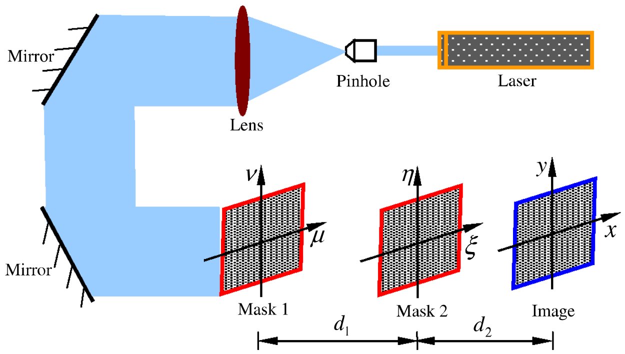
where $P(x,y)$ denotes the input image and $\hat{O}^{(n)}(x,y)$ denotes the complex-valued wavefront updated in the image plane. Finally, phase-only masks M2 and M1 can be respectively updated as [71]

$$\exp[j\hat{\varphi}^{(n)}(\xi,\eta)] = \left(\frac{\mathrm{FrT}_{-d_2}[\hat{O}^{(n)}(x,y)]}{\mathrm{FrT}_{d_1}\{\exp[j\phi^{(n)}(\mu,\nu)]\}}\right)\Bigg/\left|\frac{\mathrm{FrT}_{-d_2}[\hat{O}^{(n)}(x,y)]}{\mathrm{FrT}_{d_1}\{\exp[j\phi^{(n)}(\mu,\nu)]\}}\right|, \tag{15}$$

$$\exp[j\hat{\phi}^{(n)}(\mu,\nu)] = \frac{\mathrm{FrT}_{-d_1}(\{\mathrm{FrT}_{-d_2}[\hat{O}^{(n)}(x,y)]\}\{\exp[j\hat{\varphi}^{(n)}(\xi,\eta)]\}^{*})}{|\mathrm{FrT}_{-d_1}(\{\mathrm{FrT}_{-d_2}[\hat{O}^{(n)}(x,y)]\}\{\exp[j\hat{\varphi}^{(n)}(\xi,\eta)]\}^{*})|}. \tag{16}$$

The correlation coefficient between estimated and desired outputs is calculated to judge whether the iterative process should be stopped. When the correlation

Figure 14



Schematic setup for 2D-phase-retrieval-based optical encoding.

coefficient is smaller than the preset threshold, the updated phase-only masks $\exp[j\hat{\phi}^{(n)}(\mu,\nu)]$ and $\exp[j\hat{\varphi}^{(n)}(\xi,\eta)]$ are further used for the next iteration (i.e., $n = n + 1$). If the preset condition is satisfied, the updated phase-only masks are considered as masks M1 and M2, respectively. To some extent, the phase-retrieval algorithm used for optical encoding is similar to the principles of computer-generated holograms.

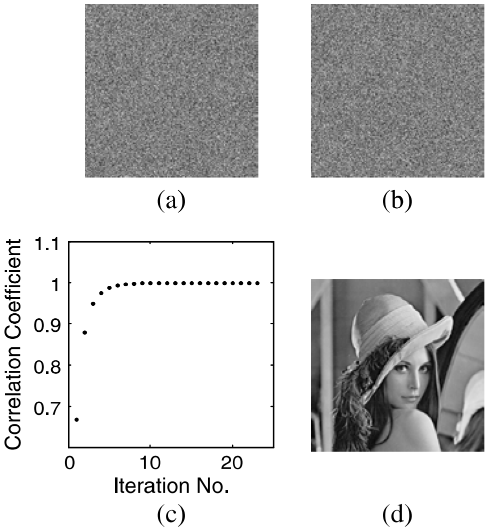
Either a digital or an optical approach can be applied for image decryption, and the collimated plane wave is generated for the illumination. The optical decryption process can be described by

$$\hat{P}(x,y) = |\mathrm{FrT}_{d_2}\{(\mathrm{FrT}_{d_1}\{\exp[j\hat{\phi}^{(n)}(\mu,\nu)]\})\exp[j\hat{\varphi}^{(n)}(\xi,\eta)]\}|^2, \tag{17}$$

where $\hat{P}(x,y)$ denotes the decrypted image. Evaluation parameters, such as mean square error and correlation coefficient [12,13,60], can be employed to evaluate the quality of decrypted images.

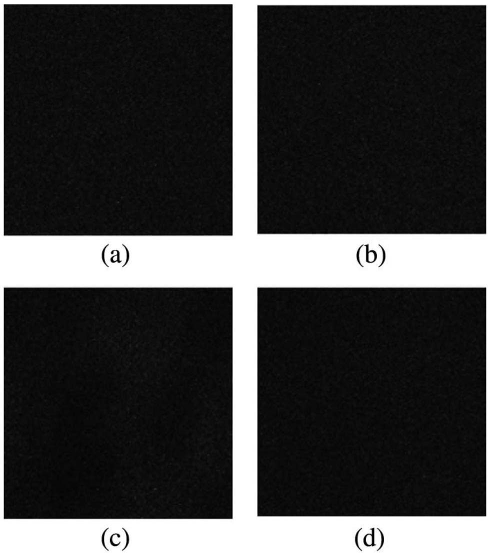
An example is presented to illustrate principles of phase-retrieval-based optical encryption. Figures 15(a) and 15(b) show the extracted phase-only masks M1 and M2, respectively. Figure 15(c) shows the iterative process using a phase-retrieval algorithm for optical encoding, and Fig. 15(d) shows the decrypted image obtained by using the correct security keys. It is illustrated that phase-only masks are effectively generated, and a rapid convergence rate can be achieved. When security keys or phase-only masks are wrong during decryption, no plaintext information can be extracted, as illustrated in Figs. 16(a)–16(d). Although a digital approach is usually employed for encoding the input image, it is convenient and simple to implement image decryption since only phase-only masks are requested. Different from holographic-based or diffractive-imaging-based optical encoding, a phase-retrieval-based optical security system generates phase-only masks as ciphertexts. Various transform domains, such as fractional

Figure 15



Extracted phase-only masks (a) M1 and (b) M2, (c) the iterative process by using a phase-retrieval algorithm for the encoding, and (d) decrypted image obtained by using correct security keys.

Figure 16



Decrypted images obtained by using (a) wrong phase-only mask M1, (b) wrong phase-only mask M2, (c) wrong distance d_2, and (d) wrong wavelength.

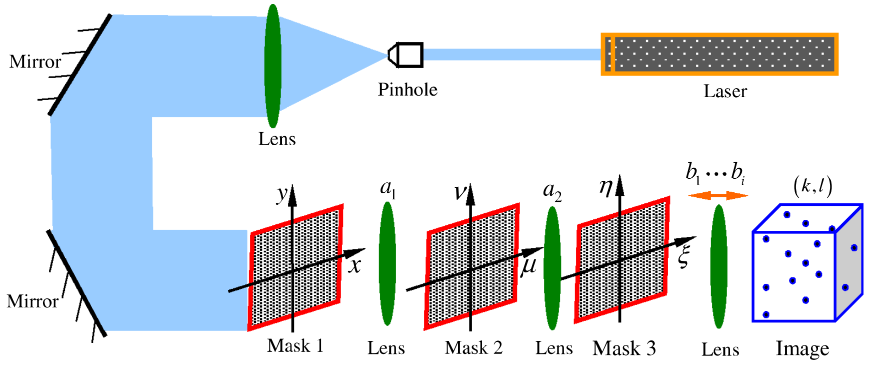
Fourier transform and gyrator transform [19,29,49], can also be integrated into the phase-retrieval-based optical encoding system.

5.2. 3D Phase Retrieval for Optical Encryption

Although phase retrieval can provide a new insight for optical image encryption, as illustrated in Section 5.1, phase-retrieval algorithms are usually limited to 2D applications. From a cryptanalysis point of view, higher security is always desirable for phase-retrieval-based optical cryptosystems. Hence, it can be worthwhile to extend 2D phase-retrieval-based optical security system into the 3D domain to enlarge key space and achieve higher security. Some studies on 3D phase-retrieval-based optical encoding have been presented in Refs. [72–74], and the main studies are focused on converting a 2D input image into 3D particle-like distribution. Since the input image is divided into a series of particles placed in 3D space, any sectional decryption will not render the plaintext information. This unique characteristic can enhance system security, since both the transverse and longitudinal positions of each particle should be available for extracting effective plaintext information.

Figure 17 shows one typical optical setup for 3D phase-retrieval-based optical encoding. As seen in Fig. 17, neighboring pixels (such as 16 × 16 pixels) of the 2D input image are combined as one particle, which is placed in one particular axial position. Here, we analyze the principles of 3D phase-retrieval-based optical encoding through embedding 3D particle-like distribution into three phase-only masks by using an iterative phase-retrieval algorithm, but it can be straightforward to encode 3D particle-like distribution into fewer or more phase-only masks in practical applications. During image encryption, masks M2 and M3 are the fixed phase-only maps, and the objective of the iterative phase-retrieval algorithm is to find accurate or approximate phase-only mask M1 under the given constraints, i.e., 3D particle-like distribution and phase-only masks M2 and M3. The encryption process is described as follows.

Figure 17



Schematic setup for 3D-phase-retrieval-based optical encoding.

(1) Wave propagation between the phase-only mask (M1) plane and the image plane is implemented:

$$O^{(i,n)}(k,l) = \mathrm{FrFT}_{b_i}\{(\mathrm{FrFT}_{a_2}\{(\mathrm{FrFT}_{a_1}\{\exp[j\phi^{(i,n)}(x,y)]\})\exp[j\varphi(\mu,\nu)]\}) \\ \times \exp[j\Re(\xi,\eta)]\}, \tag{18}$$

where particle index $i = 1, 2, \ldots,$ and n denotes the iterative number ($n = 1, 2, 3, \ldots$). Parameters n and i are set as 1 in the initial iteration.

(2) A constraint with original input image $P(k,l)$ is applied in the image plane:

$$\hat{O}^{(i,n)}(k,l) = \begin{cases} [2\Omega|P^{(i)}(k,l)| - |O^{(i,n)}(k,l)|] \times O^{(i,n)}(k,l)/|O^{(i,n)}(k,l)| & \text{if } (k,l) \in i \\ O^{(i,n)}(k,l) & \text{if } (k,l) \notin i \end{cases}. \tag{19}$$

(3) Wave backpropagation is implemented between the image plane and the phase-only mask (M1) plane:

$$O^{(i,n)}(x,y) = \mathrm{FrFT}_{-a_1}([\mathrm{FrFT}_{-a_2}(\{\mathrm{FrFT}_{-b_i}[\hat{O}^{(i,n)}(k,l)]\}\{\exp[j\Re(\xi,\eta)]\}^*)] \\ \times \{\exp[j\varphi(\mu,\nu)]\}^*), \tag{20}$$

(4) A constraint with unity amplitude is applied in the phase-only mask (M1) plane:

$$\exp[j\hat{\phi}^{(i,n)}(x,y)] = O^{(i,n)}(x,y)/|O^{(i,n)}(x,y)|, \tag{21}$$

where FrFT denotes fractional Fourier transform [29]; a_1, a_2, and b_i denote FrFT function orders, and symbol Ω denotes a ratio between summations of calculated output and original image within each signal window [72–74]. The updated phase-only mask M1 {i.e., $\exp[j\hat{\phi}^{(i,n)}(x,y)]$} is further applied for the next particle (i.e., $i = i + 1$), and Eqs. (18)–(21) are iteratively implemented for each particle until symbol i reaches the final particle. Once all particles are processed, one iterative process is completed. At this stage, iterative errors can be calculated to judge whether the iterative operation should be stopped. If the error is still larger than the preset threshold, the updated phase-only mask M1 will be further applied and Eqs. (18)–(21)

will sequentially continue for the next iteration (i.e., $n = n + 1$). Once a new iteration begins, particle index i should be reset as 1.

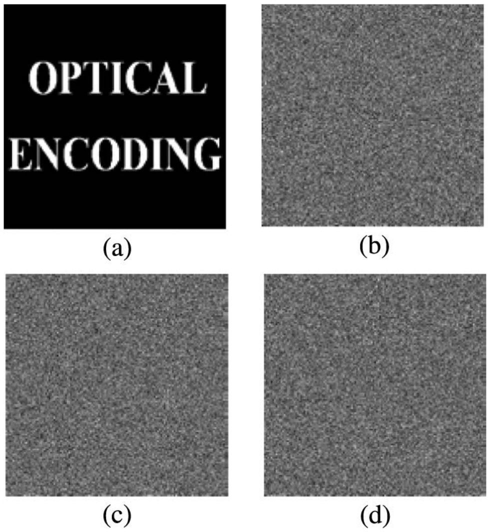
A collimated plane wave is generated for the illumination during image decryption, and each particle can be decoded by using accurate axial and transverse positions. Subsequently, all decoded particles are incorporated in the transverse domain as a decrypted image $\hat{P}(k,l)$. The decryption process aforementioned may be mathematically described by

$$\hat{P}(k,l) = \underset{i=1,2\ldots;(k,l)\in i}{\mathfrak{I}} \left| \mathrm{FrFT}_{b_i}\{(\mathrm{FrFT}_{a_2}\{(\mathrm{FrFT}_{a_1}\{\exp[j\hat{\phi}(x,y)]\})\exp[j\varphi(\mu,\nu)]\}) \right. \\ \left. \times \exp[j\mathfrak{R}(\xi,\eta)]\} \right|^2, \tag{22}$$

where $\exp[j\hat{\phi}(x,y)]$ denotes the finally extracted phase-only mask M1, and $\mathfrak{I}$ denotes an incorporating operation.

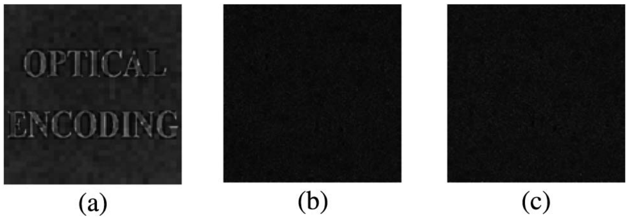
An example is given to illustrate the validity of a 3D phase-retrieval-based optical security system, and more related studies can be found in Refs. [72–74]. Figure 18(a) shows the input image, and Figs. 18(b)–18(d) show phase-only masks M1–M3, respectively. Phase-only mask M1 is extracted by using the aforementioned phase-retrieval algorithm, and phase-only masks M2 and M3 are fixed. It can be seen in Fig. 18 that the input image is fully encoded into the phase-only mask, and no plaintext information can be observed after the encoding. Figures 19(a)–19(c) show decryption results, when the correct keys are used or sectional decryptions are conducted. It can be seen in Figs. 19(b) and 19(c) that, compared with 2D phase-retrieval-based optical encoding, the 3D processing strategy can greatly enhance system security since any sectional decryption cannot render plaintext information. The key space is effectively enlarged, and the 3D phase-retrieval algorithm can enrich the application domains of optical encryption. However, since a cross-talk term is generated during

Figure 18



(a) Input image, (b) extracted phase-only mask M1, (c) phase-only mask M2, and (d) phase-only mask M3.

Figure 19



(a) Decrypted image obtained by using correct keys, and (b) and (c) decrypted images obtained at one sectional plane.

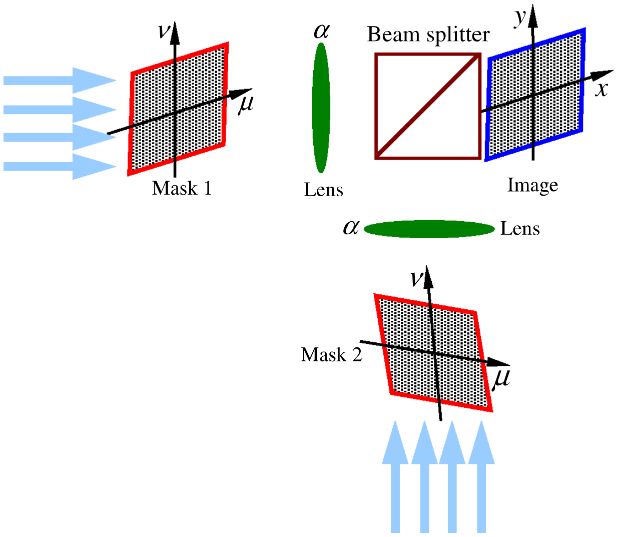
image decryption due to particle-like distribution, the quality of decrypted images can be affected. Hence, there is a trade-off between system security and quality of decrypted images [72–74].

5.3. Non-Iterative Phase Retrieval for Optical Encryption

Although a phase-retrieval algorithm can effectively embed the input image (2D or 3D) into phase-only masks, iterative operation is usually required, as illustrated in Sections 5.1 and 5.2. Recently, Zhang and Wang [75] proposed a non-iterative phase-retrieval algorithm based on interference principle for optical image encryption. A digital approach should be used to encrypt an input image into phase-only masks M1 and M2, as shown in Fig. 20, while either a digital or optical approach can be employed for image decryption. During the encryption, two complex-valued wavefronts interfere in the image plane:

$$\sqrt{P(x,y)}\ \exp[jR(x,y)] = \mathrm{FrFT}_\alpha\{\exp[j\phi(\mu,\nu)]\} + \mathrm{FrFT}_\alpha\{\exp[j\varphi(\mu,\nu)]\}, \quad (23)$$

Figure 20



Schematic setup for non-iterative interference-based optical encoding.

where $P(x, y)$ denotes the input image, $R(x, y)$ denotes 2D distribution randomly distributed in the range of $[0, 2\pi]$, and α denotes FrFT function order. Hence, phase-only masks M1 and M2 can be analytically extracted as [75–79]

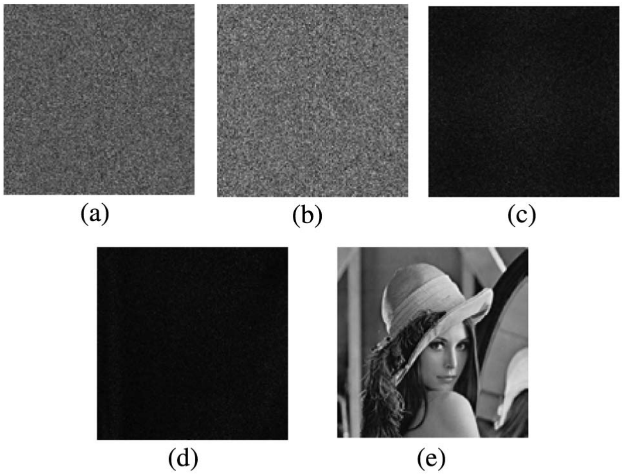
$$\begin{aligned}\phi(\mu,\nu) = {} & \mathrm{ang}\left(\mathrm{FrFT}_{-\alpha}\left\{\sqrt{P(x,y)}\,\exp[jR(x,y)]\right\}\right)\\ & - \arccos\left\{\left[\mathrm{abs}\left(\mathrm{FrFT}_{-\alpha}\left\{\sqrt{P(x,y)}\,\exp[jR(x,y)]\right\}\right)\right]/2\right\}, \end{aligned} \tag{24}$$

$$\varphi(\mu,\nu) = \mathrm{ang}\left(\mathrm{FrFT}_{-\alpha}\left\{\sqrt{P(x,y)}\,\exp[jR(x,y)]\right\} - \exp[j\phi(\mu,\nu)]\right), \tag{25}$$

where ang and abs denote the retrieval of the phase and magnitude parts, respectively.

During image decryption, the plane wave is generated for simultaneously illuminating the extracted phase-only masks M1 and M2, and the decrypted image can be obtained in the image plane by using a CCD camera. Figures 21(a)–21(e) show some encoding and decoding results based on the non-iterative phase-retrieval algorithm aforementioned. It can be seen in Figs. 21(a)–21(d) that the input image is fully encoded into phase-only masks, and phase-only masks and geometrical parameters play an important role during image decryption. Although iterative operation can be avoided, there is a silhouette problem in non-iterative phase-retrieval-based optical encryption [75]. A plaintext silhouette can be observed by using only one of the extracted phase-only masks, and cryptosystem security is limited. Recently, silhouette-removal and security-enhancement approaches [76–79], such as mask exchange and pixel scrambling, have been developed for non-iterative interference-based optical encoding.

Figure 21



Extracted phase-only masks (a) M1 and (b) M2, (c) decrypted image using wrong M1 and M2, (d) decrypted image using wrong FrFT function order, and (e) decrypted image using correct keys.

6. Phase-Truncated Strategy for Optical Encryption

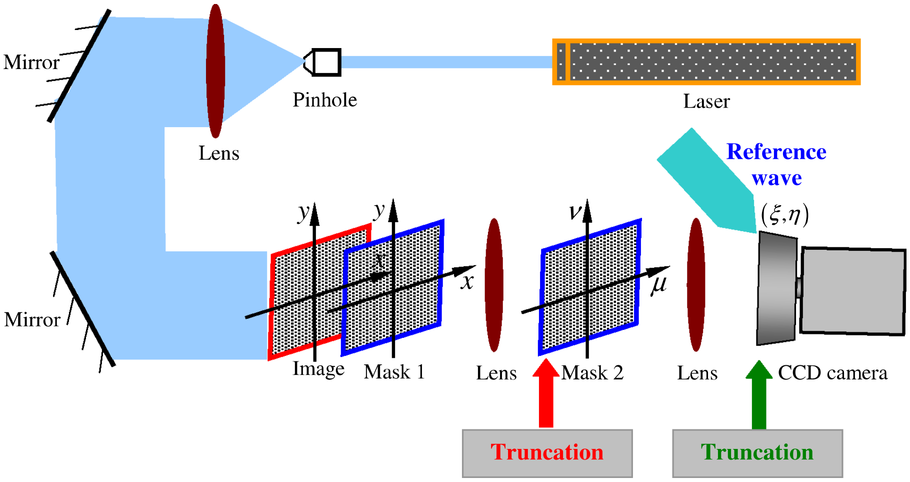
Although a number of optical security systems have been successfully applied, many optical cryptosystems are developed based on a linear strategy, and a system security may be compromised in some cases due to attacks, such as a known-plaintext attack [37,38]. Security enhancement methods are usually applied to endure attacks, and it is highly desirable that advanced strategies, such as decoding keys different from encoding keys, can be introduced into optical security systems. In recent years, several optical cryptosystems [80–82], such as phase-truncated optical encoding [81], have been developed, and decryption keys generated are different from encoding keys. The generated decryption keys could be directly related to the input image; hence attack algorithms cannot be applied to extract accurate or approximate security keys [81]. To some extent, these optical security systems cannot be claimed to be "asymmetric," since the pair of encryption and decryption keys are not independently generated by the recipient.

Here, we analyze one optical cryptosystem, i.e., phase-truncated optical encoding [81], for illustrating how different decryption keys can be generated. Figure 22 shows a schematic setup for a phase-truncated optical cryptosystem. Different from a DRPE system, phase truncation is conducted just before phase-only mask M2 and the CCD plane. Let $\exp[j\phi(x,y)]$ and $\exp[j\varphi(\mu,\nu)]$ denote phase-only masks M1 and M2, respectively located in the input image plane and Fourier domain. Wave propagation between the phase-only mask (M1) plane and the phase-only mask (M2) plane can be described by

$$W(\mu,\nu) = \mathrm{FT}\{P(x,y)\exp[j\phi(x,y)]\}, \tag{26}$$

where $P(x,y)$ denotes an input image. In a phase-truncated cryptosystem, the phase part of complex-valued wavefront is truncated, and only the amplitude part is further encoded. In the Fourier domain, amplitude and phase distributions can be respectively extracted as $A_w(\mu,\nu)$ and $P_w(\mu,\nu)$:

Figure 22



Schematic setup for phase-truncated optical encoding.

$$A_w(\mu,\nu) = |W(\mu,\nu)|, \tag{27}$$

$$P_w(\mu,\nu) = W(\mu,\nu)/|W(\mu,\nu)|. \tag{28}$$

Subsequently, wave propagation between the Fourier domain and the CCD plane is further conducted as

$$O(\xi,\eta) = \text{IFT}\{A_w(\mu,\nu)\exp[j\varphi(\mu,\nu)]\}. \tag{29}$$

Phase-truncated operation is also implemented in the CCD plane, and amplitude and phase distributions in the CCD plane can be respectively extracted as $A_o(\xi,\eta)$ and $P_o(\xi,\eta)$. $A_o(\xi,\eta)$ is considered as the ciphertext, and phase-only maps $P_w(\mu,\nu)$ and $P_o(\xi,\eta)$ are used as decryption keys that are different from encoding keys, i.e., phase-only masks M1 and M2.

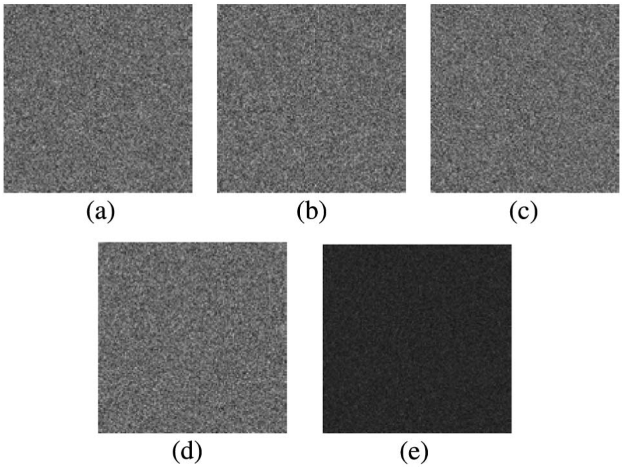
During image decryption, decryption keys should be employed to decode the ciphertext. The decryption process can be described by

$$\hat{P}(x,y) = |\text{IFT}\{|\text{FT}[A_o(\xi,\eta)P_o(\xi,\eta)]|P_w(\mu,\nu)\}|, \tag{30}$$

where $\hat{P}(x,y)$ denotes a decrypted image.

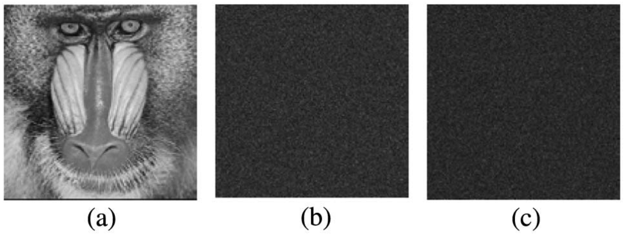
Figures 23(a)–23(e) show the encoding results based on a phase-truncated optical cryptosystem, and decryption keys are generated during the encoding that are different from phase-only masks M1 and M2. Figures 24(a)–24(c) show the decryption results when correct keys or wrong security keys are used during decryption, respectively. It can be seen in Fig. 24(b) that when encryption keys, i.e., phase-only masks M1 and M2, are used for decoding, no plaintext information can be extracted. Since decryption keys are directly related to the input image, different decryption keys can be correspondingly generated for different plaintexts. It is usually assumed in attack algorithms that the same decryption keys are available for decoding different input images. Hence, a phase-truncated optical cryptosystem can effectively endure these attacks due to its unique

Figure 23



(a) Phase-only mask M1, (b) phase-only mask M2, (c) decryption key $P_w(\mu,\nu)$, (d) decryption key $P_o(\xi,\eta)$, and (e) the ciphertext.

Figure 24



(a) Decrypted image obtained by using correct keys, (b) decrypted image obtained by using M1 and M2 for the decryption, and (c) decrypted image obtained by using wrong decryption key $P_w(\mu, \nu)$.

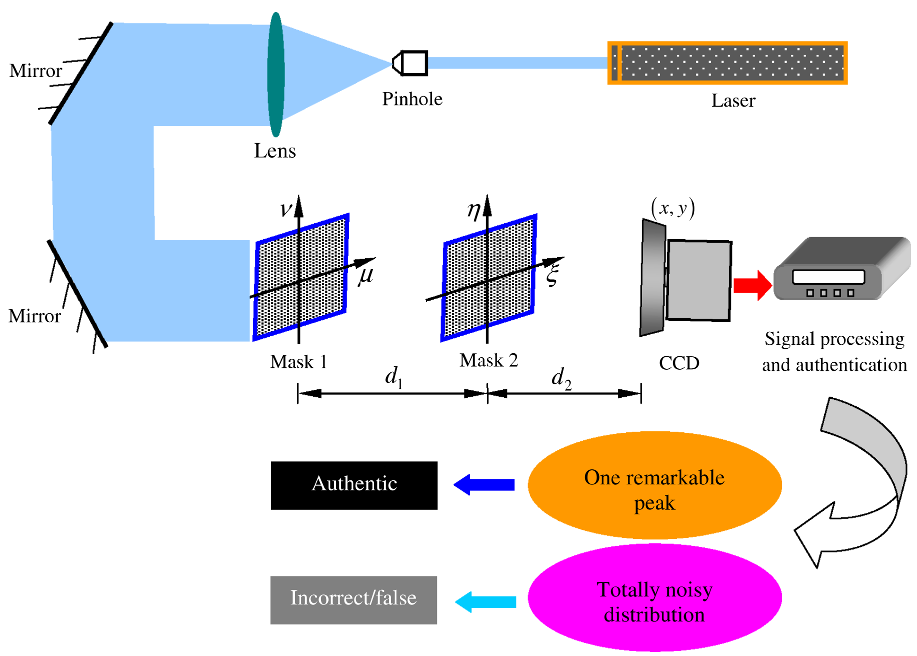
characteristics. However, since phase truncation should be conducted twice, experimental implementation can be relatively complicated compared with holographic-based or phase-retrieval-based optical security systems. Recently, it has been found [83] that a phase-retrieval-based collision algorithm can be applied to generate accurate or approximate ciphertext using different decryption keys. Hence, it is highly desirable that simple and effective approaches be further developed for enduring collision attacks in phase-truncated optical cryptosystems.

7. Sparsity-Driven Optical Information Authentication

It has been illustrated that when the same encryption keys are employed for different input images, optical cryptosystems could be vulnerable and attack algorithms may be applied to extract security keys. Particularly in long-term repeated applications, system deficiency could be more obvious. Hence, it is desirable that some new strategies be further developed for enhancing cryptosystem security. Recently, it has been found that when a sparsity constraint is used in optical security systems, decrypted images can be effectively authenticated without direct observation of plaintext information [71]. This new approach can be integrated into a number of existing optical security systems [84–91] (such as joint transform correlator architecture [88–91]), and can provide an additional security layer. Different from a photon-counting strategy [55,56], the encoding method with sparsity constraint can provide a different research perspective for optical security.

We analyze a 2D-phase-retrieval-based optical encoding and authentication system with sparse representation, as shown in Fig. 25, and it can be straightforward to apply the sparsifying principle to other optical security systems. The encoding process is similar to those described in Section 5.1, and the objective of phase retrieval is to find accurate or approximate phase-only masks M1 and M2. Let $\exp[j\hat{\phi}^{(n)}(\mu, \nu)]$ and $\exp[j\hat{\varphi}^{(n)}(\xi, \eta)]$, respectively, denote the extracted phase-only masks M1 and M2. In the optical encoding systems, there are many different ways to apply the sparsity strategy. For instance, we can use the sparse input image (such as only 2.0% of total pixels) during encoding and directly apply the generated phase-only masks $\exp[j\hat{\phi}^{(n)}(\mu, \nu)]$ and $\exp[j\hat{\varphi}^{(n)}(\xi, \eta)]$ during decryption. Alternatively, we can use the whole input image for encoding and apply sparse forms of the generated phase-only masks M1 and M2 for decryption [71].

Figure 25



Schematic setup for sparsity-driven optical information authentication.

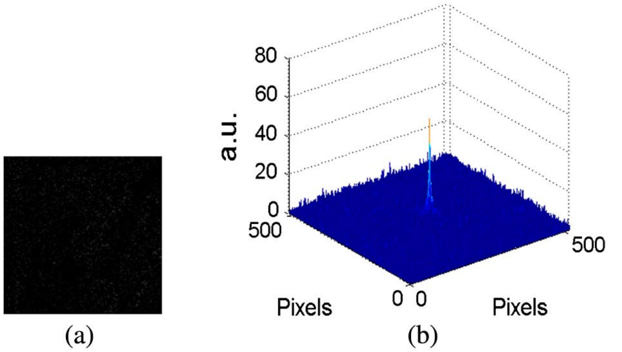
During decryption, a collimated plane wave is generated for illumination, and a decrypted image $\hat{P}(x, y)$ can be extracted by using a CCD camera. Since decrypted images contain invisible but useful plaintext information, an optical authentication method [11,55–57,71,92–98], such as nonlinear correlation [55–57,59,71,92], can be further applied to verify the decrypted images. The optical authentication method using nonlinear correlation can be described by

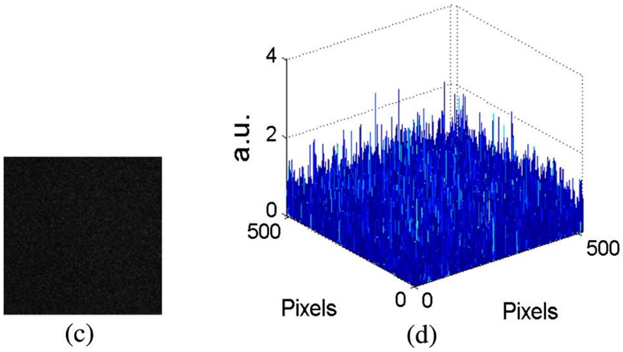
$$A(x, y) = \left| \mathrm{IFT}\left(|\{\mathrm{FT}[\hat{P}(x, y)]\}^* \{\mathrm{FT}[P(x, y)]\}|^t \frac{\{\mathrm{FT}[\hat{P}(x, y)]\}^* \{\mathrm{FT}[P(x, y)]\}}{|\{\mathrm{FT}[\hat{P}(x, y)]\}^* \{\mathrm{FT}[P(x, y)]\}|} \right) \right|^2, \tag{31}$$

where $A(x, y)$ denotes the authentication distribution and t denotes the strength of the applied nonlinearity [71,92–98]. Many complementary parameters, such as peak-to-correlation and discrimination ratios [55,56], can be further extracted from authentication distributions for evaluating correlation outputs.

We use a sparse input image (2.0% effect pixels of gray-scale image “Lena”) as one example to illustrate the principles of sparsity-driven optical information authentication. Figures 26(a)–26(d) show some decryption results when correct keys or the wrong wavelength are used during decryption and authentication. It can be seen in Figs. 26(a) and 26(c) that decrypted images do not directly render effective plaintext information. When correct keys are used for decryption, the decrypted image can be effectively authenticated and one remarkable peak can be observed. When the wrong security key is used, only noisy background is generated. In practical applications, the sparsifying level can be arbitrarily adjusted according to experimental setups and the plaintext. In an optical information authentication system, it is also important to test the discrimination capability. Another sparse input image (i.e., 2.0% effect pixels of gray-scale

Figure 26



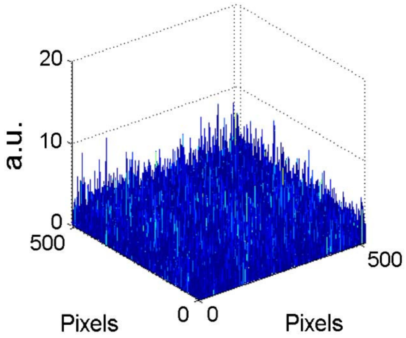


(a) Decrypted image obtained by using correct keys, (b) authentication result corresponding to (a), (c) decrypted image obtained by using wrong wavelength (error of 10.0 nm), and (d) authentication result corresponding to (c).

image "Peppers") is used in the optical security system. Figure 27 shows the authentication result when the decrypted image obtained by using correct keys is nonlinearly correlated with the original input image (i.e., "Lena"). It can be seen that discrimination capability can be guaranteed in sparsity-driven optical security systems. It is also illustrated that the sparsity strategy can be easily integrated into optical security systems, and can provide an additional security layer. More related works can be found in Refs. [55–57,71].

Table 1 clearly illustrates key features and possible drawbacks of the aforementioned optical security systems.

Figure 27



Similar image case: the authentication result.

Table 1. Brief Summary of Key Features and Possible Drawbacks of Various Optical Security Systems[a]

Type of Optical Security System	Key Features	Possible Drawbacks
Amplitude-only DRPE **Fully phase DRPE** **Lensless DRPE** **Multidimensional DRPE**	Effective; simple implementation (digital or optical); flexibly suited to various optical imaging systems; easy integration of security enhancement methods (such as mask updating); high variety; higher security in fully phase, lensless, and multidimensional	Security-enhancement approach probably required for enduring attacks; additional devices or setups requested for multidimensional DRPE
Photon-counting DRPE	Additional security layer without direct observation of input image; high capability against attacks	Application of specific devices
Diffractive-imaging-based optical encoding	Simple optical setup; insensitivity to vibration; no reference wave; high flexibility and variety; high capability against attacks	Phase-retrieval algorithms required during image decryption
2D/3D phase-retrieval-based optical encoding	Easy implementations with digital or optical approach; phase-only masks as ciphertexts; the enlarged key space in 3D case; flexible designs of encoding strategies	Relatively small key space in 2D case; cross-talk term in 3D case
Non-iterative phase-retrieval-based optical encoding	Non-iterative	Silhouette problem
Phase-truncated optical encoding	Nonlinear; decryption keys different from encoding keys; high capability against some attacks	Difficulty in experimental implementation; it cannot be used against the collision algorithm
Sparsity-driven optical information authentication	Additional security layer without direct observation of the plaintext; easy implementations; high flexibility and variety; high capability against attacks	Less ciphertext information

[a] Although possible drawbacks are described for each specific security system, some solutions or security-enhancement approaches may be correspondingly designed and applied in practice.

8. Conclusions and Perspectives

We have presented a review of optical technologies for securing information. Theoretical principles and implementation examples are given for illustrating each optical security system. Since there are a number of optical security systems for securing information, high flexibility and variety can be achieved. Significant advantages and potential weaknesses of each optical security system have also been analyzed and illustrated. It is expected that through these comparisons, a clear picture of current developments in optical security systems has been presented, and some light has been shed on future developments.

We believe that with rapid development of modern technologies, optical security systems can attract more and more attention in practical applications. In the future, it can be expected that the following aspects may be further stimulated and developed in the optical security field. (1) A number of optical security systems have been developed in recent years. When other related areas (such as materials and optical equipment) are developed, scientists and developers can collaborate to explore more applications related to optical security, such as in government and industry sectors. (2) Optoelectronic systems can be developed to optically encode and decode data in real time, and corresponding applications, such as face encryption and recognition, can be explored based on the developed optical security systems. It can be believed that electronic cryptography (such as watermarking [34,99]) can be more effectively integrated to enrich optical security systems, and intelligent algorithms, such as neural networks, can also be studied and applied. (3) In practice, easy implementations with high security, such as phase-retrieval algorithms, are highly desirable. When many digital processing approaches are applied in optical security systems, practical applications may not be feasible. Since spatial light modulators [100] have been rapidly developed, more studies related to phase-only encoding can be expected. In addition, how much capacity can be realized in phase-only encoding systems is also an interesting topic. (4) System security is always a big concern in the optical encryption field. Since a large number of optical security systems have been developed over the past decades, it is of interest that systematic work be further conducted to analyze the security of various optical encryption systems. Simultaneously, security-enhancement approaches can be correspondingly studied and suggested for each optical security system.

Acknowledgments

This work was supported by the Singapore Temasek Defence Systems Institute under grant TDSI/11–009/1A. Bahram Javidi acknowledges support under NSF NSF/CISE Award #CNS–1344271.

References

1. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding—a survey,” Proc. IEEE **87**, 1062–1078 (1999).
2. B. Javidi, “Securing information with optical technologies,” Phys. Today **50** (3), 27–32 (1997).
3. P. Réfrégier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. **20**, 767–769 (1995).

4. 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).
5. O. Matoba and B. Javidi, “Encrypted optical storage with wavelength-key and random phase codes,” Appl. Opt. **38**, 6785–6790 (1999).
6. O. Matoba and B. Javidi, “Encrypted optical memory systems based on multidimensional keys for secure data storage and communications,” IEEE Circuits Devices Mag. **16**(5), 8–15 (2000).
7. O. Matoba and B. Javidi, “Secure holographic memory by double-random polarization encryption,” Appl. Opt. **43**, 2915–2919 (2004).
8. B. Javidi and T. Nomura, “Polarization encoding for optical security systems,” Opt. Eng. **39**, 2439–2443 (2000).
9. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encrypted data by using polarized light,” Opt. Commun. **260**, 109–112 (2006).
10. X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi, “Secure optical storage that uses fully phase encryption,” Appl. Opt. **39**, 6689–6694 (2000).
11. B. Javidi and J. L. Horner, “Optical pattern recognition for validation and security verification,” Opt. Eng. **33**, 1752–1756 (1994).
12. W. Chen and X. Chen, “Space-based optical image encryption,” Opt. Express **18**, 27095–27104 (2010).
13. W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on diffractive imaging,” Opt. Lett. **35**, 3817–3819 (2010).
14. 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).
15. W. Chen and X. Chen, “Optical asymmetric cryptography using a three-dimensional space-based model,” J. Opt. **13**, 075404 (2011).
16. G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” Opt. Lett. **30**, 1306–1308 (2005).
17. G. Situ and J. Zhang, “Position multiplexing for multiple-image encryption,” J. Opt. A Pure Appl. Opt. **8**, 391–397 (2006).
18. O. Matoba and B. Javidi, “Encrypted optical memory system using three-dimensional keys in the Fresnel domain,” Opt. Lett. **24**, 762–764 (1999).
19. Z. Liu, L. Xu, C. Lin, and S. Liu, “Image encryption by encoding with a nonuniform optical beam in gyrator transform domains,” Appl. Opt. **49**, 5632–5637 (2010).
20. W. Liu, Z. Liu, and S. Liu, “Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm,” Opt. Lett. **38**, 1651–1653 (2013).
21. X. Wang, D. Zhao, F. Jing, and X. Wei, “Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics,” Opt. Express **14**, 1476–1486 (2006).
22. L. Chen and D. Zhao, “Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” Opt. Express **14**, 8552–8560 (2006).
23. 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).

24. Y. Rivenson, A. Stern, and B. Javidi, "Single exposure super-resolution compressive imaging by double phase encoding," Opt. Express **18**, 15094–15103 (2010).
25. F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," J. Opt. Soc. Am. A **15**, 2629–2638 (1998).
26. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915–1927 (1999).
27. T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A **25**, 2608–2617 (2008).
28. D. S. Monaghan, G. Situ, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Role of phase key in the double random phase encoding technique: an error analysis," Appl. Opt. **47**, 3808–3816 (2008).
29. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887–889 (2000).
30. N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun. **284**, 735–739 (2011).
31. E. Tajahuerce, J. Lancis, B. Javidi, and P. Andrés, "Optical security and encryption with totally incoherent light," Opt. Lett. **26**, 678–680 (2001).
32. M. He, Q. Tan, L. Cao, Q. He, and G. Jin, "Security enhanced optical encryption system by random phase key and permutation key," Opt. Express **17**, 22462–22473 (2009).
33. I. Yamaguchi and T. Zhang, "Phase-shifting digital holography," Opt. Lett. **22**, 1268–1270 (1997).
34. S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography," Opt. Lett. **28**, 167–169 (2003).
35. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. **25**, 28–30 (2000).
36. B. Javidi and A. Sergent, "Fully phase encoded key and biometrics for security verification," Opt. Eng. **36**, 935–942 (1997).
37. 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).
38. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. (Prentice Hall, 2006).
39. 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).
40. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**, 589–636 (2009).
41. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," Proc. IEEE **97**, 1128–1148 (2009).
42. S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt. Laser Technol. **57**, 327–342 (2014).
43. W. Chen and X. Chen, "Optical image encryption using multilevel Arnold transform and noninterferometric imaging," Opt. Eng. **50**, 117001 (2011).
44. W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on Arnold transform and interference method," Opt. Commun. **282**, 3680–3685 (2009).

45. B. Hennelly and J. T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” Opt. Lett. **28**, 269–271 (2003).
46. L. Chen and D. Zhao, “Optical image encryption with Hartley transforms,” Opt. Lett. **31**, 3438–3440 (2006).
47. P. Kumar, A. Kumar, J. Joseph, and K. Singh, “Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions,” Opt. Lett. **34**, 331–333 (2009).
48. Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, “Double image encryption by using iterative random binary encoding in gyrator domains,” Opt. Express **18**, 12033–12043 (2010).
49. J. A. Rodrigo, T. Alieva, and M. L. Calvo, “Gyrator transform: properties and applications,” Opt. Express **15**, 2190–2203 (2007).
50. W. Chen and X. Chen, “Quantitative phase retrieval of a complex-valued object using variable function orders in the fractional Fourier domain,” Opt. Express **18**, 13536–13541 (2010).
51. J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. (McGraw-Hill, 1996).
52. W. Chen and X. Chen, “Optical cryptography topology based on a three-dimensional particle-like distribution and diffractive imaging,” Opt. Express **19**, 9008–9019 (2011).
53. N. K. Nishchal, J. Joseph, and K. Singh, “Fully phase encryption using fractional Fourier transform,” Opt. Eng. **42**, 1583–1588 (2003).
54. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, “Secure optical memory system with polarization encryption,” Appl. Opt. **40**, 2310–2315 (2001).
55. E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” Opt. Lett. **36**, 22–24 (2011).
56. 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).
57. M. Cho and B. Javidi, “Three-dimensional photon counting double-random-phase encryption,” Opt. Lett. **38**, 3198–3201 (2013).
58. J. W. Goodman, *Statistical Optics* (Wiley, 2000).
59. B. Javidi, “Nonlinear joint power spectrum based optical correlation,” Appl. Opt. **28**, 2358–2367 (1989).
60. W. Chen, X. Chen, A. Anand, and B. Javidi, “Optical encryption using multiple intensity samplings in the axial domain,” J. Opt. Soc. Am. A **30**, 806–812 (2013).
61. W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on coherent diffractive imaging using multiple wavelengths,” Opt. Commun. **285**, 225–228 (2012).
62. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, “Optical image encryption via ptychography,” Opt. Lett. **38**, 1425–1427 (2013).
63. S. S. Gorthi and E. Schonbrun, “Phase imaging flow cytometry using a focus-stack collecting microscope,” Opt. Lett. **37**, 707–709 (2012).
64. L. Waller, L. Tian, and G. Barbastathis, “Transport of Intensity phase-amplitude imaging with higher order intensity derivatives,” Opt. Express **18**, 12552–12561 (2010).
65. R. W. Gerchberg and W. O. Saxton, “A practical algorithm for the determination of phase from image and diffraction plane pictures,” Optik **35**, 237–246 (1972).

66. J. R. Fienup, “Phase retrieval algorithms: a comparison,” Appl. Opt. **21**, 2758–2769 (1982).
67. R. K. Wang, I. A. Watson, and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng. **35**, 2464–2469 (1996).
68. Y. Li, K. Kreske, and J. Rosen, “Security and encryption optical systems based on a correlator with significant output images,” Appl. Opt. **39**, 5295–5301 (2000).
69. H. E. Hwang, H. T. Chang, and W. N. Lie, “Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain,” Opt. Lett. **34**, 3917–3919 (2009).
70. H. T. Chang, H. E. Hwang, C. L. Lee, and M. T. Lee, “Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain,” Appl. Opt. **50**, 710–716 (2011).
71. 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).
72. W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution,” J. Opt. **14**, 075402 (2012).
73. W. Chen and X. Chen, “Optical image encryption based on multiple-region plaintext and phase retrieval in three-dimensional space,” Opt. Lasers Eng. **51**, 128–133 (2013).
74. W. Chen and X. Chen, “Optical cryptography network topology based on 2D-to-3D conversion and phase-mask extraction,” Opt. Lasers Eng. **51**, 410–416 (2013).
75. Y. Zhang and B. Wang, “Optical image encryption based on interference,” Opt. Lett. **33**, 2443–2445 (2008).
76. Y. Zhang, B. Wang, and Z. Dong, “Enhancement of image hiding by exchanging two phase masks,” J. Opt. A Pure Appl. Opt. **11**, 125406 (2009).
77. B. Yang, Z. Liu, B. Wang, Y. Zhang, and S. Liu, “Optical stream-cipher-like system for image encryption based on Michelson interferometer,” Opt. Express **19**, 2634–2642 (2011).
78. P. Kumar, J. Joseph, and K. Singh, “Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator,” Appl. Opt. **50**, 1805–1811 (2011).
79. W. Chen and X. Chen, “Optical multiple-image encryption based on multiplane phase retrieval and interference,” J. Opt. **13**, 115401 (2011).
80. X. Peng, H. Wei, and P. Zhang, “Asymmetric cryptography based on wavefront sensing,” Opt. Lett. **31**, 3579–3581 (2006).
81. W. Qin and X. Peng, “Asymmetric cryptosystem based on phase-truncated Fourier transforms,” Opt. Lett. **35**, 118–120 (2010).
82. X. Wang and D. Zhao, “Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain,” Opt. Commun. **284**, 148–152 (2011).
83. I. Mehra, S. K. Rajput, and N. K. Nishchal, “Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification,” Opt. Eng. **52**, 028202 (2013).
84. A. Alfalou and C. Brosseau, “Dual encryption scheme of images using polarized light,” Opt. Lett. **35**, 2185–2187 (2010).

85. A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, “Simultaneous fusion, compression, and encryption of multiple images,” Opt. Express **19**, 24023–24029 (2011).
86. W. Chen, G. Situ, and X. Chen, “High-flexibility optical encryption via aperture movement,” Opt. Express **21**, 24680–24691 (2013).
87. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, “All-optical encrypted movie,” Opt. Express **19**, 5706–5712 (2011).
88. C. La Mela and C. Iemmi, “Optical encryption using phase-shifting interferometry in a joint transform correlator,” Opt. Lett. **31**, 2562–2564 (2006).
89. E. Rueda, C. Ríos, J. F. Barrera, and R. Torroba, “Master key generation to avoid the use of an external reference wave in an experimental JTC encrypting architecture,” Appl. Opt. **51**, 1822–1827 (2012).
90. 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).
91. J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, “Improved decryption quality and security of a joint transform correlator-based encryption system,” J. Opt. **15**, 025401 (2013).
92. F. Sadjadi and B. Javidi, *Physics of the Automatic Target Recognition* (Springer, 2007).
93. M. S. Millán, E. Pérez-Cabré, and B. Javidi, “Multifactor authentication reinforces optical security,” Opt. Lett. **31**, 721–723 (2006).
94. W. Chen and X. Chen, “Ghost imaging for three-dimensional optical security,” Appl. Phys. Lett. **103**, 221106 (2013).
95. A. Markman and B. Javidi, “Full-phase photon-counting double-random-phase encryption,” J. Opt. Soc. Am. A **31**, 394–403 (2014).
96. 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).
97. W. Chen and X. Chen, “Double random phase encoding using phase reservation and compression,” J. Opt. **16**, 025402 (2014).
98. A. Markman, B. Javidi, and M. Tehranipoor, “Photon-counting security tagging and verification using optically encoded QR codes,” IEEE Photon. J. **6**, 6800609 (2014).
99. S. Kishk and B. Javidi, “3D object watermarking by a 3D hidden object,” Opt. Express **11**, 874–888 (2003).
100. N. Savage, “Digital spatial light modulators,” Nat. Photonics **3**, 170–172 (2009).

Wen Chen received his B.Eng. and M.Eng. degrees from Chongqing University, China, in 2003 and 2006, respectively. Subsequently, he received the Ph.D. degree from the National University of Singapore in 2010. He was a visiting scholar at the Rowland Institute, Harvard University, from March 2013 to June 2013. He is currently a Research Fellow in the Department of Electrical and Computer Engineering, National University of Singapore. His research interests are experimental optics (i.e., optical metrology, digital holography, computer-generated holograms, optical microscopy, superresolution optical imaging, diffraction microscopy, and fringe projection) and computational optics (i.e., optical image processing, optical signal processing, fringe pattern analysis, quantitative phase retrieval, 3D numerical reconstruction, optical security, optical image encryption, optical information authentication, pattern recognition, and compressive sensing).

Bahram Javidi received the B.S. degree from George Washington University and the M.S. and Ph.D. degrees from the Pennsylvania State University, all in electrical engineering. He is the Board of Trustees Distinguished Professor at the University of Connecticut. He has more than 900 publications, including over 400 peer-reviewed journal articles, and more than 400 conference proceedings papers, including more than 110 plenary addresses, keynote addresses, and invited conference papers. His papers have been cited 12,000 times according to the citation index of *WEB of Science (h-index = 57)*. He is a coauthor on nine best paper awards.

Dr. Javidi has been named Fellow of several scientific societies, including IEEE, OSA, and SPIE. In 2010, he was the recipient of George Washington University's Distinguished Alumni Scholar Award, the university's highest honor for its alumni in all disciplines. In 2008, he received a Fellow award from the John Simon Guggenheim Foundation. He received the 2008 IEEE Donald G. Fink prized paper award among all (over 130) IEEE transactions, journals, and magazines. In 2007, The Alexander von Humboldt Foundation awarded Dr. Javidi the Humboldt Prize for outstanding U.S. scientists. He received the Technology Achievement Award from SPIE in 2008. In 2005, he received the Dennis Gabor Award in Diffractive Wave Technologies from SPIE. He was the recipient of the IEEE Photonics Distinguished Lecturer Award twice, in 2003–2004 and 2004–2005. He was awarded the IEEE Best Journal Paper Award from IEEE Transactions on Vehicular Technology twice, in 2002 and 2005. Early in his career, the National Science Foundation named Prof. Javidi a Presidential Young Investigator, and he received The Engineering Foundation and IEEE Faculty Initiation Awards. He was selected in 2003 as one of the nation's top 160 engineers between the ages of 30 and 45 by the National Academy of Engineering (NAE) to be an invited speaker at the Frontiers of Engineering Conference, which was co-sponsored by the Alexander von Humboldt Foundation. He is an alumnus of the Frontiers of Engineering of the National Academy of Engineering since 2003. He serves on the Editorial Board of the *Proceedings of the IEEE* journal (ranked #1 among all electrical engineering journals) as well as on the advisory board of the *IEEE Photonics Journal*, and he was on the founding board of editors of the IEEE/OSA *Journal of Display Technology*.

Xudong Chen received his B.S. and M.S. degrees in Electrical Engineering from Zhejiang University, Hangzhou, China, in 1999 and 2001, respectively, and the Ph.D. degree from the Massachusetts Institute of Technology in 2005. Since then he has joined the Department of Electrical and Computer Engineering, National University of Singapore, and he is currently an Associate Professor. His main research interests include electromagnetic wave theory and applications, inverse problems and optimization methods, nondestructive evaluation/ testing (NDE or NDT), optical imaging and near-field optics, microscopy, and optical encryption. He visited the University of Paris-SUD 11 in 2010 as an invited Visiting Associate Professor, and he took sabbatical leave to Stanford University from 2012 to 2013. Professor Chen was a recipient of the Young Scientist Award from the Union Radio-Scientifique Internationale (URSI) in 2010.