Research Article | Vol. 27, No. 5 | 4 Mar 2019 | OPTICS EXPRESS 7213
Optics EXPRESS

Optical image hiding under framework of computational ghost imaging based on an expansion strategy

SUI LIANSHENG,[1, 2,*] WANG JIAHAO,[1] TIAN AILING,[3] AND ANAND ASUNDI[4]

[1]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]Shaanxi Key Laboratory for Network Computing and Security Technology, Xi'an 710048, China
[3]Shaanxi Province Key Lab of Thin Film Technology and Optical Test, Xi'an Technological University, Xi'an 710048, China
[4]School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore 639798, Singapore
*liudua2010@gmail.com

Abstract: A novel optical image hiding scheme based on an expansion strategy is presented under the framework of computational ghost imaging. The image to be hidden is concealed into an expanded interim with the same size as the host image. This is implemented by rearranging the measured intensities of the original object after the process of ghost imaging. An initial Hadamard matrix is used to generate additional matrices by shifting it circularly along the column direction, so that enough 2D patterns are engendered to retrieve phase-only profiles for imaging. Next, the frequency coefficients of the host image are modified with that of the expanded interim by controlling a small weighting factor. After an inverse transform, the host image carrying the hidden information can be obtained with high imperceptibility. Security is assured by considering optical parameters, such as wavelength and axial distance, as secret keys due to their high sensitivity to tiny change. Importantly, differing from other computational ghost imaging based schemes, many phase-only profiles are used to collect the measured intensities to enhance the resistance against noise and occlusion attacks. The simulated experiments illustrate the feasibility and effectiveness of the proposed scheme.

1. Introduction

Over the past decades, substantial optical techniques have shown great potential in the field of information security on accounts of their particular advantages, such as high-speed processing, inherent parallelism and multidimensional capabilities [1–4]. Since the intriguing double random phase encoding (DRPE) has been developed by Refregier and Javidi [5], where the plain image can be encrypted into stationary white noise with the aid of two random phase masks placed in both the input and Fourier planes, a variety of optical transforms such as Fresnel transform, fractional Fourier transform, gyrator transform and others [6–14], have been studied to enhance the security of cryptosystems by considering additional parameters as the secret keys. Over time, novel cryptosystems based on other optical and digital techniques such as interference, polarized light, photon-counting, diffractive imaging, integral imaging, compressive sensing, ptychography, holography, phase retrieval, vector quantization and transport of intensity equation have been further developed [15–32].

As a novel approach to allow the reconstruction of an object by calculating intensity correlation between two optical beams, research on using computational ghost imaging in this field has attracted increasing attention in recent years [33–39]. Chen and Chen [40] used labyrinth-like phase modulation patterns to implement optical encryption, where a series of random phase only masks applied in the process of computational ghost imaging are obtained by processing a master mask with different labyrinths. Zhao et al. [41] combined

#355492 https://doi.org/10.1364/OE.27.007213
Journal © 2019 Received 18 Dec 2018; revised 18 Feb 2019; accepted 18 Feb 2019; published 27 Feb 2019

Optics EXPRESS

computational ghost imaging with compressive sensing and QR code to assure high robustness against attacks. Chen [42] extracted phase only masks from pre-generated random intensity-only maps for imaging, and varied axial distances randomly to improve security. Zhang et al. [43] reduced the amount of transmitted data largely by using a combination of compressive sensing and fast Fourier transform (FFT), where the FFT-coded image is encrypted in the configuration of computational ghost imaging. Jiang et al. [44] proposed an information security scheme based on computational temporal ghost imaging (CTGI), which takes advantage of the fact that the ultrafast signal can be recovered with a slow detector after a long exposure time. Qin and Zhang [45] coded the primary information into a data container, and performed further encryption with the conventional computation ghost imaging. Additionally, this technology has been widely applied for multiple-image encryption [46,47]. Li et al. [48] firstly obtained the sparse data of multiple plain images via lifting wavelet transform, and then compressed them in the row scanning compressive ghost imaging.

The optical schemes based on computational ghost imaging have outstanding merits such as no need for an imaging lens. Also intensity vectors are considered as encoded results, which makes computation ghost imaging an even more promising alternative in the field of image encryption, authentication and hiding. However, it can be found that most of the known schemes focus on how to reduce the number of measurements, namely how to collect lower number of intensities of the measured object. It will not only make the quality of reconstructed object low but also reduce the resistance against noise and occlusion attacks, which hinders further applications of computational ghost imaging. To avoid these shortcomings, an optical image hiding scheme is proposed based on an expansion strategy in this paper. Before embedding the hidden image into the host image in frequency domain, it is first encoded into an expanded interim, which contains plenty of measured intensities of the original image collected with computational ghost imaging. The frequency coefficients of the host image are modified with that of the interim and transformed, which makes the host image carrying the hidden information with high imperceptibility. To enhance the quality of reconstruction as well as the immunity to common attacks, phase only profiles used in the process of imaging are retrieved from 2D patterns, which are derived from a Hadamard matrix and its derivatives. Meanwhile, optical parameters such as wavelength and axial distance can be used as secret keys to enhance the security of the image hiding system.

The rest of this paper is organized as follows. In Section 2, along with the generation of phase only profiles from the Hadamard matrix, the proposed image hiding scheme based on the expanded strategy including embedding and extraction processes is theoretically introduced in detail. In Section 3, numerical results and security analysis are presented. Finally, a brief conclusion is described in Section 4.

2. Scheme description

In this section, the details of the proposed optical image hiding scheme is presented based on computational ghost imaging, where a large number of phase only profiles are used to collect the measured intensities of the original objects. Let $w(\mu,\upsilon)$ denotes the image to be hidden, which has $m\times n$ pixels, while $h(\mu,\upsilon)$ denotes the host image with $M\times N$ pixels. The diagram for illustrating the information embedding process is shown in Fig. 1(a), from which it can be seen that the original information should be encoded into an expanded image $w'(\mu,\upsilon)$ with the same size as the host image by using computational ghost imaging.

Initially, a mechanism of computational ghost imaging similar to the conventional optical configuration is applied to encode the original object into $w'(\mu,\upsilon)$, where the wave from the laser is collimated by a lens for the illumination and the space light modulator controlled by computer is used to load different phase only profiles in turn. To obtain a measured intensity,

Optics EXPRESS

the wave is modulated by one of phase only profiles to create a speckle pattern, which passes through the original object according to its transmission function $T(\mu,\upsilon)$. The total intensity B_i, collected by a single-pixel detector without spatial resolution, can be mathematically expressed as

$$B_i = \iint d\mu d\upsilon I_i(\mu,\upsilon) T(\mu,\upsilon), \tag{1}$$

where $I_i(\mu,\upsilon)$ denotes the speckle pattern and (μ,υ) is the transversal coordinates of the object plane. Essentially, the measured intensity is determined by the speckle pattern $I_i(\mu,\upsilon) = \left|E_i(\mu,\upsilon)\right|^2$, where $E_i(\mu,\upsilon)$ is the free-space propagation field for the phase only profile $\varphi_i(x,y)$ embedded into the spatial light modulator. The free-space propagation field at the axis distance z from the spatial light modulator can be described by using the Fresnel diffraction as

$$E_i(\mu,\upsilon) = \exp\left(j\varphi_i(x,y)\right) * h(x,y,z), \tag{2}$$

where $*$ denotes the convolution calculation and $h(x,y,z)$ is the point pulse function of the Fresnel propagation defined as

$$h(x,y,z) = \frac{\exp(j2\pi z/\lambda)}{jz\lambda}\exp\left(\frac{j\pi}{z\lambda}\left(x^2+y^2\right)\right), \tag{3}$$

where λ is the wavelength of the laser beam. As we all know, a large number of measurements are usually required to reconstruct the original objects with high quality. Besides this consideration, $M\times N$ measured intensities are collected with the help of corresponding number of phase only profiles, and rearranged to form the required expanded image $w'(\mu,\upsilon)$ with the same size as the host image in the proposed scheme, which will be helpful to hide the original object.

Optics EXPRESS

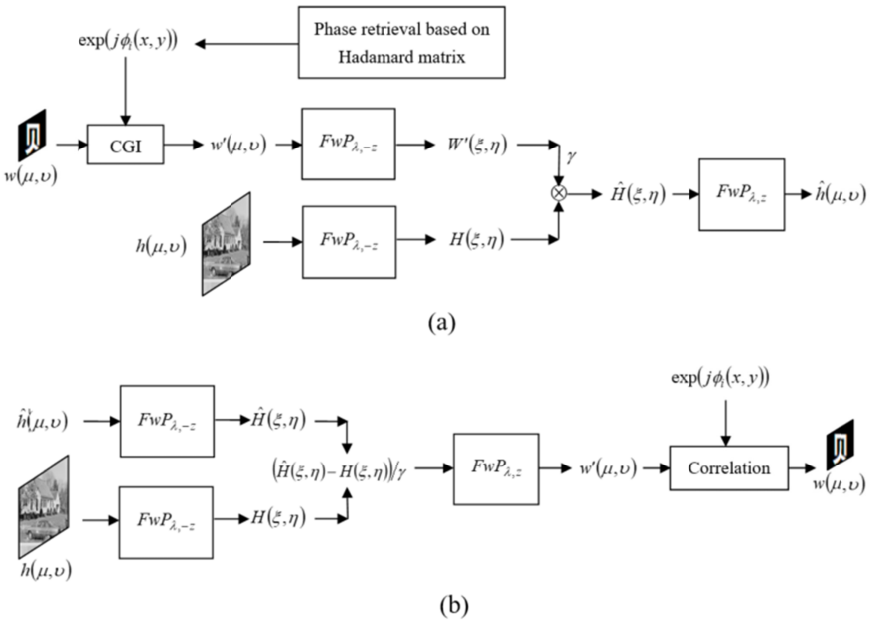

Fig. 1. Diagram of the optical image hiding scheme: (a) the information embedding process and (b) the information extraction process. CGI: computational ghost imaging; *FwP*: free-space wave propagation.

On the other hand, because the 2D patterns generated based on the Hadamard matrix are spatially orthogonal without any redundancy, the reconstructed object is clear when these patterns are used to illuminate an object to collect the measured intensities in the configuration of computational ghost imaging. Keeping this in mind, the phase only profiles derived from the Hadamard patterns by using the iterative phase retrieval algorithm are applied to record the measured intensities in the proposed scheme. Suppose that the size of the original object $w(\mu,\upsilon)$ satisfies the condition as $m\times n = 2^k$, and k is an integer, the Hadamard matrix with the order 2^k can be calculated as [36]

$$H^{(0)} = H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}. \tag{4}$$

When $k = 1$, the basic block with the order 2 is defined as

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{5}$$

Afterwards, each row of the Hadamard matrix is rearranged into a 2D pattern with $m\times n$ elements, from which a phase only profile can be derived using the modified Gerchberg–Saxton algorithm. Although a total of $m\times n$ phase only profiles can be obtained, it is obvious that the measured intensities collected based on these profiles are not enough to constitute the required expanded image $w'(\mu,\upsilon)$. Denoting $H^{(0)}$ calculated using Eq. (4) as the initial Hadamard matrix, some additional matrices can be generated from this matrix to deal with aforementioned problem. Firstly, the number of additional matrices is determined as

$$K = \lceil M/m \rceil \times \lceil N/n \rceil, \tag{6}$$

where $\lceil \cdot \rceil$ rounds the argument to the next larger integer. Secondly, along the column direction the initial matrix is shifted circularly K times to obtain additional matrices. In each shift, the shifting step Δ is set as

$$\Delta = \lfloor m/K \rfloor, \tag{7}$$

where $\lfloor \cdot \rfloor$ rounds the argument to the next smaller integer. In this way, $K+1$ matrices including the initial matrix are obtained, from which enough rows can be used to generate phase only profiles. It is worth noting that the rows whose elements all equal 1 will be considered invalid and discarded in the proposed scheme.

Besides retaining the $m \times n - 1$ effective rows of the initial Hadamard matrix, other $M \times N - m \times n + 1$ rows should be obtained from additional matrices. Then, these rows are converted into 2D patterns, from which a total of $M \times N$ phase only profiles can be retrieved. Supposing one of 2D patterns is denoted as $R_i(\mu, \upsilon)$ and the retrieved phase profile as $\varphi_i(x, y)$, similar to the modified Gerchberg–Saxton algorithm, the iterative phase retrieval process can be described as follows:

(1) Generate an initial phase profile $\varphi^{(0)}{}_i(x, y)$ in the phase only mask plane, where the phase values are randomly distributed in the range $[0, 2\pi]$.

(2) Perform the wave propagation forward to the image plane in the lth round, where the 2D pattern considered as the amplitude constraint is located, and obtain a complex-valued result as

$$U_i^{(l)}(\mu, \upsilon) = FwP_{\lambda, z}\left\{\exp\left(j\varphi^{(l)}(x, y)\right)\right\}, \tag{8}$$

where $FwP\{\cdot\}$ denotes the free-space wave propagation.

(3) Update above result with the known 2D pattern $R_i(\mu, \upsilon)$ as

$$\hat{U}_i^{(l)}(\mu, \upsilon) = \sqrt{R_i(\mu, \upsilon)}\exp\left(j\arg\left(U_i^{(l)}(\mu, \upsilon)\right)\right), \tag{9}$$

where $\arg(\cdot)$ is used to extract the phase information of the complex-valued result.

(4) Perform the wave back-propagation from the image plane to the phase only mask plane, and update the phase only profile as

$$\varphi_i^{(l+1)}(x, y) = \arg\left(FwP_{\lambda, -z}\left\{\hat{U}_i^{(l)}(\mu, \upsilon)\right\}\right). \tag{10}$$

(5) Calculate the correlation coefficient (CC) between the amplitude out $\left|U_i^{(l)}(\mu, \upsilon)\right|^2$ and the known 2D pattern, which is considered as the convergent criterion of iterative process and defined mathematically as

$$\mathrm{CC} = \frac{E[[\,|U_i|^2 - E[|U_i|^2]\,]][R_i - E[R_i]]]}{\sqrt{E[[\,|U_i|^2 - E[|U_i|^2]\,]^2]}\sqrt{E[[R_i - E[R_i]]^2]}}, \tag{11}$$

where $E[\cdot]$ denotes the expected value operator. For the sake of brevity, the coordinates of the wave propagation result and the pattern are omitted.

Optics EXPRESS

(6) Repeat (2)-(5) until the CC value reaches the pre-defined threshold, which is usually very close to 1 to make sure that the best result can be obtained. If the process is convergent after L iterations, the $\varphi_i^{(L+1)}(x,y)$ will be embedded into the spatial light modulator to collect the measured intensity of original object.

In addition, it is emphasized that the elements with value −1 in each row should be set to 0 because the intensities recorded in the image plane are positive.

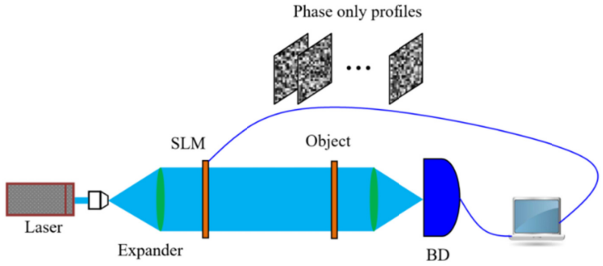

Fig. 2. Optical setup of computational ghost imaging. SLM, spatial light modulator; BD, bucket detector.

After each phase only profile is input into the spatial light modulator in the configuration of computational ghost imaging as shown in Fig. 2 and the corresponding intensity is recorded, $M \times N$ measured intensities can be collected to form an interim, namely the expanded image $w'(\mu,\upsilon)$, which will be embedded into the host image $h(\mu,\upsilon)$ by means of the free-space wave propagation analytically. With the same wavelength and the axis distance as set in the process of computational ghost imaging, $w'(\mu,\upsilon)$ and $h(\mu,\upsilon)$ are respectively transformed with the wave back-propagation, which can be mathematically expressed as

$$W'(\xi,\eta) = FwP_{\lambda,-z}\{w'(\mu,\upsilon)\}, \tag{12}$$

$$H(\xi,\eta) = FwP_{\lambda,-z}\{h(\mu,\upsilon)\}. \tag{13}$$

Conventionally, the transformed coefficients of the expanded image can be embedded into that of the host image with a small real weighting factor γ, which is described as

$$\hat{H}(\xi,\eta) = H(\xi,\eta) + \gamma W'(\xi,\eta). \tag{14}$$

Afterwards, the host image carrying the hidden information $w'(\mu,\upsilon)$ can be obtained with the wave forward-propagation, that is to say

$$\hat{h}(\mu,\upsilon) = \left| FwP_{\lambda,z}\{\hat{H}(\xi,\eta)\} \right|. \tag{15}$$

By controlling the weighting factor, the content of the host image can be noticed without the influence of hidden information.

To retrieve the hidden information, the extraction process can be realized in the simple inverse of the embedding process. As is illustrated in Fig. 1(b), the main steps should be paid attention as follows:

(1) The modified host image $\hat{h}(\mu,\upsilon)$ and original $h(\mu,\upsilon)$ are respectively transformed with the wave backpropagation. Along with the weighting factor, the resultant

$\hat{H}(\xi,\eta)$ and $H(\xi,\eta)$ are used to calculate the frequency coefficients of the hidden object, which can be described as

$$W'(\xi,\eta)=\left(\hat{H}(\xi,\eta)-H(\xi,\eta)\right)/\gamma. \tag{16}$$

(2) By making use of these frequency coefficients, the expanded image including measured intensities collected in the process of computational ghost imaging can be recovered with the wave forward-propagation, which is expressed as

$$w'(\mu,\upsilon)=\left|FwP_{\lambda,z}\left\{W'(\xi,\eta)\right\}\right|. \tag{17}$$

(3) After the expanded image is rearranged into the vector with $M\times N$ measured intensities, the hidden object can be reconstructed by using cross-correlation between the intensity B_i with the speckle pattern $I_i(\mu,\upsilon)$, which is described as

$$w(\mu,\upsilon)=\left\langle BI(\mu,\upsilon)\right\rangle-\left\langle B\right\rangle\left\langle I(\mu,\upsilon)\right\rangle=\frac{1}{N}\sum_{i=1}^{M\times N}\left(B_i-\left\langle B_i\right\rangle\right)\left(I_i(\mu,\upsilon)-\left\langle I_i(\mu,\upsilon)\right\rangle\right). \tag{18}$$

where $\langle\cdot\rangle$ denotes the ensemble average.

3. Results and analysis

To demonstrate the validity of the proposed image hiding scheme, a series of numerical simulations are carried out based on the configuration of computational ghost imaging as shown in Fig. 2, where the wavelength of the illuminating light is 632.8 nm, the axis distance from the spatial light modulator and the bucket detector is 7.4 cm and the pixel size is set to 20 μm. The original object to be hidden is a binary image with 64×64 pixels as shown in Fig. 3(a), which is the meaning of shell in Chinese. The host image named as "Car" is selected from USC-SIPI database [49], as shown in Fig. 3(b), which size is 256×256 pixels. The real weighting factor used for embedding the frequency coefficients of the expanded interim into that of the host image in the Fresnel domain is set to 0.0001, which assures that the information of original object cannot be noticed. In addition, the wavelength and axis distance used in the process of embedding are set to the same as that in the process of computational ghost imaging.

(a) (b)

Fig. 3. (a) The original object to be hidden and (b) the host image.

In each measurement of computational ghost imaging, a phase only profile with 64×64 pixels should be input into the spatial light modulator to collect the corresponding intensity, which is derived from one row of the Hadamard matrix with the order 2^{12}. Because there are a total of 2^{16} phase only profiles to be applied in the proposed optical image hiding scheme, 16

Optics EXPRESS

additional matrices are generated from the initial Hadamard matrix so that enough rows can be selected to retrieve phase only profiles. The shifting step is set to 4, which means that the initial matrix is shifted circularly 4 columns along the horizontal direction. Figures 4(a) and 4(b) show patterns that are derived from the first and last row of the initial Hadamard matrix. The corresponding phase only profiles obtained using the iterative phase retrieval algorithm after 50 iterations is displayed in the Figs. 4(c) and 4(d), respectively. The correlation between these two profiles is 0.1451, and similar results can be obtained between any two phase only profiles. So, it can be seen that the phase only profiles are strongly uncorrelated.

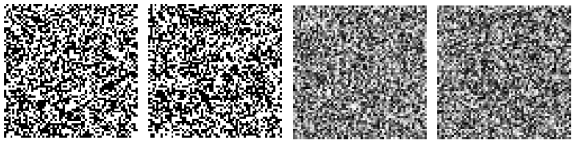

Fig. 4. (a)-(b) 2D patterns derived from the initial Hadamard matrix and (c)-(d) the corresponding phase only profiles retrieved from (a) and (b).

After 2^{16} phase only profiles are input into spatial light modulator sequentially, the same number of measured intensities of the original object can be collected to form an expanded image. As shown in Fig. 5(a), any valid information cannot be discerned visually from this expanded interim. The host image carrying the information of original object is displayed in Fig. 5(b). The correlation coefficient between it and the original host image is 0.9999, which means that there is no visual degradation that can be observed with naked eyes. The optical parameters such as wavelength and axis distance applied in the process of computational ghost imaging are usually considered as secret keys to enhance the security level. When correct keys are applied to reconstruct the hidden object, the retrieved information based on second-order correlation algorithm described as Eq. (18) can be obtained as shown in Fig. 5(c). The correlation coefficient between it and the original object is 0.9967, and the reconstructed result is very satisfactory due to its clear structure.

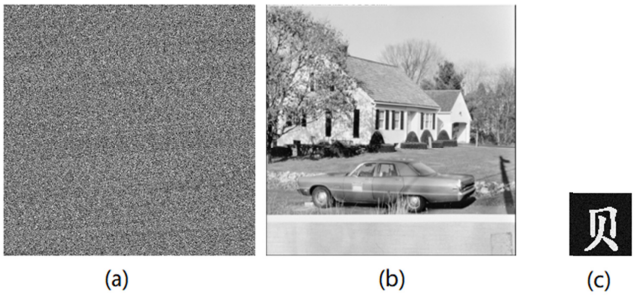

Fig. 5. (a) The expanded interim, (b) the host image carrying the information of original object and (c) the retrieved information of the original object.

As the important secret keys in the proposed image hiding scheme, the optical parameters such as wavelength and axis distance can provide necessary protection to ensure that the hidden object cannot be easily conjectured by an unauthorized user. When the wavelength has the deviation as ± 0.001 nm, the retrieved information is displayed in Figs. 6(a) and 6(b), respectively, where the distributions are very noisy. The correlation coefficient curve is plotted in Fig. 6(c), where the deviation of wavelength varies from -0.002 nm to $+0.002$ nm. It can be seen that the correlation coefficient value decreases sharply when the wavelength has a tiny change. Actually, when the deviation reaches ± 0.0004 nm, the correlation coefficient value only is 0.1089 so that the reconstructed result cannot be discerned visually. Similar conclusion can be obtained when the axis distance has the tiny variation. Figures 7(a) and

7(b) show the retrieved objects, where the axis distance has the deviation as $\pm 0.0001\,\mathrm{mm}$, respectively. The corresponding curve is plotted in Fig. 7(c). Therefore, it is safe to say that these optical parameters can play a vital role in enhancing the security of the proposed scheme due to their high sensitivity.

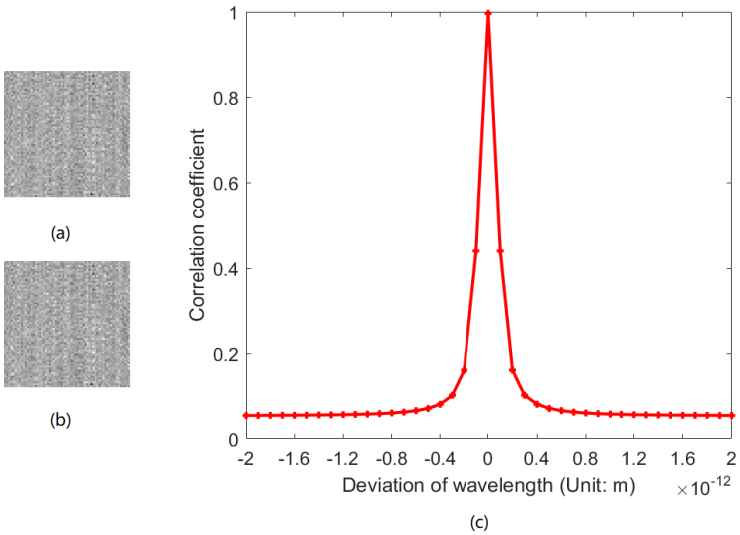

Fig. 6. (a)-(b) The reconstructed objects when the wavelength has tiny deviations and (c) correlation coefficient curve versus the variation of wavelength.

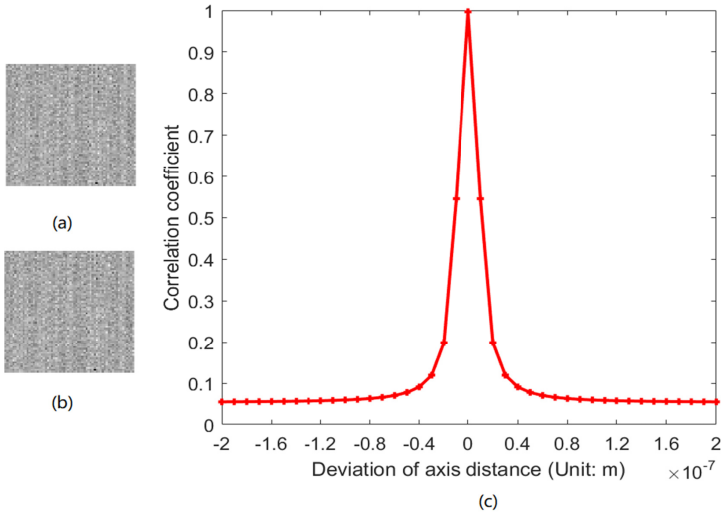

Fig. 7. (a)-(b) The reconstructed objects when the axis distance has tiny deviations and (c) correlation coefficient curve versus the variation of axis distance.

To evaluate the ability of resistance against noise and occlusion attacks, the quantitative analyses are executed in these two cases. According to noise attack, the host image carrying the hidden object is supposed to be contaminated with a Gaussian random noise denoted as $G(\mu,\upsilon)$ with mean 0 and standard deviation 0.1, which can be mathematically described as

$$h'(\mu,\upsilon)=\hat{h}(\mu,\upsilon)\times\left(1+kG(\mu,\upsilon)\right), \tag{19}$$

Optics EXPRESS

where $h'(\mu,\upsilon)$ is the contaminated host image and k is the noise strength. When the noise strength equals 0.1, 0.2, 0.3, 0.4 and 0.5, the corresponding retrieved information is shown in Figs. 8(a)-8(e), respectively. With the noise strength increasing, the structure of original object becomes more and more blurred. The structure of original object can be recognized even when $k = 0.3$, while only the residual information can be observed when the strength coefficient is larger than 0.3. In spite of this, the existence of original object can be identified using the nonlinear correlation algorithm [50]. Figure 8(f) shows the nonlinear correlation map between the reconstructed object with original one when $k = 0.5$. A remarkable peak over the noisy background can be observed, which obviously indicates the existence of original object.

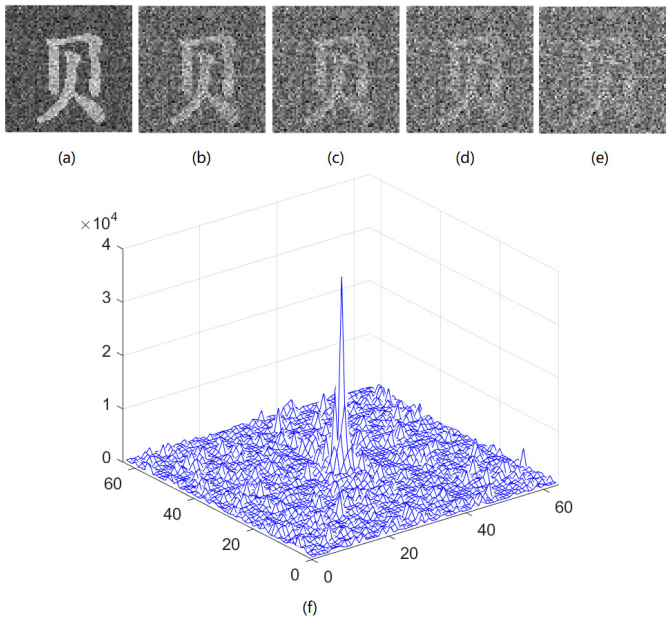

Fig. 8. (a)-(e) The reconstructed object when the noise strength equals 0.1, 0.2, 0.3, 0.4, and 0.5, respectively, and (f) the nonlinear correlation map when the noise strength equals 0.5.

To analyze the effect of occlusion attack, the host image carrying the hidden object is supposed to be occluded in the center region with different percentage. Figures 9(a)-9(e) show the retrieved information when the host image is occluded with 2.73%, 5.47%, 8.20%, 10.94% and 13.67%, respectively. With the occluded region increasing, the quality of the retrieved object gradually becomes deteriorated. When the occluded region reaches 13.67%, the structure of original object can be discerned faintly. In addition, the existence of original object still can be verified using the nonlinear correlation algorithm, which is similar to the case of noise attack. Figure 9(f) shows the nonlinear correlation map between the reconstructed object with original one when the occluded region reaches 13.67%, where a remarkable peak over the noisy background can be observed clearly. Through above analyses on noise and occlusion attacks, it can be concluded that the proposed optical image hiding scheme has high tolerance to these attacks.

Optics EXPRESS

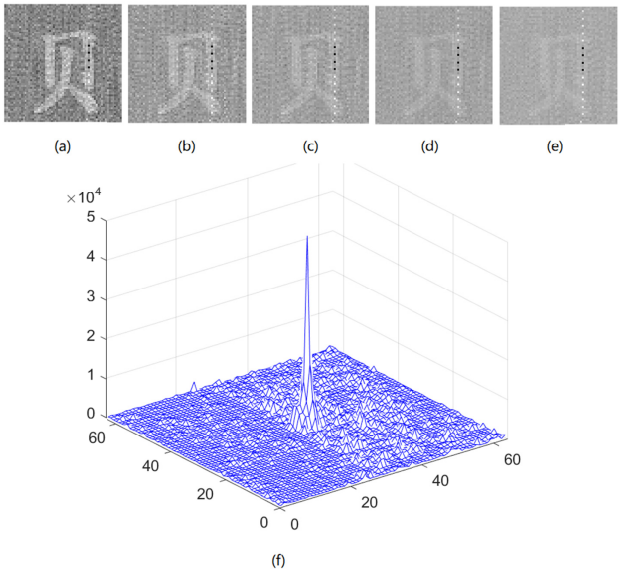

Fig. 9. (a)-(e) The reconstructed object when the occluded region reaches 2.73%, 5.47%, 8.20%, 10.94% and 13.67%, respectively, and (f) the nonlinear correlation map when the occluded region reaches 13.67%.

4. Conclusion

In summary, a novel method for optical image hiding based on computational ghost imaging is presented, where the object to be hidden is initially encoded into an interim with an expansion strategy. The origin information is recorded as a set of measured intensities with the same number as pixels of the host image in the configuration of computational ghost imaging, where an initial Hadamard matrix is used to generate additional matrices by shifting it circularly so that enough rows can be chosen to retrieve the required phase only profiles for imaging. By embedding the frequency coefficients of the expanded interim with the small weighting factor, the host image carrying the original information has good performance of imperceptibility. Meanwhile, the security is guaranteed by applying optical parameters such as wavelength and axis distance as the secret keys due to their high sensitivity. Moreover, because phase only profiles are generated from spatially orthogonal 2D Hadamard patterns, the robustness against noise and occlusion attacks is enhanced. Numerical results demonstrate that the proposed scheme is feasible and effective.

Funding

Key Laboratory Science Research Plan of Education Department of Shaanxi Province (16JS079); Xi'an Science and Technology Bureau (CXY1509 (3)).

References

1. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photonics **6**(2), 120–155 (2014).
2. A. Alfalou and C. Brosseau, "Recent advances in optical image processing," Prog. Opt. **60**, 119–262 (2015).
3. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, and A. Markman, "Roadmap on optical security," J. Opt. **18**(8), 083001 (2016).
4. Q. Wang, A. Alfalou, and C. Brosseau, "New perspectives in face correlation research: a tutorial," Adv. Opt. Photonics **9**(1), 1–78 (2017).
5. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).

Optics EXPRESS

6. Z. Liu, C. Guo, J. Tan, W. Liu, J. Wu, Q. Wu, L. Pan, and S. Liu, "Securing color image by using phase-only encoding in Fresnel domains," Opt. Lasers Eng. **68**, 87–92 (2015).
7. H. Xu, W. Xu, S. Wang, and S. Wu, "Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain," Opt. Commun. **402**, 302–310 (2017).
8. T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Security of image encryption scheme based on multi-parameter fractional Fourier transform," Opt. Commun. **376**, 47–51 (2016).
9. L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," Opt. Laser Technol. **103**, 48–58 (2018).
10. S. Liansheng, Z. Xiao, H. Chongtian, T. Ailing, and A. Krishna Asundi, "Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms," Opt. Lasers Eng. **113**, 29–37 (2019).
11. J. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and H. Yu, "Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains," Opt. Lasers Eng. **66**, 1–9 (2015).
12. L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie, "An asymmetric color image encryption method by using deduced gyrator transform," Opt. Lasers Eng. **89**, 72–79 (2017).
13. H. Singh, "Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain," Opt. Lasers Eng. **81**, 125–139 (2016).
14. O. S. Faragallah, "Optical double color image encryption scheme in the Fresnel-based Hartley domain using Arnold transform and chaotic logistic adjusted sine phase masks," Opt. Quantum Electron. **50**(3), 118 (2018).
15. Y. Qin, H. Wang, Z. Wang, Q. Gong, and D. Wang, "Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal," Opt. Lasers Eng. **84**, 62–73 (2016).
16. M. R. Abuturab, "Securing multiple information using chaotic spiral phase encoding with simultaneous interference and superposition methods," Opt. Lasers Eng. **98**, 1–16 (2017).
17. Z. Zhong, H. Qin, L. Liu, Y. Zhang, and M. Shan, "Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain," Opt. Express **25**(6), 6974–6982 (2017).
18. A. Carnicer, A. Hassanfiroozi, P. Latorre-Carmona, Y. P. Huang, and B. Javidi, "Security authentication using phase-encoded nanoparticle structures and polarized light," Opt. Lett. **40**(2), 135–138 (2015).
19. D. Maluenda, A. Carnicer, R. Martínez-Herrero, I. Juvells, and B. Javidi, "Optical encryption using photon-counting polarimetric imaging," Opt. Express **23**(2), 655–666 (2015).
20. I. Moon, F. Yi, M. Han, and J. Lee, "Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms," Appl. Opt. **55**(16), 4328–4335 (2016).
21. I. Muniraj, C. Guo, R. Malallah, J. P. Ryle, J. J. Healy, B. G. Lee, and J. T. Sheridan, "Low photon count based digital holography for quadratic phase cryptography," Opt. Lett. **42**(14), 2774–2777 (2017).
22. A. Fatima, I. Mehra, and N. K. Nishchal, "Optical image encryption using equal modulus decomposition and multiple diffractive imaging," J. Opt. **18**(8), 085701 (2016).
23. L. Chen, G. Chang, B. He, H. Mao, and D. Zhao, "Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition," Opt. Lasers Eng. **88**, 221–232 (2017).
24. Y. Qin, Z. Wang, H. Wang, Q. Gong, and N. Zhou, "Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container," Opt. Lasers Eng. **105**, 118–124 (2018).
25. X. Li, M. Zhao, Y. Xing, L. Li, S. T. Kim, X. Zhou, and Q. H. Wang, "Optical encryption via monospectral integral imaging," Opt. Express **25**(25), 31516–31527 (2017).
26. B. Deepan, C. Quan, Y. Wang, and C. J. Tay, "Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique," Appl. Opt. **53**(20), 4539–4547 (2014).
27. N. Rawat, I. C. Hwang, Y. Shi, and B. G. Lee, "Optical image encryption via photon-counting imaging and compressive sensing based ptychography," J. Opt. **17**(6), 065704 (2015).
28. S. K. Rajput and O. Matoba, "Optical voice encryption based on digital holography," Opt. Lett. **42**(22), 4619–4622 (2017).
29. Y. Wang, C. Quan, and C. J. Tay, "Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm," Opt. Lasers Eng. **78**, 8–16 (2016).
30. S. Liansheng, X. Meiting, and T. Ailing, "Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain," Opt. Lett. **38**(11), 1996–1998 (2013).
31. L. Sui, M. J. Xu, C. Huang, A. Adhikari, A. Tian, and A. Asundi, "Multiple-image encryption by space multiplexing based on vector quantization and interference," OSA Cont. **1**(4), 1370–1384 (2018).
32. L. Sui, X. Zhao, C. Huang, A. Tian, and A. Asundi, "An optical multiple-image authentication based on transport of intensity equation," Opt. Lasers Eng. **116**, 116–124 (2019).
33. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**(14), 2391–2393 (2010).
34. M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," Appl. Phys. Lett. **101**(10), 101108 (2012).
35. M. Zafari, R. Kheradmand, and S. Ahmadi-Kandjani, "Optical encryption with selective computational ghost imaging," J. Opt. **16**(10), 105405 (2014).
36. L. Wang and S. Zhao, "Fast reconstructed and high-quality ghost imaging with fast Walsh-Hadamard transform," Photon. Res. **4**(6), 240–244 (2016).

Optics EXPRESS

37. S. Yuan, X. Liu, X. Zhou, and Z. Li, "Multiple-image encryption scheme with a single-pixel detector," J. Mod. Opt. **63**(15), 1457–1465 (2016).
38. S. Liansheng, C. Yin, L. Bing, T. Ailing, and A. K. Asundi, "Optical image encryption via high-quality computational ghost imaging using iterative phase retrieval," Laser Phys. Lett. **15**(7), 075204 (2018).
39. S. Liansheng, C. Yin, W. Zhanmin, T. Ailing, and A. K. Asundi, "Single-pixel correlated imaging with high-quality reconstruction using iterative phase retrieval algorithm," Opt. Lasers Eng. **111**, 108–113 (2018).
40. W. Chen and X. Chen, "Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption," EPL **109**(1), 14001 (2015).
41. S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique," Opt. Commun. **353**, 90–95 (2015).
42. W. Chen, "Correlated-photon secured imaging by iterative phase retrieval using axially-varying distances," IEEE Photonics Technol. Lett. **28**(18), 1932–1935 (2016).
43. Z. Leihong, P. Zilan, W. Luying, and M. Xiuhua, "High-performance compression and double cryptography based on compressive ghost imaging with the fast Fourier transform," Opt. Lasers Eng. **86**, 329–337 (2016).
44. S. Jiang, Y. Wang, T. Long, X. Meng, X. Yang, R. Shu, and B. Sun, "Information security scheme based on computational temporal ghost imaging," Sci. Rep. **7**(1), 7676 (2017).
45. Y. Qin and Y. Zhang, "Information Encryption in ghost imaging with customized data container and XOR operation," IEEE Photonics J. **9**(2), 1–8 (2017).
46. J. Wu, Z. Xie, Z. Liu, W. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on computational ghost imaging," Opt. Commun. **359**, 38–43 (2016).
47. X. Li, X. Meng, X. Yang, Y. Yin, Y. Wang, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," IEEE Photonics J. **8**(4), 1–11 (2016).
48. X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme," Opt. Lasers Eng. **102**, 106–111 (2018).
49. Original images: http://sipi.usc.edu/database/database.php.
50. W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," Opt. Lett. **38**(4), 546–548 (2013).