ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Optical encryption of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography

Ying Wang(王莹), Qi Liu(刘琦), Jun Wang(王君), Qiong-Hua Wang(王琼华)
Citation: Chin. Phys. B . 2018, 27(3): 034202. **doi:** 10.1088/1674-1056/27/3/034202

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Reflective ghost imaging free from vibrating detectors

Heng-xing Li(李恒星), Yan-feng Bai(白艳锋), Xiao-hui Shi(施晓辉), Su-qin Nan(南苏琴), Li-jie Qu(屈利杰), Qian Shen(沈倩), Xi-quan Fu(傅喜泉)
Chin. Phys. B . 2017, 26(10): 104204. **doi:** 10.1088/1674-1056/26/10/104204

Wavefront analysis for plenoptic camera imaging

Yin-Sen Luan(栾银森), Bing Xu(许冰), Ping Yang(杨平), Guo-Mao Tang(汤国茂)
Chin. Phys. B . 2017, 26(10): 104203. **doi:** 10.1088/1674-1056/26/10/104203

Optical encryption scheme based on ghost imaging with disordered speckles

Yu-dong Zhang(张玉东), Sheng-mei Zhao(赵生妹)
Chin. Phys. B . 2017, 26(5): 054205. **doi:** 10.1088/1674-1056/26/5/054205

Latest development of display technologies

Hong-Yue Gao(高洪跃), Qiu-Xiang Yao(姚秋香), Pan Liu(刘攀), Zhi-Qiang Zheng(郑志强), Ji-Cheng Liu(刘吉成), Hua-Dong Zheng(郑华东), Chao Zeng(曾超), Ying-Jie Yu(于瀛洁), Tao Sun(孙涛), Zhen-Xiang Zeng(曾震湘)
Chin. Phys. B . 2016, 25(9): 094203. **doi:** 10.1088/1674-1056/25/9/094203

Locating the position of objects in non-line-of-sight based on time delay estimation

Xue-Feng Wang(王雪峰), Yuan-Qing Wang(王元庆), Jin-Shan Su(苏金善), Xing-Yu Yang(杨兴雨)
Chin. Phys. B . 2016, 25(8): 084203. **doi:** 10.1088/1674-1056/25/8/084203

Optical encryption of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography*

Ying Wang(王莹), Qi Liu(刘琦), Jun Wang(王君)†, and Qiong-Hua Wang(王琼华)

School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, *China*

(Received 5 September 2017; revised manuscript received 31 October 2017; published online 11 February 2018)

We present an optical encryption method of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography. By modifying the Mach–Zehnder interferometer, the interference of the multiple objects beams and the one reference beam is used to simultaneously encrypt multiple objects into a ciphertext. During decryption, each three-dimensional object can be decrypted independently without having to decrypt other objects. Since the single-pixel digital holography based on compressive sensing theory is introduced, the encrypted data of this method is effectively reduced. In addition, recording fewer encrypted data can greatly reduce the bandwidth of network transmission. Moreover, the compressive sensing essentially serves as a secret key that makes an intruder attack invalid, which means that the system is more secure than the conventional encryption method. Simulation results demonstrate the feasibility of the proposed method and show that the system has good security performance.

Keywords: multiple three-dimensional objects encryption, single-pixel digital holography, phase-shifting interference, compressive sensing

PACS: 42.30.–d, 42.30.Va, 42.40.My, 42.40.Kw **DOI:** 10.1088/1674-1056/27/3/034202

1. Introduction

In recent years, many optical encryption technologies of two-dimensional (2D) information have been proposed and implemented.[1–6] Compared with the traditional 2D information, the three-dimensional (3D) information is superior because it can accurately render sensations of the depth, location, and spatial relations of 3D scenes information.[7–9] Therefore, the development of 3D display and 3D information encryption will greatly promote the information visualization and security of multiple dimensional data, such as medical imaging and virtual reality.[10–12] Hence, optical encryption of 3D objects becomes a hot issue in the field of security. Javidi *et al.* presented an encryption 3D display system interfaced with data newsletter for encrypted digital holograms.[13] Meanwhile, Kim *et al.* demonstrated a technique for 3D information security with virtual optics based hologram encryption.[14] Kong *et al.* proposed a novel approach for encrypting 3D scene information hierarchically based on computer-generated holograms (CGHs).[15] However, the above mentioned encryption systems are encrypting on a single object.

The multiple 3D objects encryption (MOE) algorithm means encrypting the scenes information of multiple 3D objects (more than two objects) into a ciphertext. The encryption technique can hide more information, which can increase the efficiencies of encryption, decryption information storage, and transmission. Therefore, the MOE technique is more promising than the single 3D object encryption technique. However, there are still some issues that need addressing in the multiple 3D objects encryption algorithm, which are the major limiting factors in the development of multiple object cryptography. Two main issues are crosstalk, which means how to reconstruct each high-quality single object from a single ciphertext, and decryption flexibility, which means each 3D object can be decrypted arbitrarily. Recently, Li *et al.* effectively solved the above two problems by proposing a three-step phase shifting method for the multiple-3D-object secure information system.[16,17] The huge storage required for storing and transmitting the ciphertext is another major issue. To the best of our knowledge, it has not been resolved. In other words, it is quite difficult to encrypt more than one object simultaneously with the current optical method. Therefore, there is little in the literature on the multiple 3D encryption system.

In this paper, we propose a multiple 3D objects encryption method based on multiple interferences and single-pixel digital holography. This system can simultaneously encrypt the information of multiple 3D objects into a single ciphertext by multiple interferences. At the same time, in the decryption process of each 3D object can be decrypted separately, which is very flexible. Moreover, in order to alleviate the problem of a large amount of encryption data in Ref. [16], the single pixel digital holography is introduced to record the ciphertext. This is the most important improvement in comparison with Ref. [16]. By using this approach, even if the measurements of the ciphertext are less than the number of original samples pixels, the original samples can be reconstructed through compressed sensing theory. Therefore, it greatly reduces the storage burden and bandwidth of the encrypted data transmission

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61405130 and 61320106015).

†Corresponding author. E-mail: jwang@scu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

network while not impacting the image quality. In addition, it also greatly increases the number and space of keys. Simulation results demonstrate the feasibility of the method, and it shows that the system has good security.

2. The principle of encryption and decryption

Here some basic principles related to our proposed scheme are introduced.

2.1. Single-pixel digital holography

The single-pixel digital holography[18–21] is a promising method for a holographic technique, which utilizes the concept of the single pixel camera proposed by Baraniuk.[22,23] By using this technique, the hologram can be reconstructed from the samples smaller than the Nyquist rate. The approach allows image compression to be performed during measurement rather than in the post-processing stage. The main principle of the single-pixel digital holographic technique combined the single pixel detector and compressive sensing (CS)[24–26] theory is to obtain the intensity measurement of a scene by imaging the scene using a structured mask implemented by the programmable spatial light modulator (SLM).

The data acquisition framework model of a single pixel digital holographic system based CS method is given as

$$\boldsymbol{X} = \psi \boldsymbol{x}, \tag{1}$$

where $\boldsymbol{X}$ is the real-valued coefficient signal of length N, assuming that the $N \times N$ dimensional coefficient basis ψ provides the K-sparse representation of the signal $\boldsymbol{X}$, and $\boldsymbol{x}$ is an $N \times 1$ dimensional vector with K nonzero elements.

In the CS process, instead of sampling $\boldsymbol{X}$ directly, the linear measurements ($M < N$) are adopted, which can be expressed as

$$\boldsymbol{y} = \boldsymbol{\Phi} \boldsymbol{X}, \tag{2}$$

where $\boldsymbol{\Phi}$ is an $M \times N$ measurement matrix, which should be incoherent with ψ, and $\boldsymbol{y}$ is the M measurements. By combining the sparse representation and measurement process, equation (2) can be converted to

$$\boldsymbol{y} = \boldsymbol{\Phi} \psi \boldsymbol{x}. \tag{3}$$

To recover the sparse signal $\boldsymbol{X}$ from the measurements $\boldsymbol{y}$ for $M \ll N$ correctly, $\boldsymbol{\Phi}$ should be satisfying the restricted isometry property (RIP),[24] here the definition of RIP in k order is as follows:

$$(1 - \delta_k) \|x\|_2^2 \leq \|\boldsymbol{\Phi} \boldsymbol{x}\|_2^2 \leq (1 + \delta_k) \|\boldsymbol{x}\|_2^2, \tag{4}$$

where $\delta_k \in [0, 1]$ is an isometry constant. The original signal $\boldsymbol{X}$ can be recovered by solving the following non-convex optimization problem:

$$\min \|\boldsymbol{x}\|_o \text{ subject to } \boldsymbol{y} = \boldsymbol{\Phi} \psi \boldsymbol{x}. \tag{5}$$

In the proposed scheme, we use the Walsh–Hadamard matrices for the measurement matrix and the wavelet basis for the sparsifying basis.

2.2. Encryption process

The experimental setup of the proposed multiple 3D objects encryption system is shown in Fig. 1. It consists of an improved Mach–Zehnder interferometer based on a single pixel imaging system. The collimated laser beam through the beam expander is split into multiple parallel beams by several beam splitters. Each beam is directed to the object which results in multiple object beams. Then, each beam is propagated through the Fresnel diffraction, and the diffracted field of each object is sampled by different measurement matrix patterns with a liquid crystal spatial light modulator. Afterward, the all sampled diffracted field would be encrypted to a single ciphertext with multiple-interference and phase-shifting technique.

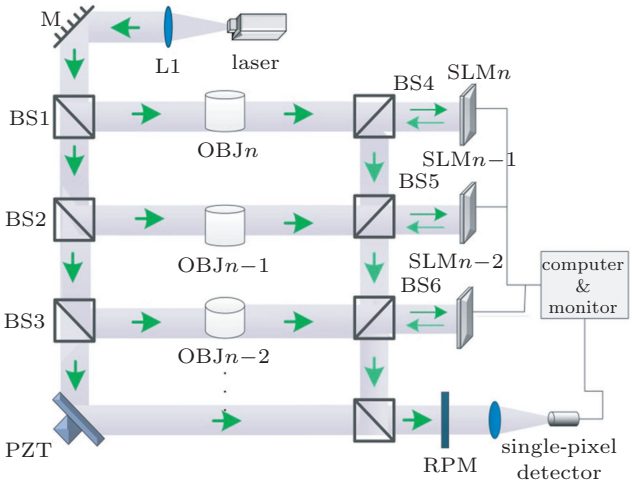


Fig. 1. (color online) Schematic diagram of the optical setup: L, lens; M, mirror; SF, spatial filter; BS, beam splitter; RPM, random phase mask; SLM, spatial light modulator; PZT, piezoelectric.

Since the two methods are applied with multiple-interference theory, these two experimental set-ups are similar. However, compared with the experimental set-up in Ref. [16], we replace the common CCD by a single-pixel camera in capturing which needs a reflective liquid crystal on silicon (LCOS) SLM for each object. Here, the SLM is to display the computer generated binary patterns and to modulate the object diffraction pattern, which plays a role of sampling the object light field.

Note that since $2n$ beam splitters are employed, there are so many optical surfaces in the encryption process that will result in undesired interferences, this degrades the reconstructed image. Therefore, the number of encrypted objects is limited in order to ensure the quality of the reconstructed image in practical optical implementation.

Assume that the complex amplitude distributions of the objects needed to encrypt are $f_1(xy), f_2(xy), \ldots, f_n(xy)$, respectively. Then each beam is transformed to the spatial frequency domain through Fresnel diffraction with optical wavelength λ and propagation distance z, the complex amplitude distribution of each object beam is obtained as

$$F_i(x,y) = \mathrm{FrT}\{f_i(x,y);\lambda;z_i\}, \tag{6}$$

where FrT denotes the Fresnel transformation; the optical wavelength λ and propagation distance z act as the secret keys during the decryption.

To adapt the concept of a single-pixel camera to solve the problem of a large amount of data during the holographic interference imaging, we use reflective LCOS SLM to sample the diffraction pattern of each object. These M binary patterns are generated by a computer and sequentially displayed onto the SLMs. The diffraction field of each object with N pixels is multiplied in parallel by M different binary patterns (with $M < N$), and the total intensity of the resulting matrices is computed as

$$s_i(x,y) = \Phi_i F_i(x,y), \tag{7}$$

where Φ_i denotes the measurement matrix. Continually, multiple sampled object beams propagate forward to pass through an RPM with size $M \times N$ that is the decryption key, and the light fields of all objects can be written as

$$\begin{aligned} U(x,y) = {} & \{[s_1(x_1,y_1) \times M(x,y)] + [s_2(x,y) \times M(x,y)] + \cdots \\ & + [s_n(x,y) \times M(x,y)]\}. \end{aligned} \tag{8}$$

On the other hand, in the reference arm, the phase of the plane beam is modulated by the PZT to achieve phase shifting. Two-step-only quadrate phase shifting holography ($\varphi = 0; \pi/2$) is used to record the encrypted data. Hence the complex amplitudes of the two holograms are I_0 and $I_{\pi/2}$, respectively, which can be expressed as

$$I(x,y;0) = A_\mathrm{U}^2 + A_\mathrm{R}^2 + 2A_\mathrm{U}A_\mathrm{R}\cos(\varphi_1), \tag{9}$$

$$I\left(x,y;\frac{\pi}{2}\right) = A_\mathrm{U}^2 + A_\mathrm{R}^2 + 2A_\mathrm{U}A_\mathrm{R}\cos(\varphi_2), \tag{10}$$

$$\mathrm{Eny}(x,y) = [I_0 - (A_\mathrm{U}^2 + A_\mathrm{R}^2)] + \mathrm{i}[I_{\pi/2} - (A_\mathrm{U}^2 + A_\mathrm{R}^2)], \tag{11}$$

where A_U and A_R denote the amplitudes of the object wave and the reference wave, respectively, $\varphi_1 = 0$, $\varphi_2 = \pi/2$; and $A_\mathrm{U}^2 + A_\mathrm{R}^2$ is the zero order light of the hologram generated from $U(x,y)$. The final cipher holograms are transmitted to the corresponding authorized user for decrypting all of the 3D objects.

It should be emphasized that one arbitrary three-dimensional object is the crosstalk noise of the other three-dimensional objects, which makes it impossible for us to identify the corresponding decrypted 3D object. The complex opposite of the cross talk noise can be utilized as the auxiliary decryption keys to decrypt a high-quality 3D object. The $I_{\mathrm{T}1}$ and $I_{\mathrm{T}2}$ include the optical fields of the other objects excepting OBJi which are transmitted to the corresponding authorized user to decrypt OBJi

$$\begin{aligned} T_i(x,y) = {} & \mathrm{FrT}\{s_1(x_1,y_1);z_1\} + \cdots \\ & + \mathrm{FrT}\{s_{i-1}(x_{i-1},y_{i-1});z_{i-1}\} \\ & + \mathrm{FrT}\{s_{i+1}(x_{i+1},y_{i+1});z_{i+1}\} + \cdots \\ & + \mathrm{FrT}\{s_n(x_n,y_n);z_n\}, \end{aligned} \tag{12}$$

$$I_{\mathrm{T}1}(x,y;0) = A_\mathrm{T}^2 + A_\mathrm{R}^2 + 2A_\mathrm{T}A_\mathrm{R}\cos(\varphi_1), \tag{13}$$

$$I_{\mathrm{T}2}\left(x,y;\frac{\pi}{2}\right) = A_\mathrm{T}^2 + A_\mathrm{R}^2 + 2A_\mathrm{T}A_\mathrm{R}\cos(\varphi_2), \tag{14}$$

$$\begin{aligned} \mathrm{Key2}(x,y) = {} & -[I_{\mathrm{T}1} - (A_\mathrm{T}^2 + A_\mathrm{R}^2)] \\ & - \mathrm{i}[I_{\mathrm{T}2} - (A_\mathrm{T}^2 + A_\mathrm{R}^2)], \end{aligned} \tag{15}$$

where A_T and A_R denote the amplitudes of the object wave and the reference wave, respectively, $\varphi_1 = 0$, $\varphi_2 = \pi/2$; and $A_\mathrm{T}^2 + A_\mathrm{R}^2$ is the zero order light of the hologram generated from $T(x,y)$.

2.3. Decryption process

Since the 3D scene information can be firstly decrypted by the single interference method in Ref. [16] and then reconstructed by a computer using the CS theory, the decryption process of our proposed method can be realized by a pure digital method or partly realized by the optical method as in Ref. [16]. The optical part of decryption is shown in Fig. 2.

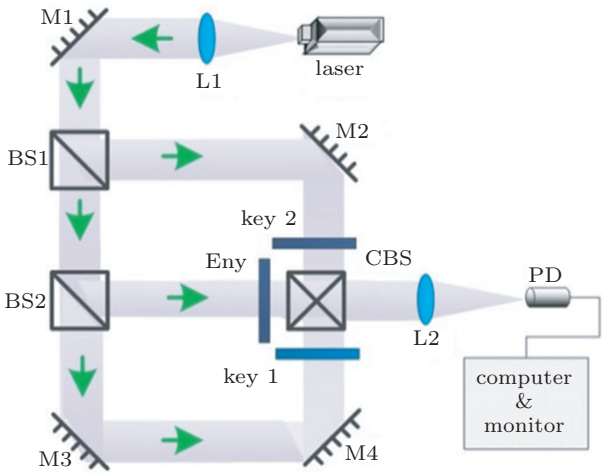


Fig. 2. (color online) Schematic diagram of the decryption setup: L, lens; M, mirror; SF, spatial filter; BS, beam splitters; PD, point detector.

Firstly, the plane wave is split into three plane waves by two BS. One of the plane waves passes through the ciphertext and the other two pass through key 1 and key 2 respectively. Continuously, the multiple plane waves interfere via a cube cross beam splitter (CBS). After it is transformed to the spatial domain with the correct optical wavelength and right propagation distance, the compressed 3D scene information is obtained as

$$\mathrm{C_OBJ}i(x,y) = \mathrm{abs}\{\mathrm{IFrT}(\mathrm{Eny} + \mathrm{key1_}i + \mathrm{key2_}i);zi;\lambda\}, \tag{16}$$

where IFrT stands for the inverse Fresnel transform. Finally, the compressed 3D scene information is reconstructed by a computer using the CS theory. The recovered 3D scene information is given by

$$\mathrm{OBJ}i(x,y) = \mathrm{CS}^{-1}[\mathrm{C_OBJ}i(x,y);\Phi], \tag{17}$$

where CS^{-1} denotes the decompress process.

3. Experimental results and analysis

To check the validity of the proposed scheme, several numerical simulations have been performed by MATLAB (R2013a), which is executed on a 64-bit computer. By the CGH chromatography,[27] a 3D object can be considered as the integration of many different depth slices of images. In our proposed system, we assume that the input object to be encrypted consists of two level images, binary or gray scale image. Three transparent 3D objects with the same size are presented in Fig. 3. They are located at different distances, $z_1 = 20$ cm, $z_2 = 30$ cm, $z_3 = 40$ cm, from the single detector output plane. The optical wavelength λ is 532.6 nm.

3.1. Encryption and decryption results

We show the encryption results in Fig. 4. The two holograms I_0 and $I_{\pi/2}$ are captured by the single pixel detector when the 3D objects are illuminated by coherent light in the optical setup, which are shown in Figs. 4(a) and 4(b). Moreover, the phase and amplitude distributions of the ciphertext, Eny, are shown in Figs. 4(c) and 4(d), whose size is 180×256, with a compression ratio of 70%.

The decryption process has been shown in Fig. 2. Key 1 shown in Fig. 5(a) is the public phase key to decrypt all objects. Assume that OBJ1 is to be decrypted, the optical fields of the other two objects, excepting OBJ1, are the assistant key, key 2-1 for decrypting OBJ1, which can be achieved by utilizing the process employed previously. Its phase and amplitude distributions are shown in Figs. 5(b1) and 5(b2), respectively. And the corresponding decryption 3D scenes are depicted in Figs. 5(b3) and 5(b4). The phase and amplitude distributions of key 2-2 and the corresponding decrypted 3D scenes of OBJ2 are depicted in Figs. 5(b1) and 5(c4). Figures 5(d1) and 5(d2) show the phase and amplitude distributions of key 2-3 for decrypting OBJ3. Figures 5(d3) and 5(d4) show the decrypted 3D scenes of OBJ3.

From the results obtained, we can clearly see that the image is clearly reconstructed. To evaluate the quality of the reconstructed image, we use the correlation coefficient (CC)

$$\mathrm{CC} = \frac{E\{[f - E(f)][F - E(F)]\}}{\sqrt{E\{[f - E(f)]^2\}E\{[F - E(F)]^2\}}}, \tag{18}$$

where E denotes the expectation value, and f and F denote the original image and the decryption image, respectively. When the compression ratio is 70%, the CC values of all three objects with correct keys are listed in Table 1. In Table 1, there is no CC value below 0.9. It means that the qualities of the decrypted slice images about 3D objects are very high. To further validate the proposed scheme, we compare the CC values

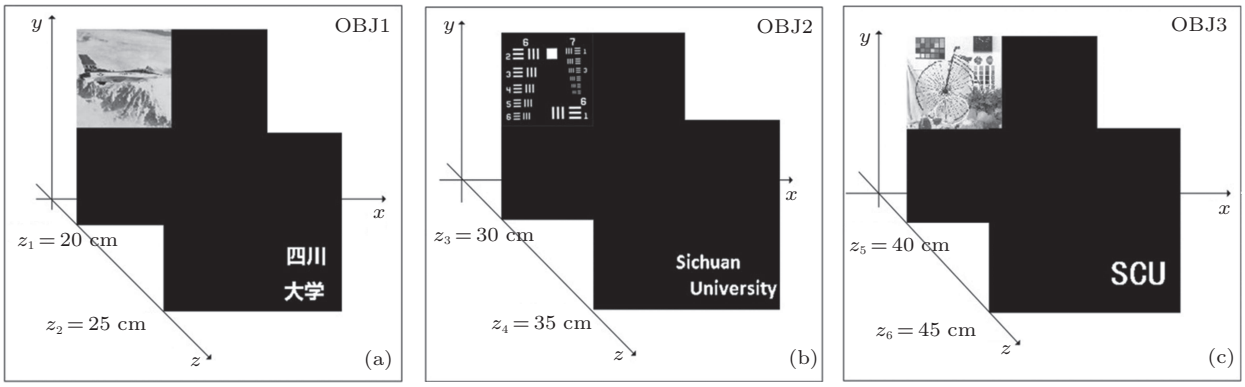


Fig. 3. 3D objects to be encrypted: (a) OBJ1, (b) OBJ2, (c) OBJ3.

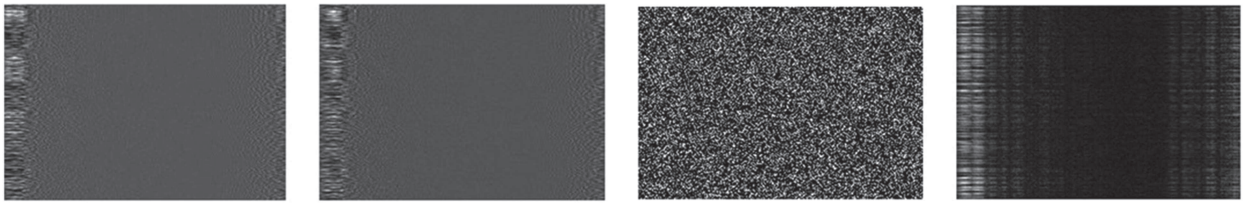


Fig. 4. (a) Hologram I_0; (b) hologram $I_{\pi/2}$; (c) phase distribution of Eny; (d) amplitude distribution of Eny.

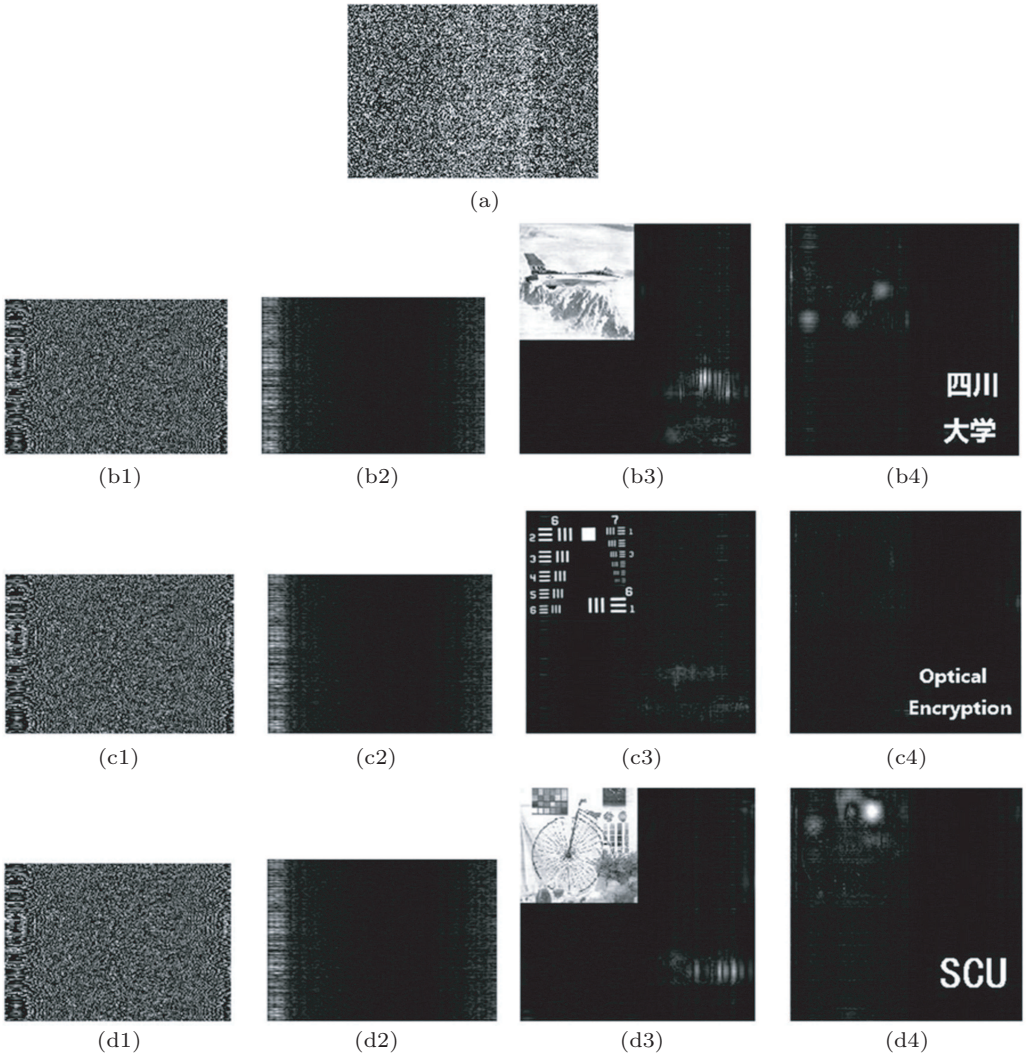


Fig. 5. Simulated results using the proposed method: (a) phase distributions of key 1; (b1) phase distributions of key 2-1; (b2) amplitude distributions of key 2-1; (b3) decrypted image of OBJ1-1; (b4) decrypted image of OBJ1-2; (c1) phase distributions of key 2-2; (c2) amplitude distribution of key 2-2; (c3) decrypted image of OBJ2-1; (c4) decrypted image of OBJ2-2; (d1) phase distribution of key 2-3; (d2) amplitude distribution of key 2-3; (d3) decrypted image of OBJ3-1; (d4) decrypted image of OBJ3-2.

of the proposed scheme with that of Ref. [16], in which the three-step phase shifting method for the multiple 3D objects secure information system was proposed. The simulation results are illustrated in Table 1. The qualities of decryption slice images about 3D objects using our method are slightly better than those from Ref. [16].

Table 1. CC values of the decrypted slice images of 3D objects.

Object	Proposed method		Ref. [16]	
	CC of the first image	CC of the second image	CC of the first image	CC of the second image
OBJ1	0.9979	0.9998	0.9819	0.9958
OBJ2	0.9899	0.9978	0.9889	0.9866
OBJ3	0.9968	0.9986	0.9867	0.9945

3.2. Compression performance

The ratio of a sample size to the original sample size gives the compression ratio ($(M/N)\times 100$). The larger the compression ratio, the worse the image quality. To test the compression performance, we gradually decrease the sample ratio of the proposed scheme by changing the parameter M. To verify the results, the peak signal-to-noise ratio (PSNR) between the original image and decryption image is employed and expressed as

$$\mathrm{PSNR} = 10\log_{10}(255^2/\mathrm{MSE}), \tag{19}$$

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[u(i,j)-v(i,j)]^2, \tag{20}$$

where MSE denotes the mean square error, m and n are the dimensions of the image, $u(i,j)$ is the pixel value of the recovered original image without compression, and $v(i,j)$ is the pixel value of the reconstructed image with compression. Figure 6 shows the relationship between the average values of the PSNR for the decrypted 3D object at different slices and its compression ratio.

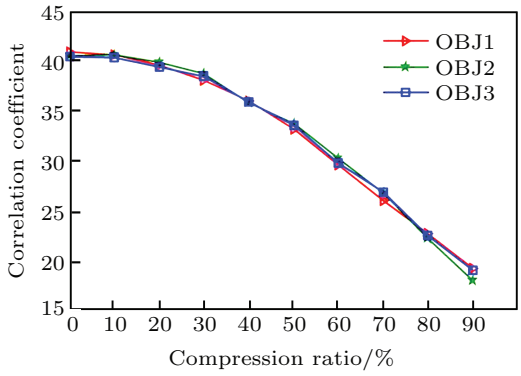


Fig. 6. (color online) Variation of average PSNR versus the sample ratio.

The results show that the reduction of the compression ratio will increase the observed details in the decrypted image. Hence, PSNR also increases. As can be seen from the diagram, when the compression ratio is less than 60%, the PSNR values of the decrypted objects are greater than 30 dB, which means that the quality of the decrypted objects is acceptable.

3.3. Key space and sensitivity analysis

The most important feature for optical encryption is high security of the algorithm. In the proposed system, a total of five secret keys are used: measurement matrix $\boldsymbol{\Phi}$; phase key key 1; assistant key key 2; decryption distance z, and wavelength λ. Taking the OBJ1 for example, figure 7 shows the decrypted 3D scene information of OBJ1 with partial correct keys. The incorrect sensing matrix $\boldsymbol{\Phi}$ is replaced by a random phase mask, and the phase distribution is shown in Fig. 7(a1). The CC values of the decrypted first sliced image and second sliced image of the OBJ1 are 0.11 and 0.16, respectively. The corresponding decrypted images are depicted in Figs. 7(a2) and 7(a3), which are completely noise-like images.

When key 1-1 is the only incorrect key shown in Fig. 7(b1) the CC value of the decrypted first sliced image of the OBJ1 in Fig. 7(b2) is 0.11. Simultaneously, the CC value of the decrypted second sliced image of the OBJ1 in Fig. 7(b2) is 0.16. When assistant decryption key key 2-1 is the only incorrect one as shown in Fig. 7(c1), the CC values of the decrypted first sliced image and second sliced images are 0.47 and 0.42, respectively. The corresponding decrypted images are depicted in Figs. 7(c2) and 7(c3), which are indistinct images.

The wavelength λ of the illuminating beam and diffraction distance z both are important parameters in the encryption. In order to illustrate the relation between the decryption image and the wavelength λ of the illuminating beam and the diffraction distance z, we give the average CC values of the decryption objects at different slices versus different λ and z in Figs. 8(a) and 8(b), respectively. It is easy to find that the CC value reaches maximum only when the values of λ and z are correct. In the case of a small derivation, the CC value decreases quickly and it fails to recognize the original image visually. The high sensitivity results in great difficulty in duplicating the decryption system.

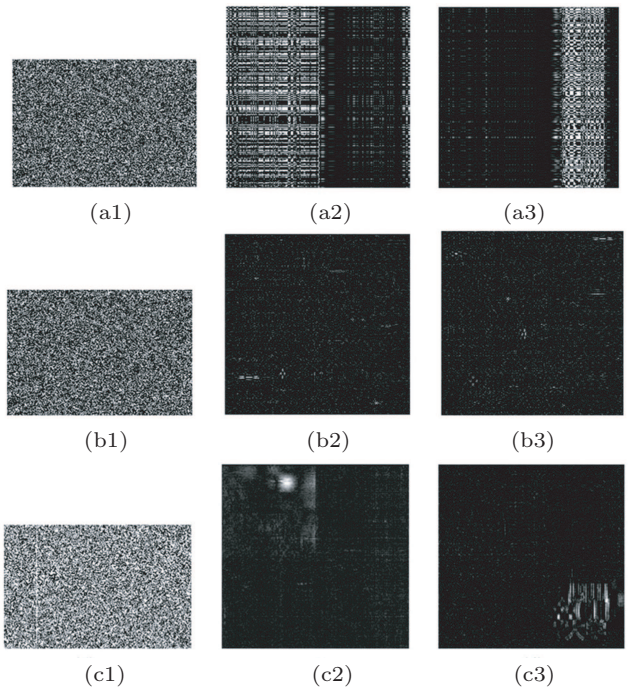


Fig. 7. (a1) Incorrect sensing matrix $\boldsymbol{\Phi}$; (a2) decrypted image of OBJ1-1 with (a1); (a3) decrypted image of OBJ1-2 with (a1); (b1) incorrect key 1-1; (a2) decrypted image of OBJ1-1 with (b1); (b3) decrypted image of OBJ1-2 with (b1); (c1) incorrect key 2-1; (c2) decrypted image of OBJ1-1 with (c1); (a3) decrypted image of OBJ1-2 with (c1).

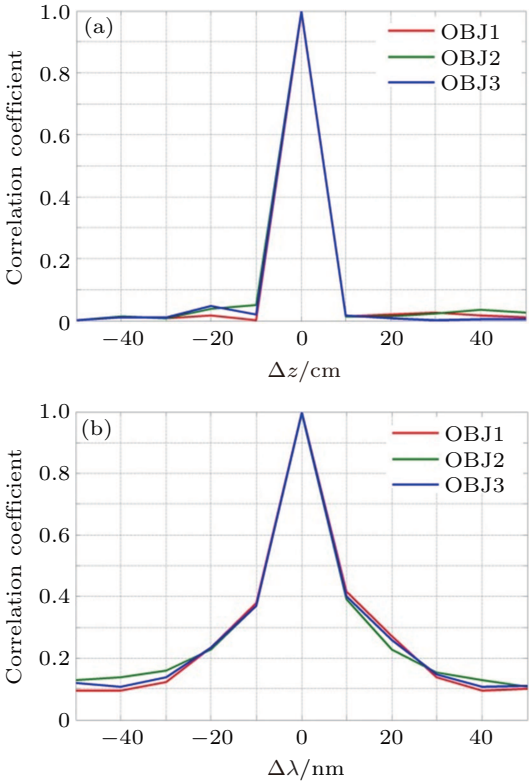
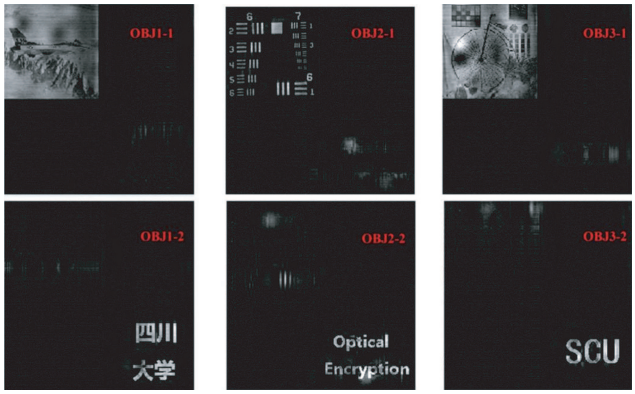


Fig. 8. (color online) Keys analysis of wavelength and diffraction distance: CC curves for (a) $z_1 + \Delta z$; (b) $\lambda + \Delta\lambda$.

3.4. Robustness test against noise of the system

The quality of the decrypted image is associated with its corresponding encrypted image. In this section, we test the robustness of the proposed encryption scheme to additive noise attacks, where Gaussian noise with zero mean is adopted. Q is defined as noise intensity. Figures 9(a)–9(c) show the images reconstructed using the proposed scheme when Q equals 0.5.



(a) (b) (c)

Fig. 9. (color online) Robustness to Gaussian noise with zero mean and variance $Q = 0.5$: (a) OBJ1; (b) OBJ2; (c) OBJ3.

To further validate the proposed scheme, we compare the CC values of the decrypted image with different noise intensities of the proposed scheme with that of Ref. [16].

The calculated CC values are shown in Table 2. Compared with the traditional method, the CC values of the proposed scheme are higher than those of the traditional method under the condition of Gauss noise. As can be seen from the simulation results, the proposed scheme has higher robustness.

Table 2. CC values for decrypted slice images under the occlusion attack.

	Q	Object	First slice image	Second slice image
Proposed	0.1	OBJ1	0.9978	0.9756
	0.1	OBJ2	0.9801	0.9819
	0.1	OBJ3	0.9872	0.9858
	0.3	OBJ1	0.9123	0.9373
	0.3	OBJ2	0.9594	0.9390
	0.3	OBJ3	0.9646	0.9697
	0.6	OBJ1	0.8205	0.8739
	0.6	OBJ2	0.9127	0.8785
	0.6	OBJ3	0.8188	0.9251
Ref. [16]	0.1	OBJ1	0.9082	0.9669
	0.1	OBJ2	0.9567	0.9725
	0.1	OBJ3	0.9249	0.9486
	0.3	OBJ1	0.8311	0.8669
	0.3	OBJ2	0.8919	0.6481
	0.3	OBJ3	0.7975	0.8012
	0.6	OBJ1	0.7118	0.7009
	0.6	OBJ2	0.7245	0.7698
	0.6	OBJ3	0.4821	0.6961

4. Conclusions

In this paper, an efficient multiple 3D information security system is proposed. This method provides an efficient and flexible mode of multiple 3D information encryption and decryption. Each object plays the role of an assistant secret key for the other object to realize the mutual encryption and each 3D object can be decrypted separately. The quality of the decrypted slice image of each object is high according to the CC values. Due to the single-pixel digital holography, the data ciphertext and secret key of this method are effectively reduced and enhanced, respectively. In addition, it is easy to expand the optical device in the case of adding more 3D objects to encrypt. Moreover, the measurement operation serves as a secret key that makes an intruder attack invalid, which means that the system is more secure than the method in Ref. [16]. Simulation results demonstrate that our proposed method can reconstruct the original 3D scene information from under sampling holograms. It is verified that this method has high encryption capacity, data security and system robustness, as well as being able to avoid the influence of overlapping and crosstalk of multiple objects.

References

[1] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[2] Zhang Y D and Zhao S M 2017 *Chin. Phys. B* **26** 054205
[3] Chai X L, Gan Z H, Yuan K, Lu Y and Chen Y R 2017 *Chin. Phys. B* **26** 020504
[4] Ye G D, Huang X L, Zhang Y and Wang Z X 2017 *Chin. Phys. B* **26** 010501
[5] Zhang X Y, Zhang G J, Li X, Ren Y Z and Wu J H 2016 *Chin. Phys. B* **25** 054201
[6] Shi Y, Li T, Wang Y, Gao Q, Zhang S and Li H 2013 *Opt. Lett.* **38** 1425
[7] Zhang Y, Xu B and Zhou N R 2017 *Opt. Commun.* **392** 223
[8] Li X W and Lee I K 2015 *Opt. Laser Eng.* **66** 112
[9] Hong K, Yeom J, Jang C, Hong J and Lee B 2014 *Opt. Lett.* **39** 127
[10] Zhang H, Tan Q and Jin G 2012 *Opt. Eng.* **51** 5801
[11] Ichihashi Y, Nakayama H, Ito T, Masuda N, Shimobaba T, Shiraki A and Sugie T 2009 *Opt. Express.* **17** 13895
[12] Tajahuerce E and Javidi B 2000 *Appl. Opt.* **39** 6595
[13] Matoba O and Javidi B 2004 *Appl. Opt.* **43** 2285
[14] Shiu M T, Chew Y K, Chan H T, Wong X Y and Chang C C 2015 *Appl. Opt.* **54** A84
[15] Kong D, Shen X, Cao L, Zhang H, Zong S and Jin G 2016 *Opt. Commun.* **380** 387
[16] Li W N, Shi C X, Piao M L and Kim N 2016 *Appl. Opt.* **55** 4052
[17] Li W N, Lee S M, Gil S K and Kim N 2017 *Appl. Opt.* **56** 6214
[18] Clemente P, Durán V, Tajahuerce E, Andrés P and Climent V J 2013 *Opt. Lett.* **38** 2524
[19] Yuan S, Liu X, Zhou X and Li Z 2016 *Journal of Modern Optics* **15** 1
[20] Li J, Wang Y. Rong L and Li Y 2013 *Digital Holography and Three-Dimensional Imaging DW2A* 9
[21] Liu J P, Guo C H, Hsiao W J, Poon T C and Tsang P 2015 *Opt. Lett.* **40** 2366
[22] Duarte M F, Davenport M A, Takhar D, Laska J N, Sun T, Kelly K F and Baraniuk R G 2008 *IEEE Signal Processing Magazine* **25** 83
[23] Chan W L, Charan K, Takhar D, Kelly K F, Baraniuk R G and Mittleman D M 2008 *Appl. Phys. Lett.* **93** 121105
[24] Xiao D, Cai H K and Zhen H Y 2016 *Chin. Phys. B* **24** 060505
[25] Zhou, N R, Pan S, Cheng S and Zhou Z 2016 *Optics & Laser Technology* **82** 121
[26] Zhao Y, Hu Y and Liu J 2017 *IEEE T. Instrum. Meas.* **66** 1789
[27] Huang R, Rhee K H and Uchida S 2014 *Multimedia Tools & Applications* **72** 71