SCIENTIFIC REPORTS

OPEN

Optical cryptography with biometrics for multi-depth objects

Aimin Yan[1], Yang Wei[1], Zhijuan Hu[1], Jingtao Zhang[1], Peter Wai Ming Tsang[2] & Ting-Chung Poon[3]

Received: 21 June 2017
Accepted: 12 September 2017
Published online: 11 October 2017

We propose an optical cryptosystem for encrypting images of multi-depth objects based on the combination of optical heterodyne technique and fingerprint keys. Optical heterodyning requires two optical beams to be mixed. For encryption, each optical beam is modulated by an optical mask containing either the fingerprint of the person who is sending, or receiving the image. The pair of optical masks are taken as the encryption keys. Subsequently, the two beams are used to scan over a multi-depth 3-D object to obtain an encrypted hologram. During the decryption process, each sectional image of the 3-D object is recovered by convolving its encrypted hologram (through numerical computation) with the encrypted hologram of a pinhole image that is positioned at the same depth as the sectional image. Our proposed method has three major advantages. First, the lost-key situation can be avoided with the use of fingerprints as the encryption keys. Second, the method can be applied to encrypt 3-D images for subsequent decrypted sectional images. Third, since optical heterodyning scanning is employed to encrypt a 3-D object, the optical system is incoherent, resulting in negligible amount of speckle noise upon decryption. To the best of our knowledge, this is the first time optical cryptography of 3-D object images has been demonstrated in an incoherent optical system with biometric keys.

Information security has become a practical and serious issue with the increasing growth of internet and telecommunications. Optical information encryption techniques have attracted the interest of many researchers because of their unique advantages, such as multi-dimensional capability[1,2]. Since double random phase encoding (DRPE)[3] was proposed, many encryption methods, such as fractional Fourier transform[4], Fresnel transform[5], digital holography[6] and polarization[7], have been further developed in order to enhance cryptosystem security. However, DRPE has been found to be quite vulnerable[8,9]. Recently, optical asymmetric cryptosystems, such as phase-truncated fractional Fourier transform[10] and Yang-Gu algorithm[11], have been proposed to solve the inherent issue in symmetric cryptosystems. Optical asymmetric key cryptosystems break the linearity of the DRPE technique and make the security system more reliable. Subsequently, asymmetric cryptosystems based on gyrator wavelet transform, fractional Fourier transform and joint transform correlator architecture[12–14] have been developed and optical cryptosystem security is further improved.

Biometric information authentication is also emerging as an important research field in the domain of optical security. Tashima *et al.*[15] and Takeda *et al.*[16] have proposed the encryption methods using fingerprint keys with DRPE to avoid some attacks and improve security. In traditional cryptography, key is not strongly linked with its owner. This results in difficulty for the user to remember a long decryption key or in the situation where the private key is lost and hence a new set of private and public keys have to be generated again in the case of asymmetrical cryptography. Biometrics, such as fingerprint, face and iris, is one of the most trustworthy concerns with high degree of assurance for person verification. Hence, researchers are trying to integrate biometrics with cryptography. However, most of the biometric authentication techniques are geared towards encrypting 2-D information such as image and digital data. Practically, there is a growing demand to utilize 3-D information of the object with the advent of 3-D imaging. For example, 3-D information can be encrypted by use of digital holography[17–20]. But it is difficult to encrypt a large 3-D object by conventional digital holography because of the finite size of pixels in a recording CCD camera[21]. Chen *et al.*[22] have demonstrated asymmetric cryptography using 3-D space-based model, and it was shown that conventional 2-D processing can be converted into 3-D space. Yang *et al.*[23] introduced an encryption algorithm for 3-D information using optical asymmetric keys and digital

[1]Key Laboratory of Optoelectronic Material and Device, College of Mathematics and Science, Shanghai Normal University, Shanghai, 200234, China. [2]Department of Electronic Engineering, City University of Hong Kong, Hong Kong, SAR, China. [3]Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, 24061, USA. Correspondence and requests for materials should be addressed to P.W.M.T. (email: eewmtsan@cityu.edu.hk)

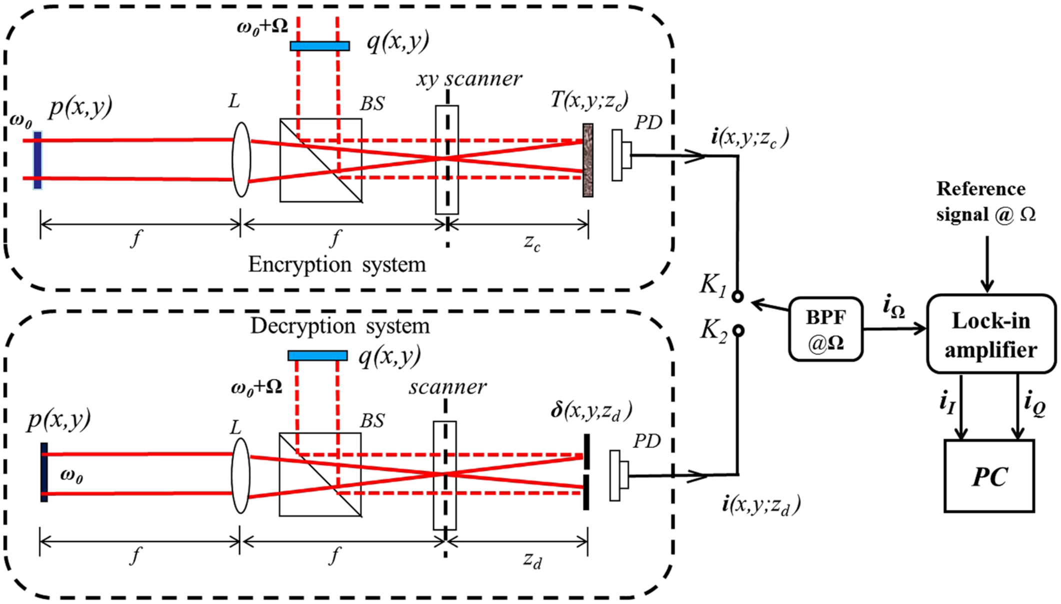

Figure 1. Overall cryptosystem: BPF@Ω is an electronic bandpass filter tuned at frequency Ω.

interferometry. However, most of the optical encryption techniques have been coherent optical techniques which inherently have poor signal-to-noise ratio (S/N) compared to their incoherent counterparts[24]. Poon *et al.*[25] have proposed optical scanning cryptography (OSC) to encrypt information incoherently based on optical scanning holography (OSH)[26]. Its first experiment has been demonstrated recently together with biometric encryption and decryption[9]. Although the S/N of the decrypted image is enhanced, the method has been developed only to the encryption of 2-D planar images.

In this work, we propose novel optical cryptography with biometric keys for encrypting multi-depth 3-D objects. The proposed system is also incoherent, meaning speckles noise is absent from its encryption and decryption of the 3-D object. To our knowledge, it is the first time an optical encryption system with such capabilities is successfully developed and reported. Organization of the paper is given as follows. In the next section, the framework and theory of our cryptographic system are described. Subsequently, we shall describe our proposed method for encrypting 3-D object images based on the cryptographic framework. Next, experimental results are shown to demonstrate the feasibility of our approach, and finally in the last section, we make some concluding remarks.

General theory on proposed cryptosystem

In Fig. 1, we show an overall cryptosystem, where the optical system on the top presents a subsystem of optical encoding or encryption when the switch is at K_1, and the optical system on the bottom shows an optical subsystem for decryption when the switch is at K_2. Note that the two subsystems basically are the same except that in the encryption system, 3-D object image of complex amplitude $T(x, y; z_c)$ to be encrypted, at coding distance z_c away from the *xy* scanner, is scanned with the switch at K_1, whereas in the decryption system, a pin hole, $\delta(x, y; z_d)$, at z_d away from the *xy* scanner, is scanned when the switch is at K_2. The parameter z_d is referred to as the 'decoding distance'. In what follows, we discuss the general principle of the optical system.

Encryption theory. In the encryption system shown in Fig. 1, we have two encoding masks, $p(x, y)$ and $q(x, y)$. In practice, they can be loaded on spatial light modulators in the optical system. $p(x, y)$ and $q(x, y)$ are illuminated by plane waves at temporal frequencies ω_0 and $\omega_0 + \Omega$, respectively. The two fields after the two masks are combined by beamsplitter (*BS*) and projected onto input represented by complex amplitude distribution $T(x, y; z_c)$, which is located $2f + z_c$ away from $p(x, y)$ with f being the focal length of Lens L. Again, z_c is the coding distance. The distance from $q(x, y)$ to the input is given by $z_q = z_{q0} + z_c$. The input is 2-D scanned by the combination of the two fields and this can be done, for example, by projecting the combined optical beams through an *xy* mirror-scanner onto the input, which is shown in Fig. 1. In the system, we have utilized different transforms for the two different encoding masks in order to add complexity to the overall system. We have Fresnel transform of $q(x, y)$ along one optical path and then on the other optical path, we have Fourier transform of $p(x, y)$, that is the spectrum of $p(x, y)$ through Lens L. Therefore, the use of Fresnel transform of q(x, y) and the Fourier transform of $p(x, y)$ are combined to encode the input. Mathematically, the field on input $T(x, y; z_c)$ due to $p(x, y)$ is, besides some constant terms,

$$\begin{aligned}&[\Im\{p(x,\, y)\}_{k_x=k_0x/f,k_y=k_0y/f} * h(x,\, y;\, z_c)]\exp(j\omega_0 t)\\ &=[\tilde{p}\,(k_0x/f,\, k_0y/f)] * h(x,\, y;\, z_c)\exp(j\omega_0 t) = P(x,\, y;\, 2f + z_c)\exp(j\omega_0 t)',\end{aligned} \quad (1)$$

where the definition of Fourier transform is

$$\Im\{g(x, y)\}_{k_x,k_y} = \tilde{g}(k_x, k_y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g(x, y)\exp(jk_x x + jk_y y)dxdy$$

with k_x and k_y denoting spatial frequencies. Symbol * denotes convolution between the two functions[21,26] and $h(x, y; z) = \exp(-jk_0 z)\frac{jk_0}{2\pi z}\exp\left\{\frac{-jk_0(x^2+y^2)}{2z}\right\}$ is the free space impulse response in Fourier optics[21,26]. Now, for the field on input $T(x, y; z_c)$ due to $q(x, y)$, according to Fresnel diffraction, is

$$\begin{aligned}&[q(x, y)_* h(x, y; z_q = 2f + z_c)]\exp[j(\omega_0 + \Omega)t]\\ &=Q(x, y; z_q = 2f + z_c)\exp[j(\omega_0 + \Omega)t]\end{aligned}, \tag{2}$$

where we have assumed equal optical path length (OPL) for both $p(x, y)$ and $q(x, y)$ for simplicity, i.e., we let $z_q = z_{q0} + z_c = 2f + z_c$.

The total scanning field on the object, according to equations (1) and (2) is, therefore, given by

$$S(x, y; z_c) = P(x, y; 2f + z_c)\exp(j\omega_0 t) + Q(x, y; 2f + z_c)\exp[j(\omega_0 + \Omega)t], \tag{3}$$

and the field after the input transparency is $S(x', y'; z_c)T(x' + x, y' + y; z_c)$, where $x = x(t)$ and $y = y(t)$ represent the instantaneous 2-D position of the object during the action of *xy*-scanning. Finally, the photodetector (PD) gives the current output by spatially integrating the intensity:

$$\begin{aligned}&i(x, y; z_c) \propto \int_A |S(x', y'; z_c)T(x' + x, y' + y; z_c)|^2 dx'dy'\\ &= \int_A |\{P(x', y'; 2f + z_c)\exp(j\omega_0 t) + Q(x', y'; 2f + z_c)\exp[j(\omega_0 + \Omega)t]\}\\ &\times T(x' + x, y' + y; z_c)|^2 dx'dy',\end{aligned} \tag{4}$$

where A is the active area of the PD. After bandpass filtering of $i(x, y; z_c)$ at the heterodyne frequency Ω, the heterodyne current is

$$i_\Omega(x, y; z_c) \propto \mathrm{Re}[i_{\Omega p}(x, y; z_c)\exp(j\Omega t)], \tag{5}$$

where

$$i_{\Omega p}(x, y; z_c) = \int_A P^*(x', y'; 2f + z_c)Q(x', y'; 2f + z_c)|T(x' + x, y' + y; z_c)|^2 dx'dy'] \tag{6}$$

is the current phasor, which contains the amplitude and phase information of $i_\Omega(x, y; z_c)$.

The phasor current above can be expressed in terms of correlation as follows:

$$i_{\Omega p}(x, y; z_c) = P(x, y; 2f + z_c)Q^*(x, y; 2f + z_c) \otimes |T(x, y; z_c)|^2, \tag{7}$$

where correlation of $g_1(x, y)$ and $g_2(x, y)$ is defined as

$$g_1(x, y) \otimes g_2(x, y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g_1^*(x', y')g_2(x + x', y + y')dx'dy'.$$

Taking the Fourier transform of equation (7), we have

$$\Im\{i_{\Omega p}(x, y; z_c)\} = \Im^*\{P(x, y; 2f + z_c)Q^*(x, y; 2f + z_c)\}\Im\{|T(x, y; z_c)|^2\}.$$

We can now define the optical transfer function (OTF) of the system as

$$\begin{aligned}OTF(k_x, k_y; z_c) &= \Im\{i_{\Omega p}(x, y; z_c)\}/\Im\{|T(x, y; z_c)|^2\}\\ &= \Im^*\{P(x, y; 2f + z_c)Q^*(x, y; 2f + z_c)\}\end{aligned}. \tag{8}$$

So the output heterodyne current from the PD can be expressed as, using equation (8),

$$\begin{aligned}&i_\Omega(x, y; z_c) \propto \mathrm{Re}[i_{\Omega p}\exp(j\Omega t)]\\ &=\mathrm{Re}[\Im^{-1}\{\Im\{|T(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\}\exp(j\Omega t)]]\end{aligned}. \tag{9}$$

The amplitude and phase of the above current can be extracted conveniently by a lock-in amplifier as shown in Fig. 1 and the two final outputs, the in-phase component $i_I(x, y; z_c)$ and the quadrature component $i_Q(x, y; z_c)$ are as follows:

$$i_I(x, y; z_c) = \mathrm{Re}\,[\Im^{-1}\{\Im\{|T(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\}] \tag{10a}$$

$$i_Q(x, y; z_c) = \mathrm{Im}\,[\Im^{-1}\{\Im\{|T(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\}]. \tag{10b}$$

A complex record of the coded or encrypted object can be constructed in a computer according to the following complex relation:

$$\begin{aligned} & i_I(x,\, y;\, z_c) + j i_Q(x,\, y;\, z_c) \\ & \quad = \Im^{-1}\{\Im\{|T(x,\, y;\, z_c)|^2\} OTF(k_x,\, k_y;\, z_c)\} = H_C^{en}(x,\, y;\, z_c) \end{aligned} \cdot \tag{11}$$

$H_C^{en}(x,\, y;\, z_c)$ is called the encrypted hologram of the 3-D object, $|T(x, y; z_c)|^2$. It is clear from the above that the object intensity distribution, i.e., $|T(x, y; z_c)|^2$, is being processed and, therefore, the optical system is incoherent. The spectrum of the object is now processed or encrypted by the OTF given by equation (8).

The OTF in equation (8) can be expressed in terms of the two coding masks, $p(x, y)$ and $q(x, y)$, by using expressions $P(x, y; 2f + z_c)$ and $Q(x, y; 2f + z_c)$ from equations (1) and (2), respectively into equation (8). After some lengthy manipulations, we have

$$\begin{aligned} OTF(k_x,\, k_y;\, z_c) = {} & e^{j\frac{z_c+2f}{2k_0}(k_x^2+k_y^2)} \\ & \times \iint p^*(x',\, y') \tilde{q}\left(-\frac{k_0}{f}x' - k_x,\, -\frac{k_0}{f}y' - k_y\right) e^{j\frac{k_0}{f}({x'}^2+{y'}^2)} e^{j\frac{z_c+2f}{f}(x'k_x+y'k_y)} dx'dy' \end{aligned} \cdot \tag{12}$$

This *OTF* is able to record holographically the encrypted object, located at a distance of $z_c + f$ distance away from Lens *L*, as indicated by the quadratic phase term, $e^{j\frac{z_c+2f}{2k_0}(k_x^2+k_y^2)}$, in front of the integral[26]. The remaining integral term is responsible for coding or encrypting the object, and the degree of encryption can be manipulated by masks $p(x, y)$ and $q(x, y)$. The overall effect is that we have an encrypted complex hologram, $H_C^{en}(x,\, y;\, z_c)$, of object $|T(x, y; z_c)|^2$ according to equations (11) and (12).

Decryption theory. The decryption process for recovering the object image $|T(x, y; z_c)|^2$ from the encrypted hologram $H_C^{en}(x,\, y;\, z_c)$ is outline as follows. To begin with, we have assumed the *unity condition* given by $OTF^*(k_x, k_y; z_d)$ $OTF(k_x, k_y; z_d) = 1$, where z_d is the decoding distance and $z_c \in z_d$, i.e., z_c belongs to z_d. As such, it can be easily inferred from equation (11) that the original object $|T(x, y; z_c)|^2$ can be recovered by multiplying the Fourier transform of the encrypted data $H_C^{en}(x,\, y;\, z_c)$ with the conjugate of the optical transfer function evaluated at decoding distance $z_d = z_c$, i.e.,

$$\begin{aligned} & \Im^{-1}\{\Im\{H_c^{en}(x,\, y;\, z_c)\} OTF^*(k_x,\, k_y;\, z_d) | z_d = z_c\} \\ & \quad = \Im^{-1}\{\Im\{|T(x,\, y;\, z_c)|^2\} OTF(k_x,\, k_y;\, z_c) OTF^*(k_x,\, k_y;\, z_c)\} \cdot \\ & \quad = \Im^{-1}\{\Im\{|T(x,\, y;\, z_c)|^2\}\} = |T(x,\, y;\, z_c)|^2 \end{aligned} \tag{13}$$

The function $OTF^*(k_x, k_y; z_c)$, which encapsulates the pair of masks $p(x, y)$ and $q(x, y)$, is needed in order to decrypt the information. To determine $OTF^*(k_x, k_y; z_c)$ (assuming, $p(x, y)$, $q(x, y)$, z_c are available) for recovering $|T(x, y; z_c)|^2$, we first obtain a pin hole hologram $H^\delta(k_x, k_y; z_d = z_c)$ by scanning a pin hole with the system shown in Fig. 1 when the switch is at K_2. From equation (11), it can be seen that the pin hole hologram can be derived by replacing the term $|T(x, y; z_c)|^2$ with the pin hole function denoted by $\delta(x, y; z_d)$, i.e., $|T(x, y; z_c)|^2 = \delta(x, y; z_d)$ with $z_c = z_d$, resulting in a pin hole hologram given by

$$\begin{aligned} H^\delta(x,\, y;\, z_d) = {} & i_I(x,\, y;\, z_d) + j i_Q(x,\, y;\, z_d) = \Im^{-1}\{\Im\{\delta(x,\, y;\, z_d)\} OTF(k_x,\, k_y;\, z_d)\} \\ & = \Im^{-1}\{OTF(k_x,\, k_y;\, z_d)\} \end{aligned},$$

thus giving

$$OTF^*(k_x,\, k_y;\, z_d) = \Im\{H^\delta(x,\, y;\, z_d)\}^*.$$

Hence, $OTF^*(k_x, k_y; z_d)$, to be used in equation (13), is derived from the pin hole hologram. From the above equation and equation (13), we can infer that the encrypted image can be recovered by convolving the encrypted hologram, $H_C^{en}(x,\, y;\, z_c)$, with the pinhole hologram, $H^\delta(x, y; z_c)$, i.e., it can be shown readily that

$$\begin{aligned} & H^\delta(x,\, y;\, z_d = z_c) \otimes H_C^{en}(x,\, y;\, z_c) \\ & \quad = \Im^{-1}\{\Im\{|T(x,\, y;\, z_c)|^2\} OTF(k_x,\, k_y;\, z_c) OTF^*(k_x,\, k_y;\, z_c)\}, \\ & \quad = |T(x,\, y;\, z_c)|^2 \end{aligned} \tag{14}$$

where $\otimes$ denotes correlation involving *x* and *y*[21,26]. Equation (14) expresses the essential feature of the proposed technique succinctly. We simply obtain two holograms, $H_C^{en}(x,\, y;\, z_c)$ and $H^\delta(x,\, y;\, z_c)$, experimentally for the overall encryption and decryption process.

In this Section, we have discussed the encryption and decryption of a planar image. In the next Section we shall describe how our proposed method can be extended to optical cryptography of 3-D object images with the incorporation of biometrics information.

Optical cryptography with biometrics on 3-D object images

To start with, we would like to explain the extension of our proposed method to biometric optical cryptography.

Optical cryptography with biometrics.

In order to allow for biometric authentication, in the encryption system the *encryption key* $q(x, y)$, is derived from the product of the message sender's fingerprint $FP_1(x, y)$, and a random phase mask $RPM_1(x, y)$, i.e., $q(x, y) = FP_1(x, y)\ RPM_1(x, y)$. This can be realized optically if we stack two spatial light modulators together, one for the fingerprint and the other for the phase mask. The other mask, $p(x, y)$, again can be treated the same way as $p(x, y) = FP_2(x, y)\ RPM_2(x, y)$, where $FP_2(x, y)$ is the message receiver's fingerprint, and $RPM_2(x, y)$ is another random phase mask. $RPM_1(x, y)$ and $RPM_2(x, y)$ are two independent random functions that allow the system to be of high security. Both random phase masks can be preset in the encryption and decryption systems, so that the message sender and the message recipient do not have to remember or keep them to avoid the lost-key situation.

To further enhance the security of the cryptographic system, the message sender's fingerprint information $q(x, y)$ (hereafter referred to as the 1st key) is shared in advance with the message receiver. The 2nd key $p(x, y)$ is only sent to the sender when the recipient request the sending of an encrypted image. With this additional measure, the encrypted hologram cannot be decrypted even if one possessed the 1st key from the sender through theft or other illegitimate means.

Since fingerprints, $FP_1(x, y)$ and $FP_2(x, y)$, are of amplitude information, the use of $p(x, y) = FP_2(x, y)\ RPM_2(x, y)$ and $q(x, y) = FP_1(x, y)\ RPM_1(x, y)$ in Eq. (12) will not meet the unity condition as the obtained *OTF* will have amplitude distribution. To overcome the issue, let us work on Eq. (14) by noticing that the OTF given by Eq. (12) is complex in general and we could write $OTF(k_x, k_y; z_c) = \mathrm{A}(k_x, k_y; z_c)e^{j\theta}((k_x, k_y; z_c))$. In light of this, by taking the Fourier transform of Eq. (14), we have

$$\Im\{H^{\delta}(x, y; z_d = z_c) \otimes H_C^{en}(x, y; z_c)\} = \Im\{|T(x, y; z_c)|^2\}\mathrm{A}^2(k_x, k_y; z_c),$$

which can be manipulated to give

$$|T(x, y; z_c)|^2 = \Im^{-1}\{\Im\{H^{\delta}(x, y; z_d = z_c) \otimes H_C^{en}(x, y; z_c)\}/\mathrm{A}^2(k_x, k_y; z_c)\}. \tag{15}$$

Under this situation, we need to know the encrypted hologram, $H_C^{en}(x, y; z_c)$, the pinhole hologram, $H^{\delta}(x, y; z_c)$ as well as $\mathrm{A}^2(k_x, k_y; z_c)$ in order to perfectly decrypt $|T(x, y; z_c)|^2$. The knowledge of $\mathrm{A}(k_x, k_y; z_c)$ can be obtained experimentally through the pin hole hologram $H^{\delta}(x, y; z_d = z_c)$ as

$$\mathrm{A}(k_x, k_y; z_c) = |\Im\{H^{\delta}(x, y; z_d = z_c)\}| = |OTF(k_x, k_y; z_c)|. \tag{16}$$

Hence with the inclusion of the term $\mathrm{A}^2(k_x, k_y; z_c)$ in order to perfectly decrypt the image, we call this process as the compensation process.

Optical cryptography on 3-D object images.

We model a 3-D object images as a collection of planar objects as $\sum_{m=1}^{M}|T_m(x, y; z_m)|^2$, where $|T_m(x, y; z_m)|^2$ is the 2-D intensity distribution at various axial depths, z_m, i.e., it is the sectional images of the 3-D object. Hence, for 3-D objects, $H_C^{en}(x, y)$ becomes, according to Eq. (11),

$$H_C^{en}(x, y) = \Im^{-1}\left\{\sum_{m=1}^{M}\left\{\Im[|T_m(x, y; z_m)|^2]OTF(k_x, k_y; z_m)\right\}\right\}. \tag{17}$$

So in the case of encrypting a 3-D object, we have many decoding distances z_m. To extract or decrypt a specific transverse plane at z_k, where $k = [1, M]$, we first record the pinhole hologram $H^{\delta}(x, y; z_k)$ at $z_d = z_k$ in the decryption stage, and then correlate it with the encrypted hologram as

$$\begin{aligned} &H^{\delta}(x, y; z_d = z_k) \otimes H_C^{en}(x, y) \\ &= \Im^{-1}\left\{\sum_{m=1}^{M}\left\{\Im[|T_m(x, y; z_m)|^2]OTF(k_x, k_y; z_m)\right\}OTF^*(k_x, k_y; z_k)\right\} \quad . \\ &= |T_k(x, y; z_k)|^2 + \Im^{-1}\left\{\sum_{m\neq k}^{M}\left\{\Im[|T_m(x, y; z_m)|^2]OTF(k_x, k_y; z_m)\right\}OTF^*(k_x, k_y; z_k)\right\} \end{aligned} \tag{18}$$

From equation (18), the first term of the expression on the right-hand-side is the full recovery of the sectional image of the original object image at z_k, while the rest of the terms are defocused noise. By repeating the above process from $k = 1$ to $k = M$, all the sectional images of the object can be recovered. We will show experimental results in the next section.

Experimental results

In order to verify the feasibility of the proposed optical cryptosystem, the proof-of-principle experiment has been implemented. The experimental setup is shown in Fig. 2.

A laser at frequency ω_0 is used to split into two beams. The laser's wavelength is 632.8 nm with laser power of 15 mW. The two masks $q(x, y)$ and $p(x, y)$ are illuminated by the laser at frequency $\omega_0 + \Omega_1$ and $\omega_0 + \Omega_2$, respectively. Two acousto-optic modulators, AOM$_1$ and AOM$_2$, operating at frequencies Ω_1 and Ω_2, are used to upshift the laser beam frequency at ω_0, to $\omega_0 + \Omega_1$ and $\omega_0 + \Omega_2$, respectively. The heterodyne frequency is at

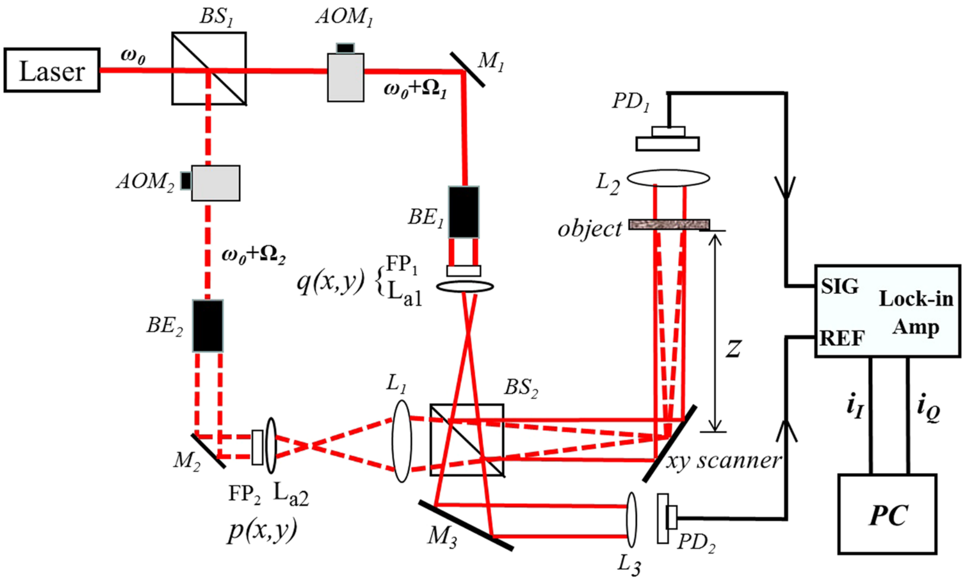

Figure 2. Experimental setup for the optical cryptosystem ($BS_{1,2}$: beam splitter, L_1: Fourier transform lens, L_2: a lens for collecting all the optical energy onto photodetector PD_1, which gives the scanned heterodyne signal. The output of photodetector PD_2 gives a heterodyne frequency as a reference signal to the lock-in amplifier).

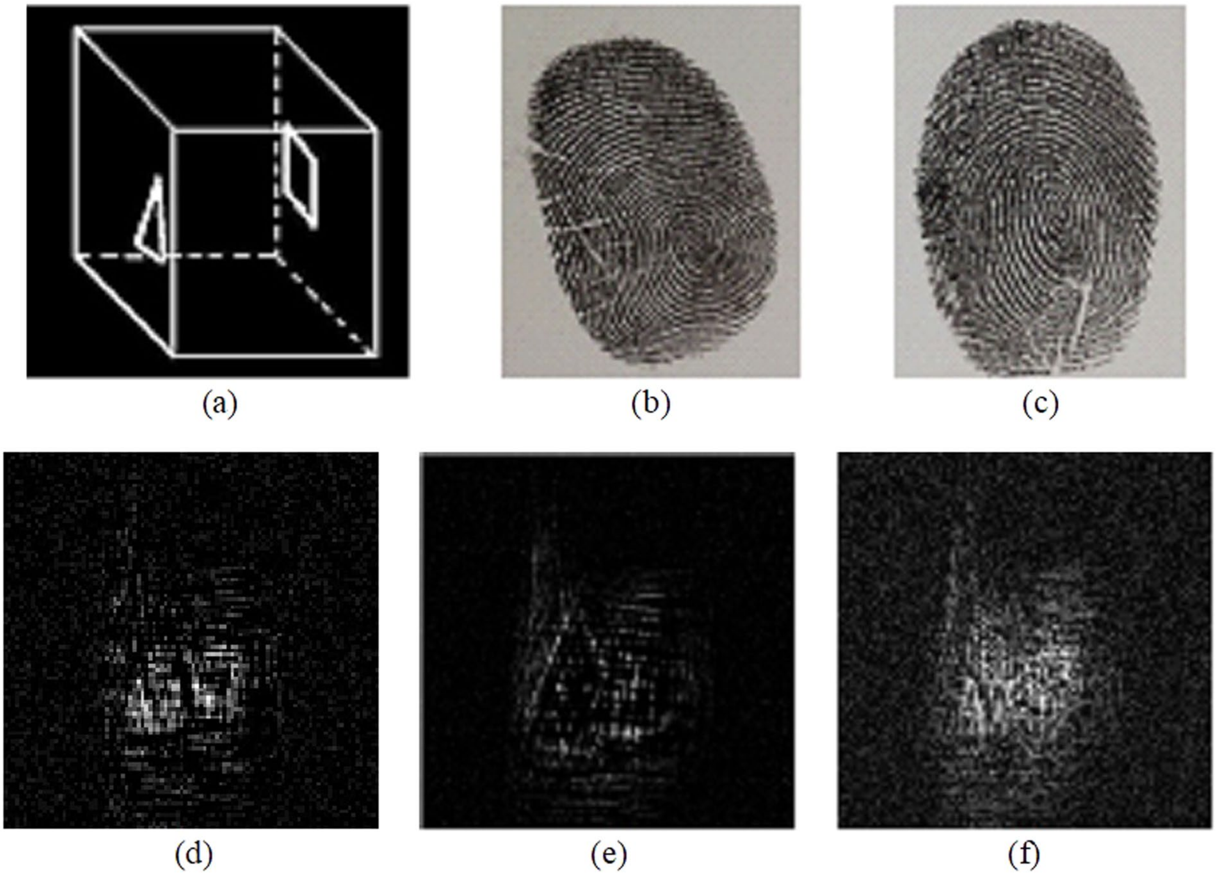

Figure 3. (**a**) 3-D object to be encrypted, (**b**) message sender's fingerprint (**c**) message receiver's fingerprint, (**d**) Real part of encrypted complex hologram $H_C^{en}(x,\ y)$, (**e**) Imaginary part of encrypted complex hologram $H_C^{en}(x,\ y)$, and (**f**) intensity distribution of the encrypted complex hologram.

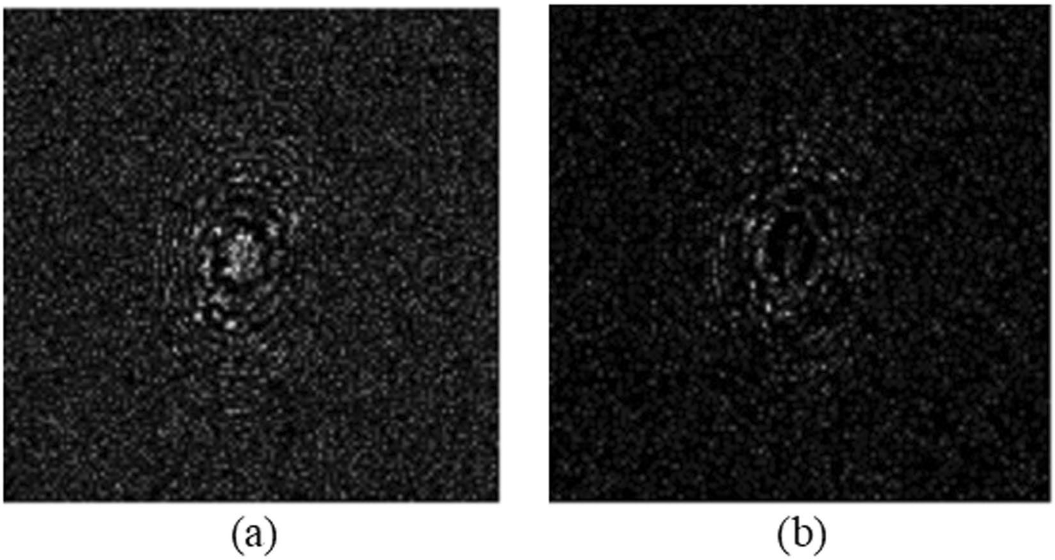

Figure 4. (**a**) Real part, and (**b**) imaginary part of the pinhole hologram measured at decoding distance $z_{d1} = 30$ cm, i.e., $H^{\delta}(x, y; z_{d1} = 30\,\text{cm})$.

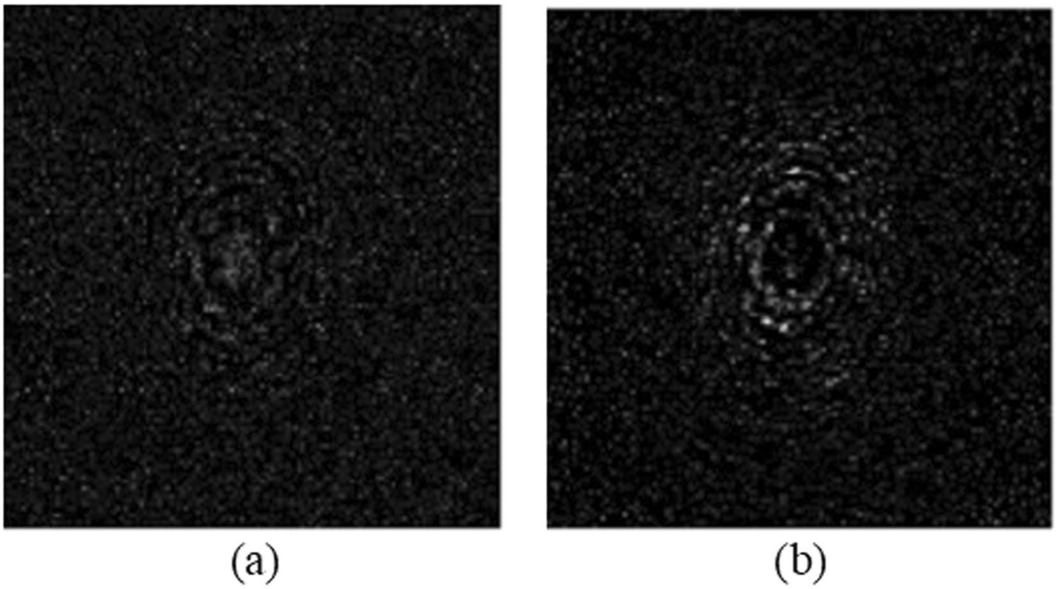

Figure 5. (**a**) Real part, and (**b**) imaginary part of the pinhole hologram measured at decoding distance $z_{d2} = 35.5$ cm, i.e., $H^{\delta}(x, y; z_{d2} = 35.5\,\text{cm})$.

$(\Omega_1 - \Omega_2)/2\pi = 25$ kHz. The two masks $p(x, y)$ and $q(x, y)$ in general can be implemented by SLMs displaying the fingerprint images and random phase masks. However, owing to the current resource limitation in our laboratory, we simply make a proof-of-concept study with two lenses (L_{a1} and L_{a2} with focal length of $f_{a1} = 75.6$mm and $f_{a2} = 150$ mm, respectively) generating quadratic phase modulation instead of random phases. Hence, $q(x, y) = FP_1(x, y)\exp[j\pi(x^2 + y^2)/(\lambda f_{a1})]$ and $p(x, y) = FP_2(x, y)\exp[j\pi(x^2 + y^2)/(\lambda f_{a2})]$. Again $FP_1(x, y)$ is the message sender's fingerprint, and $FP_2(x, y)$ is the message receiver's fingerprint. In the experiments, the fignerprints are in the form of transparencies. BE_1 and BE_2 are two expanders so that the output of them will give uniform plane waves illuminating the two masks $q(x, y)$ and $p(x, y)$. The size of fingerprint images is a transparency of about 1.4 cm × 1.8 cm, and the focal length of Fourier transform lens L_1 is 300 mm.

Figure 3(a) shows a 3-D object to be encrypted, consisting of a triangle and a square separated by 5.5 cm along the depth of the object. "Δ" is located at $z = 30$ cm and "□" at $z = 35.5$ cm. The 3-D object is approximately $1 \times 1 \times 5.5\,\text{cm}^3$ and is transmissive on an opaque background with an opening linewidth of about 100 μm. Figure 3(b) shows the message sender's fingerprint. Figure 3(c) shows the message receiver's fingerprint, and

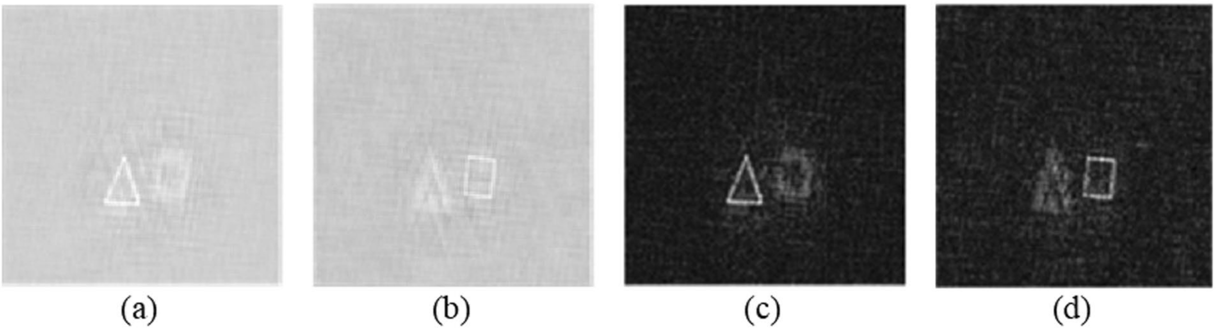

Figure 6. Decrypted sectional images using the pinhole holograms measured at (**a**) $z_{d1} = 30$ cm and (**b**) $z_{d2} = 35.5$ cm for unprocessed decrypted images when the unity condition is not met for fingerprint images, and at (**c**) $z_{d1} = 30$ cm and (**d**) $z_{d2} = 35.5$ cm for processed decrypted images.

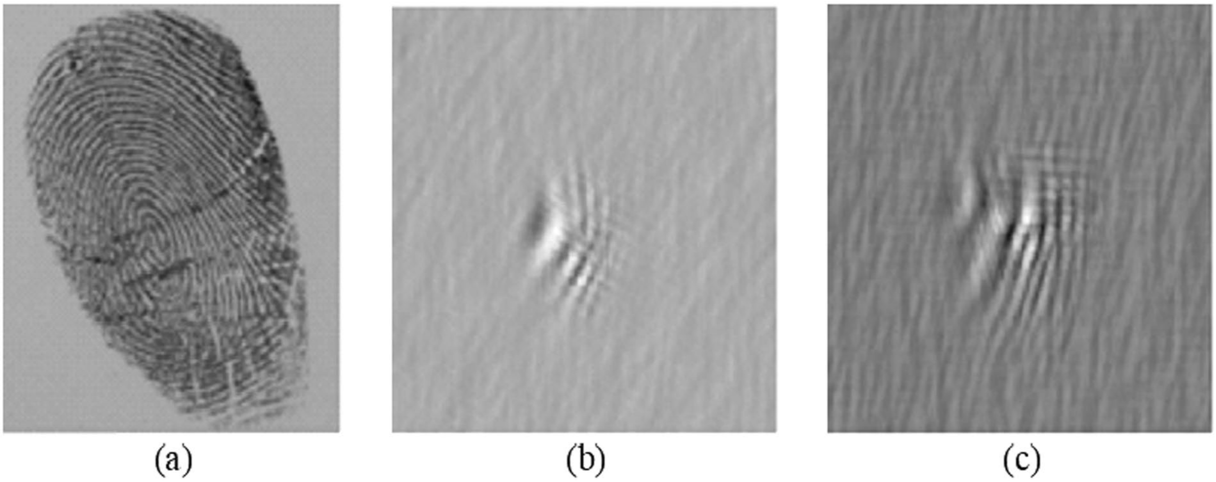

Figure 7. (**a**) Fingerprint as wrong decryption key, the decrypted images using the pinhole holograms generated by the wrong decryption key at the position of (**b**) $z_{d1} = 30$ cm, and (**c**) $z_{d2} = 35.5$ cm.

Fig. 3(d),(e),(f) show the real part, the imaginary part and the intensity of the encrypted complex hologram, respectively, which are generated from the in-phase and quadrature-phase signals [see Eq. (11)]. It can be seen from Fig. 3(f) that the pattern of the object is seriously disturbed and no useful information about the original object can be identified.

From the developed decryption theory, in the decryption stage, we need to find the pin hole hologram. In light of it, we use a pinhole of 0.28 mm in diameter to replace the object and record the pinhole holograms at the corresponding decoding distances of $z_{d1} = 30$ cm and $z_{d2} = 35.5$ cm. In this case, the message sender's fingerprint (see Fig. 3b) has been sent to the decryption stage and the message receiver's fingerprint [see Fig. 3(c)] is the decryption key. Each pinhole hologram at different decoding distances becomes the decrypting hologram for that distance as shown in Eq. (18). The real and imaginary parts of the pin holograms for $z_{d1} = 30$ cm and $z_{d2} = 35.5$ cm are shown in Figs 4 and 5, respectively.

Figure 6 shows the decrypted sectional images at the decoding distances $z_{d1} = 30$ cm and $z_{d2} = 35.5$ cm. For Fig. 6(a),(b), since the fingerprint images do not satisfy the unity condition, i.e., $OTF^{*}(k_x, k_y; z_d = z_c)OTF(k_x, k_y; z_c) \neq 1$, the effect of low contrast of the decrypted images is obvious. In obtaining Fig. 6(a),(b), we simply correlate the pin hole hologram, $H^{\delta}(x, y; z_d = z_c)$, with the encrypted hologram, $H_C^{en}(x, y; z_c)$. Figures 6 (c),(d) show the processed decrypted image according to Eq. (15) to overcome the fact that the unity condition is not met for fingerprint images, in that $A^2(k_x, k_y; z_c)$, derived from the pin hologram hologram [see Eq. (16)], is used to perform the compensation process we discussed in Eq. (15). Note that pattern "Δ" is focused at the location of $z_{d1} = 30$ cm and the decrypted image is blurred elsewhere, corresponding to out-of-focus haze in 3-D imaging. Similarly, pattern "□" is focused at the location of $z_{d2} = 35.5$ cm with out-of-focus haze around the focused image. Hence, we have demonstrated that 3-D object can be encrypted and its sectional images can be decrypted in the proposed cryptosystem.

We have also examined experimentally the proposed system by using different fingerprints for decryption. In the experiment, the encryption system and encryption parameters are exactly the same as before. But, in the decryption process, different fingerprint image is used along with Lens L_{a2} taken away. Figure 7(a) shows the wrong fingerprint image used in the decryption system. Figure 7(b),(c) show the decrypted images using the

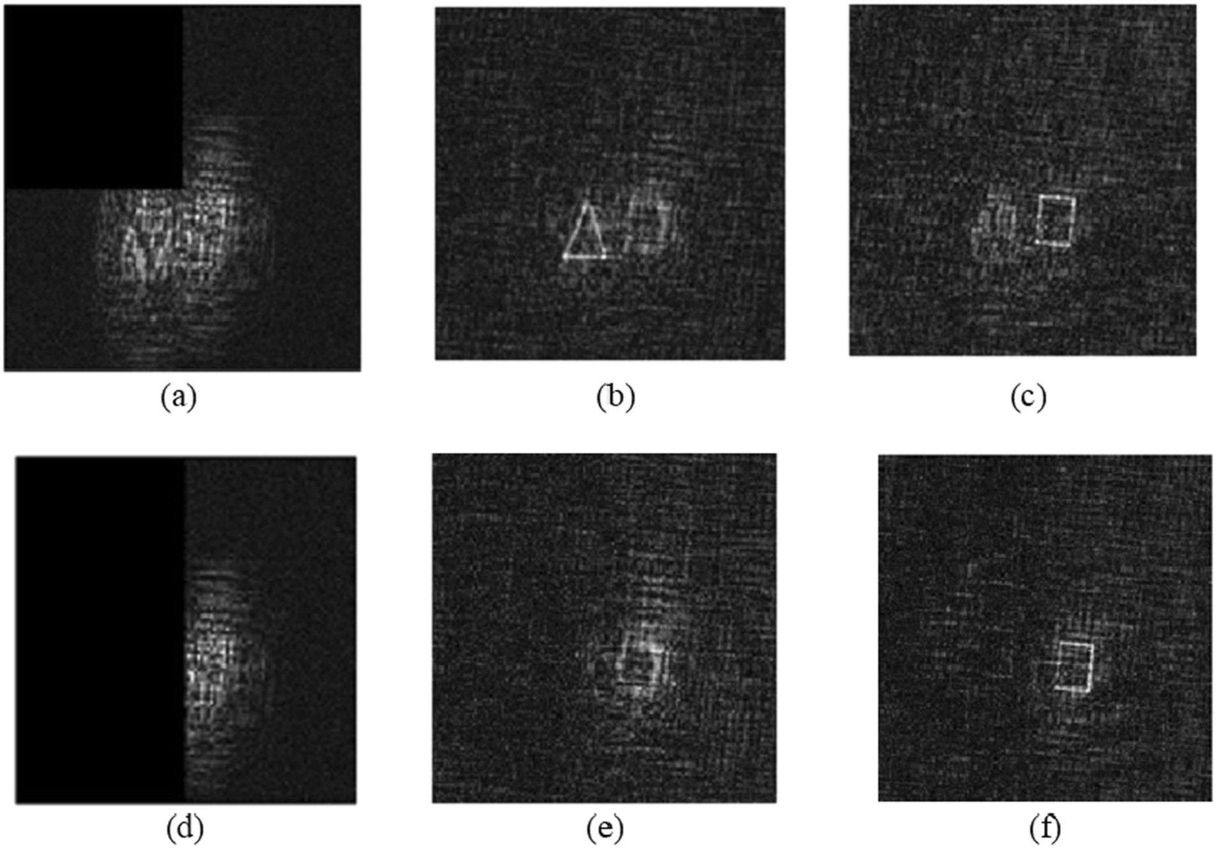

Figure 8. Occlusion results for the decrypted images with different degrees of occlusion. (**a**) with 25% occlusion (blanking the second quadrant of the hologram), (**b**) corresponding decrypted image from (**a**) at decoding distance z_1, (**c**) corresponding decrypted image from (**a**) at decoding distance z_2, (**d**) with 50% occlusion, i.e., blanking half (left side) of the hologram, (**e**) corresponding decrypted image from (**d**) at decoding distance z_1, and (**f**) corresponding decrypted image from (**d**) at decoding distance z_2.

pinhole holograms generated by the wrong fingerprint at two positions of $z_{d1} = 30$ cm and $z_{d2} = 35.5$ cm, respectively. We notice that although the decoding distance is correct, the object cannot be correctly decrypted and reconstructed because the wrong fingerprint key generates the wrong pinhole holograms for decryption. The original secret image cannot be deciphered even the encryption key is known by attackers. As a result, high security against illegal attacks can be obtained by the proposed cryptosystem.

We would also like to make a brief evaluation and assessment on the vulnerability of our method towards plaintext attacks. From Eq. (11) we can infer that theoretically, the encryption key will be deduced based on a pair of known, planar images $|T_1(x, y; z_c)|^2$ and $|T_2(x, y; z_c)|^2$, and their encrypted holograms $H_{C1}^{en}(x, y, z_c)$ and $H_{C2}^{en}(x, y, z_c)$. Both holograms are assumed to be encrypted at the same distance z_c. The process of deducing the encryption key is outlined as follows. First we compute the difference between the two encrypted holograms, each represented with Eq. (11), as

$$\begin{aligned} H_{diff} &= H_{C1}^{en}(x, y, z_c) - H_{C2}^{en}(x, y, z_c) \\ &= \Im^{-1}\{\Im\{|T_1(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\} - \Im^{-1}\{\Im\{|T_2(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\}^{\cdot} \end{aligned} \tag{19}$$

Next we apply Fourier transform to both sides of the above equation, which results in

$$\Im\{H_{diff}\} = \{\Im\{|T_1(x, y; z_c)|^2\}OTF(k_x, k_y; z_c)\} - \Im\{|T_2(x, y; z_c)|^2 OTF(k_x, k_y; z_c)\}. \tag{20}$$

Rearranging the terms in Eq. (20), the encryption function can be deduced, as given by

$$OTF(k_x, k_y; z_c) = \frac{\Im\{H_{diff}\}}{\Im\{|T_1(x, y; z_c)|^2\} - \Im\{|T_2(x, y; z_c)|^2\}}. \tag{21}$$

As such if the intensity images are accidentally exposed through theft or other hacking activities, there is a good chance that the encryption key will also be deduced with Eqs (19–21). However, this kind of attack is difficult, if not impossible to achieve in practice, as the object that is being encrypted is directly converted into the encrypted hologram with the proposed system. In another words, the intensity image of the object is never recorded physically, and hence unknown even to the person who is performing the encryption.

While resistance to occlusion is, in general, not mandatory in encryption, in any case, we have performed a couple of cases rather than exhaustive investigation to provide some indication of the robustness of the proposed technique. According to our actual situation in the experiment, the decrypted images at decoding distance $z_1 = 30$ cm and $z_2 = 35.5$ cm are shown in Fig. 6(c),(d)). We define the mean square error (MSE) as

$$\mathrm{MSE}(z) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[|I_o(i,\, j;\, z) - I_r(i,\, j;\, z)|]^2, \tag{22}$$

where $I_o(i, j; z)$ is a part of the decrypted image from the encrypted hologram without occlusion, $I_r(i, j; z)$ is a part of the decrypted image from the occluded encrypted hologram with $z = z_1$ or z_2 based on the decoding distance; (i, j) denotes pixel positions. $(M \times N)$ denotes the total number of pixels of the image we have selected on the reconstruction plane. In our calculation, we have used $M = N = 64$. Figure 8 shows the results for two kinds of occlusion.

When one-fourth of the encrypted hologram occluded at the top left corner (Fig. 8(a)), the calculated $\mathrm{MSE}(z_1)$ and $\mathrm{MSE}(z_2)$ values between the decrypted images without occlusion (Fig. 6(c),(d)) and the corresponding decrypted images with occlusion (Fig. 8(b),(c)) using all the correct keys are 0.264 and 0.199, respectively. It is shown that the decrypted images using the pinhole holograms at z_1 and z_2 can be recognized in the case of 25% occlusion of the encrypted hologram. When half of the encrypted hologram is occluded (Fig. 8(d)), the corresponding decrypted images with occlusion have the MSE values of $\mathrm{MSE}(z_1) = 3.478$ and $\mathrm{MSE}(z_2) = 0.195$, respectively for Fig. 8e,f). In this case, we observe that the object (triangle) cannot be decrypted at the decoding distance z_1 in the case of 50% occlusion because most of the hologram of the "triangle" has been occluded. But at the decoding distance z_2, the decrypted image of the "square" can be recognized but with some errors.

Concluding remarks

We have proposed a cryptosystem for 3-D object images based on the optical heterodyne technique and biometric fingerprint keys. With our proposed method, a 3-D multi-depth object image can be encrypted into a complex encrypted hologram. Subsequently, the 3-D object image can be recovered from the encrypted hologram by correlating the encrypted hologram with a set of pinhole holograms, each located at a specific depth plane. We have applied the optical cryptosystem we have built to encrypt and decrypt 3-D object images. When the correct biometric keys are available, all the sectional images are recovered from the encrypted hologram with only mild defocused noise, and practically free from speckle noise. If the incorrect biometric keys are presented, the decrypted images are completely different from the original ones. As a concluding remark, our proposed method has successfully extended conventional optical scanning cryptography (OSC)[25] to biometric cryptography of 3-D object images. We have also enhance security against illegal attacks with a double key arrangement, whereby the key representing the fingerprint of the recipient is passed to the sender only when an encrypted image is requested by the recipient.

References

1. Matoba, O., Nomura, T., Elisabet, P.-C., Millan, M. S. & Javidi, B. Optical techniques for information security. *Proc. IEEE* **97**, 1128–1148 (2009).
2. Liu, S., Guo, C. & Sheridan, J. T. A review of optical image encryption techniques. *Opts & Laser Tech.* **57**, 327–342 (2014).
3. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20**, 767–769 (1995).
4. Unnikrishnan, G., Joseph, J. & Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **25**, 887–889 (2000).
5. Situ, G. & Zhang, J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **29**, 1584–1586 (2004).
6. Javidi, B. & Nomura, T. Securing information by use of digital holography. *Opt. Lett.* **25**, 28–30 (2000).
7. Alfaloul, A. & Brosseau, C. Dual encryption scheme of images using polarized light. *Opt. Lett.* **35**, 2185–2187 (2010).
8. Carnicer, A., Montes-Usategui, M., Arcos, S. & Juvells, I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **30**, 1644–1646 (2005).
9. Yan, A., Poon, T.-C., Hu, Z. & Zhang, J. Optical image encryption using optical scanning and fingerprint keys, *J. Mod. Opt.* 1–4 (2016).
10. Qin, W. & Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **35**, 118–120 (2010).
11. He, W., Meng, X. & Peng, X. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: comment. *Opt. Lett.* **38**, 1651–1653 (2013).
12. Mehra, I. & Nishchal, N. K. Optical asymmetric image encryption using gyrator wavelet transform. *Opt. Commun.* **354**, 344–352 (2015).
13. Rajput, S. K. & Nishchal, N. K. Image encryption based on interference that uses fractional Fourier domain asymmetric keys. *Appl. Opt.* **51**, 1446–1452 (2012).
14. Chang, H. T. & Chen, C. T. Asymmetric-image verification for security optical systems based on joint transform correlator architecture. *Opt. Commum.* **239**, 43–54 (2004).
15. Tashima, T. *et al.* Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack. *Opt. Exp.* **18**, 13772–13781 (2010).
16. Takeda, M., Nakano, K., Suzuki, H. & Yamaguchi, M. Encoding plaintext by Fourier transform hologram in double random phase encoding using fingerprint keys. *J. Opt.* **14**, 094003–094011 (2012).
17. Tajahuerce, E. & Javidi, B. Encrypting three-dimensional information with digital holography. *Appl. Opt.* **39**, 6595–6601 (2000).
18. Kishk, S. & Javidi, B. Watermarking of three-dimensional objects by digital holography. *Opt. Lett.* **28**, 167–169 (2003).
19. Kishk, S. & Javidi, B. 3D object watermarking by a 3D hideedn object. *Opt. Express* **11**, 874–888 (2003).
20. Nishchal, N. & Naughton, T. J. Flexible optical envryption with multiple users and multiple security levels. *Opts. Commun.* **284**, 735–739 (2011).

21. Poon, T.-C. & Liu, J.-P. *Introduction to Modern Digital Holography with MATLAB*, Cambridge University Press, Cambridge, U.K. (2014).
22. Chen, W. & Chen, X. Optical asymmetric cryptography using a three-dimensional space-based model. *J. Opt.* **13**, 075404–75410 (2011).
23. Yang, Y. *et al*. Three-dimensional information encryption with optical asymmetric cryptography and digital interferometry. *Proc. SPIE* **8202**, 820207–820219 (2011).
24. Indebetouw, G. & Poon, T.-C. Novel approaches of Incoherent image processing with emphasis on scanniig methods. *Opt. Engineering* **31**, 2159–2167 (1992).
25. Poon, T.-C., Kim, T. & Doh, K. Optical scanning cryptography for secure wireless transmission. *Appl. Opt.* **42**, 6496–6503 (2003).
26. Poon, T.-C. *Optical Scanning Holography with MATLAB*, Springer, U.S. (2007).

Acknowledgements

This work is partially sponsored by the National Nature Science Foundation of China under grant (No. 61575124, 11674231, 61475168).

Author Contributions

Dr. Aimin Yan developed the proposed method, prepared the manuscript and experimental results. Yang Wei participates in the development of the method, preparation of manuscript and experimental results. Zhijuan Hu participates in the development of the method, preparation of manuscript and experimental results. Jingtao Zhang participates in the development of the method, preparation of manuscript and experimental results. Dr. Peter Wai Ming Tsang (corresponding author) provides suggestions in the proposed method, and participation in the preparation and submission of the manuscript. Prof. Ting-Chung Poon provides suggestions in the proposed method, and participation in the preparation and submission of the manuscript. Figures 1, 2, 3(a) to 3(f), 4(a), 4(b), 5(a), 5(b), 6(a) to 6(d), 7(a) to 7(c), 8 are drawn and prepared by Dr. Aimin Yan, Yang Wei, Zhijuan Hu, and Jingtao Zhang. Base images of Figures 3(a) to 3(f), 4(a), 4(b), 5(a), 5(b), 6(a) to 6(d), 7(a) to 7(c) are produced by Dr. Aimin Yan.

Additional Information

Competing Interests: The authors declare that they have no competing interests.