Asymmetric Cryptosystem Based on Optical Scanning Cryptography and Elliptic Curve Algorithm

Xiangyu Chang
Shanghai Normal University
Wei Li
Shanghai Normal University
Aimin Yan (yanaimin@shnu.edu.cn)
Shanghai Normal University
Peter Wai Ming Tsang
City University of Hong Kong
Ting-Chung Poon
Virginia Tech

Research Article

Keywords: optical scanning cryptography (OSC), elliptic curve cryptography (ECC) algorithm, asymmetric cryptosystem.

Posted Date: December 29th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1148931/v1

Asymmetric Cryptosystem Based on Optical Scanning Cryptography and Elliptic Curve Algorithm

Xiangyu Chang[1], Wei Li[1], Aimin Yan[1,*], Peter Wai Ming Tsang [2,*], and Ting-Chung Poon[3]

[1]Shanghai Normal University, College of Mathematics and Science, Shanghai 200234, China
[2]City University of Hong Kong, Department of Electronic Engineering Hong Kong, SAR China
[3] Virginia Tech, Bradley Department of Electrical and Computer Engineering, Blacksburg, VA 24061, USA
[*]yanaimin@shnu.edu.cn;
[*]eewmtsan@cityu.edu.hk

We propose an asymmetric cryptosystem based on optical scanning cryptography (OSC) and elliptic curve cryptography (ECC) algorithm. In the encryption stage of OSC, an object is encrypted to cosine and sine holograms by two pupil functions calculated via ECC algorithm from sender's biometric image, which is sender's private key. With the ECC algorithm, these holograms are encrypted to ciphertext, which is sent to the receiver. In the stage of decryption, the ciphered holograms can be decrypted by receiver's biometric private key which is different from the sender's private key. The approach is an asymmetric cryptosystem which solves the problem of the management and dispatch of keys in OSC and has more security strength than it. The feasibility of the proposed method has been convincingly verified by numerical and experiment results.

Optical image encryption has attracted much attention in recent years because of its inherent capability of high parallelism and multidimensional freedoms (amplitude, phase and polarization). Since Refrégiér and Javidi first proposed the double random phase encoding (DRPE) technique [1], researchers have introduced many extended optical encryption methods such as a series of optical transforms [2-5], digital holography [6-8], joint transform correlator [9-11] and ghost imaging[12-14]. Furthermore, optical scanning cryptography (OSC) [15-19] envisioned by Poon has become a prospective technology. Different from that of other CCD-based hologram acquisition systems, it can capture the hologram of a physical object with a fast scanning mechanism along with single-pixel recording. Indeed, some encryption systems have been proposed based on OSC. Yan et al. obtained experimental results of encryption using fingerprint keys[18]. Furthermore, they first demonstrated optical cryptography of 3-D object images in an incoherent optical system with biometric keys[19]. However, like most of optical encryption systems, OSC is a symmetric cryptosystem whose encryption key and decryption key are generally identical or mutually conjugate. The key must be transmitted through another secured channel when the encrypted image is delivered. So, it is hard to make sure the security of keys management and dispatch. Qin and Peng have proposed a novel and inspirational asymmetric cryptography based on phase-truncated Fourier transform (PTFT) and DRPE [20], but it cannot solve the problem of management and dispatch of keys. To solve these problems, the public key cryptosystem has been introduced into optical encryption.

In a public key cryptosystem, each user has a pair of keys: one published publicly (known as the public key) and another stored in a secure location (known as the private key) [21-23]. Yuan et al. have proposed an asymmetric system

based on DRPE and Rivest-Shamir-Adelman (RSA) [24], which has simultaneous transmission for an encrypted image and a double random-phase encryption key. Meng et al. have reported an asymmetric cryptosystem combining two-step phase-shifting interferometry with RSA public-key cryptography[25]. In addition to the RSA, elliptic curve cryptography (ECC) is another popular digital encryption algorithm, which was introduced by Miller[26] and Koblitz[27]. Compared with RSA algorithm, ECC has smaller parameters with equivalent levels of security[22-23]. Specifically, ECC based on 600-bit keys has the same security level as a 21000-bit RSA system[23]. It will take an enormous time to solve the elliptic curves discrete logarithm problem, even if the attacker uses the fastest known algorithm. Hence, ECC is more attractive for mobile communication because of the smaller key sizes and hence the more on bandwidth saving. Indeed, researchers have been introducing ECC to optical systems. Fan et al. have proposed an asymmetric cryptosystem based on two-step phase-shifting interferometry (PSI) and ECC[28]. Abd El-Latif and Niu have presented an efficient hybrid image encryption scheme[29], which generates a keystream using cyclic elliptic curve point and chaotic system which in turn is used for encryption of data stream from the image. Soon Liu et al. have given a cryptanalysis of Abd El-Latif's scheme[30], which is based on cyclic elliptic curve and chaotic system. In addition, there are many other related ECC methods[31-33]. However, most of those methods have applied ECC algorithm by complicated encoding the image first. And some methods may be ineffective simply by only encrypting parameters of optical cryptosystems using ECC algorithm because the optical system itself is vulnerable to ciphertext-only attack (COA). In other words, attacker can recover plaintext from ciphertext without encrypting parameters. For example, OSC is a linear encryption system which can be vulnerable to COA by using phase retrieval algorithm[34-35]. So, it is indispensable to improve its security by improving the encryption system.

In this paper, we propose an asymmetric cryptosystem based on ECC algorithm and OSC system with biometric. It is capable of patching the security holes in OSC by cascading OSC system and ECC algorithm. And our proposed method solves the management and dispatch of keys in the optical system. Furthermore, it is a simple system that does not need to encode image into numbers. Organization of our paper is given as follows. In section 2, we give a brief review of the OSC system. Section 3 describes our proposed system. And experimental evaluations are given in section 4, followed by a conclusion summarizing the important findings.

Optical scanning cryptography (OSC)

Optical scanning holography (OSH) is a method developed by Poon and Korpel [16] for capturing holograms of physical objects with a single pixel sensor. Being different from other hologram acquisition methods that utilize digital cameras as the hologram recording devices, OSH is not restricted in the field of vision and the size of the hologram. Apart from hologram capturing, OSH can also be applied in optical encryption. In this section, we will give a brief introduce about optical scanning cryptography (OSC), an integration of OSH and encryption, as detailed description has been given in [16]. A 2-D array of data or function (e.g., a hologram) is denoted by a symbol in bold. For example, a 2-D array is represented by symbol $\boldsymbol{A}$, and an entry at the y^{th} row and the x^{th} column is denoted as $A(x, y)$.

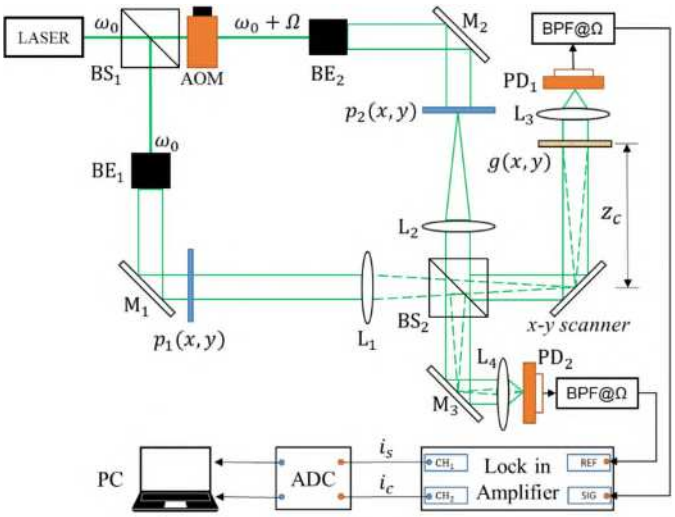


Fig. 1. Architecture of the optical scanning cryptosystem. BS_1 and BS_2: beam splitters; AOM: acousto-optical modulator; BE_1 and BE_2: beam expanders; M_1, M_2 and M_3: silver mirrors; L_1 and L_2: Fourier lens; L_1 and L_2: light-collecting lens; PD_1 and PD_2: photo-detectors; BPF: band-pass filter; ADC: analog-to-digital converter; PC: personal computer.

As shown in Fig. 1, both of the encryption and decryption systems are based on the architecture of Mach-Zehnder interferometer. After beam splitter (BS1), the laser beam with temporal frequency ω_0 has been divided into two beams, and the frequency of one of the beams becomes $\omega_0 + \Omega$ by using an acousto-optic modulator (AOM) operating with frequency Ω . The two beams are collimated by beam expanders, BE1 and BE2, and illuminate two pupil functions $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$, respectively. It should be noted that these two pupil functions can be utilized to perform processing on the hologram that is acquired by the OSC system. The pair of beams emerging through the two pupils pass through Fourier lens L1 and L2, and are recombined into a scanning beam by a beam splitter (BS2). Subsequently, the combined beam is steered in a zigzag manner with a mirror that is driven by an x-y scanner. The combined field $\boldsymbol{S}$, located at a distance z_c away from the back focal plane of lens L1, can be given as

$$S(x,y;z_c) = [FT\{p_1(x,y)\} * h(x,y;z_c)]\exp(j\omega_0 t) + [FT\{p_2(x,y)\} * h(x,y;z_c)]\exp[j(\omega_0+\Omega)t] \quad (1)$$

where FT denotes the Fourier transform, j is the imaginary unit and symbol "$*$" is the 2-D convolution operation. $h(x,y;z_c)$ is the free impulse response in Fourier optics[16]. The specimen is a translucent object with intensity distribution $\boldsymbol{g}$, and located at an axial distance z_c away from the focal plane of lens L1. The scanning beam is impinged on the specimen, and at each scan point photo-detector (PD) is employed to receive all the light scattered from the object, giving an electrical signal current as output. After bandpass filtering (BPF) of the signal current, heterodyne current at frequency Ω is obtained. The heterodyne current is then processed by a lock-in amplifier to give a couple of signal currents i_c and i_s, which represent the in-phase hologram $\boldsymbol{H_{cos}}$, and the quadrature hologram $\boldsymbol{H_{sin}}$, respectively. Mathematically, a complex- hologram acquired with the OSC system is given by

$$H(x,y) = H_{cos}(x,y) + jH_{sin}(x,y) = FT^{-1}\{FT\{|g(x,y)|^2\}OTF_\Omega(k_x,k_y;z_c)\} \quad (2)$$

where FT^{-1} denotes the inverse Fourier transforms and OTF_Ω is the optical transfer function (OTF) of the optical scanning system and expressed by

$$OTF_\Omega(k_x,k_y;z_c) = \exp\left[j\frac{z_c}{2k_0}(k_x^2+k_y^2)\right] \times \iint p_1^\dagger(x',y')p_2\left(x'+\frac{f}{k_0}k_x, y' + \frac{f}{k_0}k_y\right)\exp\left[j\frac{z_c}{2k_0}(x'k_x+y'k_y)\right]dx'dy' \quad (3)$$

where symbol "†" denotes the complex conjugation. k_0 is the wave number and f is the efficient focal length of lens L1 and L2. k_x and k_y denote the spatial frequencies along the x and y directions, respectively. From Eq. (2), the object can be encrypted by OTF_Ω determined by pupil functions $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$.

For decryption, we replace the object with a pinhole, $\delta(x, y)$, located z_d away from the back focal plane of lens L1. After the similar processing as in the encryption stage, we can obtain the pinhole hologram $\boldsymbol{H_{pin}}$ expressed as

$$H_{pin}(x, y; z_d) = FT^{-1}\{OTF_\Omega(k_x, k_y; z_d)\} \tag{4}$$

If the two pupils are both matched in the encryption and decryption stages and $z_c = z_d$, decryption hologram $\boldsymbol{H_{de}}$ is easy deduced by using the following calculation:

$$H_{de}(x, y) = FT^{-1}\{FT\{|g(x, y)|^2\}OTF_\Omega \times OTF_\Omega^\dagger\} = |g(x, y)|^2 \tag{5}$$

subject to condition $OTF_\Omega(k_x, k_y; z_c) \times OTF_\Omega^\dagger(k_x, k_y; z_d) = 1$ and for $z_c = z_d$.

If the pupil functions $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$ are derived from biometric signatures, such as fingerprints, the OSC and the captured hologram are referred as biometric encrypted optical scanning cryptography (BE-OSC), and biometric encrypted optical scanning hologram (BE-OSH), respectively.

The proposed biometric and asymmetric cryptosystem

The block diagram of our proposed method is shown in Fig. 2 and outlined as follows. To begin with, the parts on the left and the right hand sides of the vertical dotted line are the encryption side (operated by Alice), and the decryption side (operated by Bob), respectively. There are two shaded-shadow blocks showing different purposes. The gray blocks show the generation of secret and public keys and the blue blocks show the flow of encryption method.

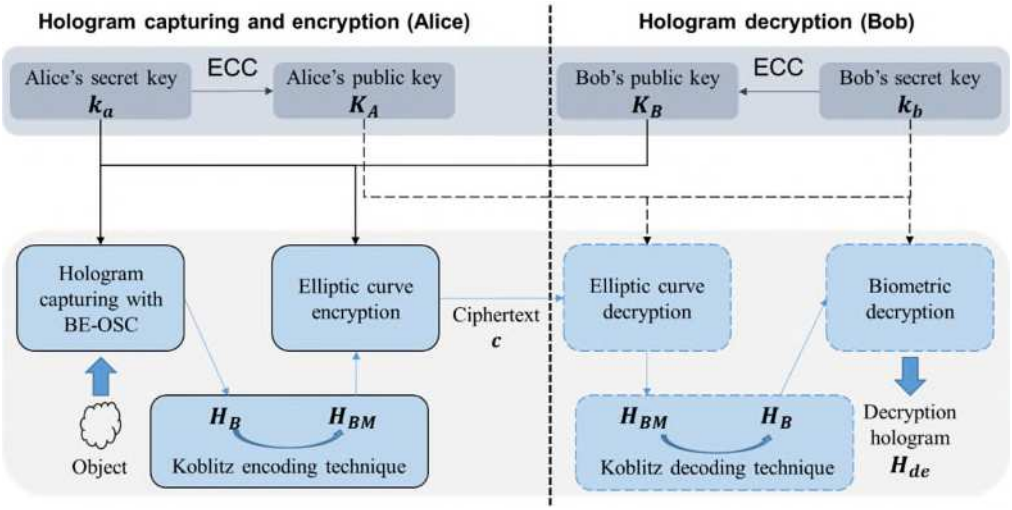


Fig. 2. Block diagram of our proposed system

On the top blocks, Alice's and Bob's public key $\boldsymbol{K_A}$ and $\boldsymbol{K_B}$ are generated from corresponding private keys $\boldsymbol{k_a}$ and $\boldsymbol{k_b}$ by ECC algorithm, respectively. Both sides share public keys, $\boldsymbol{K_A}$ and $\boldsymbol{K_B}$. We shall describe how these pair of keys are generated later. On the bottom blocks, the object is scanned by the OSC system in Fig. 1, and encrypted with the pupils functions which are derived from public key $\boldsymbol{K_B}$ and private key $\boldsymbol{k_a}$. $\boldsymbol{k_a}$ is a biometric image of Alice, resulting in biometric encrypted optical scanning hologram (BE-OSH) $\boldsymbol{H_B}$. Subsequently, the hologram $\boldsymbol{H_B}$ is embedded in $\boldsymbol{H_{BM}}$, which is represented as elliptic curve coordinates by Koblitz encoding technique. And $\boldsymbol{H_{BM}}$ is encrypted to ciphertext $\boldsymbol{c}$ by ECC, based on the same keys, $\boldsymbol{K_B}$ and $\boldsymbol{k_a}$. On the decryption side, hologram $\boldsymbol{H_{BM}}$ is obtained from the ciphertext with public key $\boldsymbol{K_A}$ and secret key $\boldsymbol{k_b}$ that is only known to Bob. The biometric hologram, $\boldsymbol{H_B}$, is obtained from $\boldsymbol{H_{BM}}$ through using Koblitz decoding technique. Finally, the decryption hologram $\boldsymbol{H_{de}}$ of the

object is then obtained by decrypting $\boldsymbol{H_B}$ with public key $\boldsymbol{K_A}$ and secret key $\boldsymbol{k_b}$. In the following subsections, we shall explain the biometric encrypted OSC and the ECC in details.

Biometric encrypted OSC. In section 2, we have an overview of optical scanning cryptography. As for biometric encrypted OSC system, the pair of pupils are each replaced with a phase mask which is calculated from the user's biometric image, such as fingerprint, iris and so on. In Fig. 2, the pair of phase masks are represented by public key $\boldsymbol{K_B}$ and private key $\boldsymbol{k_a}$. $\boldsymbol{k_a}$ is Alice's biometric image. The result of the scanning is biometric encrypted hologram $\boldsymbol{H_B}$ and the hologram is given by

$$\boldsymbol{H_B} = \boldsymbol{H_{Bc}} + j\boldsymbol{H_{Bs}} = FT^{-1}\{FT\{|g(x,y)|^2\}OTF_{\Omega}(k_x, k_y; z_c)\} \tag{6}$$

As such, the process will be equivalent to encrypting the holographic information with the pupil functions being the encryption keys, and hologram $\boldsymbol{H_B}$ can be taken as the ciphertext of the source image $\boldsymbol{g}$. From Eq. (3), we can infer that if functions $\boldsymbol{p_1}$ and $\boldsymbol{p_2}$ are not available to the public, the optical transfer function $OTF_{\Omega}(k_x, k_y; z_c)$ is unknown. Hence it is not possible to deduce the image of the specimen from biometric encrypted hologram $\boldsymbol{H_B}$ through an inverse relation.

However, OSC system is vulnerable to ciphertext-only attack because the system is a linear system. This is an inherent drawback in linear optical encryption systems, which are vulnerable to COA [34-35]. Assume that attackers get ciphertext only, the modulus of the Fourier transform of the ciphertext can be easily obtained as follows:

$$|FT\{H_B(x,y)\}| = |FT\{|g(x,y)|^2\}| \tag{7}$$

Then the problem to recover plaintext can be transformed into phase retrieval with a single intensity measurement. And it can be solved by using a phase retrieval algorithm, such as Gerchberg-Saxton (GS), the hybrid input-output algorithm (HIO) and so on [35]. In view of this, we have incorporated a second stage in elliptic curve cryptography (ECC) to encrypt hologram $\boldsymbol{H_B}$, so as to enhance the security level of the holographic data.

Elliptic curve cryptography. Elliptic curve cryptography (ECC) is an asymmetric encryption method that is resistant to COA, even known-plaintext attack (KPA) which knows more assumed information than COA. As ECC has been reported in numerous literature, only a brief outline is provided for the sake of completion. E_p is an elliptic curve equation over a finite field and expressed by

$$E_p = \{(x,y) \in \mathrm{R}^2 | y^2 = x^3 + ax + b \ (mod\ p), 4a^3 + 27b^2 \neq 0\} \cup \{O\} \tag{8}$$

where a and b are two real constants, which are the parameters of the elliptic curve. Symbol "mod" denotes the modulo operation and p is a prime number. O is the identity element, a point at infinity. If a point $P(x,y)$ on addition with infinity point O, the results is the point itself.

$$P \oplus O = O \oplus P = P \tag{9}$$

where "$\oplus$" is point addition which is the basic operation in ECC. There are three cases in the point addition between two points, $P(x_1, y_1)$ and $Q(x_2, y_2)$, which add up to generate a third point $R(x_3, y_3)$:

If $x_1 \neq x_2$, the coordinate of R is computed as

$$x_3 = \{\lambda^2 - x_1 - x_2\}\ mod\ p \tag{10}$$
$$y_3 = \{\lambda(x_1 - x_3) - y_1\}\ mod\ p \tag{11}$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}\ mod\ p \tag{12}$$

If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, the coordinate of R is computed as

$$x_3 = \{\lambda^2 - 2x_1\} \, mod \, p \quad (13)$$

$$y_3 = \{\lambda(x_1 - x_3) - y_1\} \, mod \, p \quad (14)$$

where

$$\lambda = \frac{3x_1^2 + a}{2y_1} \, mod \, p \quad (15)$$

If $x_1 = x_2$ and $y_1 = y_2 = 0$, the point will meet at infinity.

$$P \oplus P = O \quad (16)$$

If $x_1 = x_2$ but $y_1 \neq y_2$, the third point will be a point at infinity.

$$P \oplus Q = O. \quad (17)$$

Otherwise, the point negation "$\ominus$" is expressed as

$$P(x_1, y_1) \ominus Q(x_2, y_2) = P(x_1, y_1) \oplus Q(x_2, -y_2). \quad (18)$$

In scalar multiplication "$\otimes$", a point is multiplied with an integer k. The operation is realized by adding the point to itself by k times. For example, if P is multiplied by 3, it will be moved to a new point given by

$$3 \otimes P = P \oplus P \oplus P \quad (19)$$

When parameters of elliptic curve a, b, p and base point $P(x, y)$ are known, the following steps of ECC is given below.

Encryption:

a) Receiver (Bob) selects a random integer k_b from the interval $[1, n-1]$, where n is the cyclic order, as the private key. The corresponding public key $K_B = k_b \otimes P$ is publicized.

b) The value of plaintext $m = (m_1, m_2)$ is included in elliptic curve coordinates. And it is encrypted with a point which is obtained by scalar multiplication between Bob's public key K_B and Alice's private key k_a, a random integer from the interval $[1, n-1]$. Ciphertext $c = (c_x, c_y)$ is encrypted according to

$$c = m \oplus (k_a \otimes K_B) \quad (20)$$

Finally, the ciphertext and sender's public key $K_A = k_a \otimes P$ are sent to the receiver using the form of $\{K_A, c\}$.

Decryption:

c) Receiver decrypts the ciphertext with private key k_b according to

$$m = c \ominus (k_b \otimes K_A) \quad (21)$$

Encrypting the BE-OSC with the ECC

Next, we shall describe how the ECC is applied to encrypt the biometric encrypted hologram $\boldsymbol{H_B}$. Without loss of generality, we assume that BE-OSC generates a square hologram of size $M \times M$. For clarity of explanation, the following terminology is defined. The sender is Alice and the receiver is Bob. $E_p(a, b)$ denotes an elliptic curve that is characterized with Eq. (8). $P(x, y)$ is the base point and $\boldsymbol{P} = P \times \boldsymbol{I}$ where $\boldsymbol{I}$ represents a $M \times M$ unit matrix. These parameters are known to Alice and Bob. $\boldsymbol{k_a}$ and $\boldsymbol{k_b}$ are two $M \times M$ arrays of integers within the range $[1, n-1]$. The value of $\boldsymbol{k_a}$ and $\boldsymbol{k_b}$ is biometric image or randomly generated and taken to be the secret key of the user on the encryption side (i.e. Alice) and decryption side (i.e. Bob), respectively.

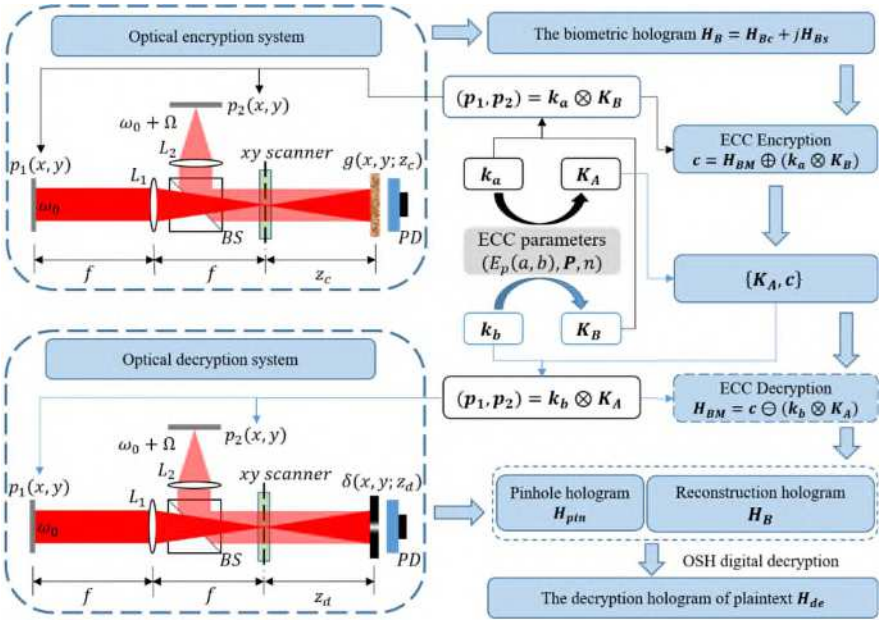


Fig. 3. Schematic diagram of the proposed asymmetric cryptosystem

Referring to Fig. 3, a pair of public keys, $\boldsymbol{K_A}$ and $\boldsymbol{K_B}$ are generated by Alice with secret key $\boldsymbol{k_a}$, and Bob with secret key $\boldsymbol{k_b}$, respectively, as given by

$$\boldsymbol{K_A} = \boldsymbol{k_a} \otimes \boldsymbol{P} = (\boldsymbol{K_{Ax}}, \boldsymbol{K_{Ay}}) \tag{22}$$

$$\boldsymbol{K_B} = \boldsymbol{k_b} \otimes \boldsymbol{P} = (\boldsymbol{K_{Bx}}, \boldsymbol{K_{By}}) \tag{23}$$

As explain previously, the scalar multiplication in Eq. (19) is an operation to move base point $P(x, y)$ to a new position that is determined with its corresponding term in $\boldsymbol{k_a}$ or $\boldsymbol{k_b}$. Hence each member of $\boldsymbol{K_A}$ and $\boldsymbol{K_B}$ is also a point on $E_p(a, b)$, and its value is an ordered pair corresponding to the horizontal and vertical coordinates of the point.

After generation of the public keys, Bob's public key $\boldsymbol{K_B}$ is published and sent to Alice. And the pair of phase masks of the pupils that are used in the encryption stage of OSC is derived from $\boldsymbol{K_B}$ and $\boldsymbol{k_a}$ as

$$(\boldsymbol{p_1}, \boldsymbol{p_2}) = \boldsymbol{k_a} \otimes \boldsymbol{K_B} \tag{24}$$

After optical encryption, source image $\boldsymbol{g}$ is encrypted to hologram $\boldsymbol{H_B} = \boldsymbol{H_{Bc}} + j\boldsymbol{H_{Bs}}$. As mentioned at last subsection, the source data of plaintext must belong to the elliptic curve so that ECC operators can be applied. To encrypt hologram $\boldsymbol{H_B}$ obtained from BE-OSC, each hologram pixel is mapped to a point on the curve based on Koblitz encoding technique, resulting in hologram $\boldsymbol{H_{BM}} = (\boldsymbol{H_{BMc}}, \boldsymbol{H_{BMs}})$. Subsequently, $\boldsymbol{H_{BM}}$ is encrypted into a ciphertext as

$$\boldsymbol{c} = \boldsymbol{H_{BM}} \oplus (\boldsymbol{k_a} \otimes \boldsymbol{K_B}) = (\boldsymbol{c_x}, \boldsymbol{c_y}) \tag{25}$$

When Bob receives $\{\boldsymbol{K_A}, \boldsymbol{c}\}$ sent from Alice, the mapped hologram can be recovered from the ciphertext with Bob's private key $\boldsymbol{k_b}$.

$$\boldsymbol{H_{BM}} = \boldsymbol{c} \ominus (\boldsymbol{k_b} \otimes \boldsymbol{K_A}) \tag{26}$$

After decryption, hologram $\boldsymbol{H_B}$ can be obtained from $\boldsymbol{H_{BM}}$ through Koblitz decoding technique. Simultaneously, two pupils are deduced by Bob's private key $\boldsymbol{k_b}$ and Alice's public key $\boldsymbol{K_A}$.

$$(\boldsymbol{p_1}, \boldsymbol{p_2}) = \boldsymbol{k_b} \otimes \boldsymbol{K_A} \tag{27}$$

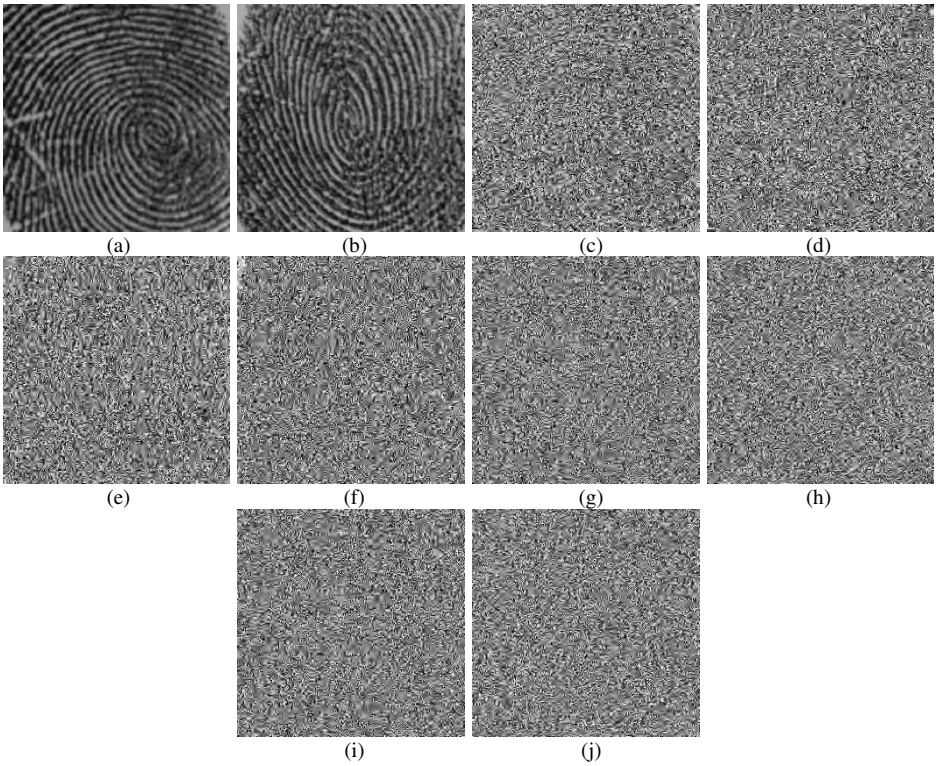
Then pinhole hologram $\boldsymbol{H_{pin}}$ is obtained from Eq. (4). Finally, the decryption hologram of the specimen $\boldsymbol{H_{de}}$ is decrypted from the pinhole hologram by Eq. (5).

Experimental results

We have employed some simple experiment to demonstrate the feasibility and effectiveness of the proposed method. In our experiment, we have two settings: (1) Alice's and Bob's private keys are their fingerprints. In reality, private keys can be any integer random matrices from interval $[1, n-1]$. (2) To obtain high-quality encrypted holograms in optical encryption system, one pupil function $\boldsymbol{p_1}$ can consist of a fingerprint image $FP(x,y)$ and a positive lens with focal length f_0, i.e. $p_1 = FP(x,y)\exp[jk_0(x^2+y^2)/2f_0]$. Another pupil is a delta function, i.e. $p_2(x,y) = \delta(x,y)$. In the optical decryption system, the pinhole hologram can be obtained by putting in a pin hole as an object. These preferences are convenient and enough to demonstrate our proposed method. Based on the use of MATLAB R2016a with a personal computer, it is easy to verify the feasibility of the proposed asymmetric system.

To reduce the computation time, we set $a = 1,\ b = 1$ in Eq. (8) with prime number $p = 29989$ and base point $P(29142,23400)$. Alice and Bob use their fingerprint as their private keys shown in Figs. 4(a) and (b), respectively. Bob uses the ECC algorithm to generate Bob's public key $\boldsymbol{K_B}$ and publicizes it and $\boldsymbol{K_B}$ has two parts, $\boldsymbol{K_{Bx}}$ and $\boldsymbol{K_{By}}$, as shown in Figs. 4(e) and (f). When Alice wants to send the image 'goat' $\boldsymbol{g}$, as shown in Fig. 5(a), Alice needs to obtain two pupils $(\boldsymbol{p_1}, \boldsymbol{p_2})$, as shown in Figs. 4(g) and (h), by calculating $\boldsymbol{k_a} \otimes \boldsymbol{K_B}$. Then, the digital holograms of plaintext are recorded by the OSC system shown in Fig.1. The output of the OSC system is a cosine hologram $\boldsymbol{H_{Bc}}$ and a sine hologram $\boldsymbol{H_{Bs}}$, as shown in Figs. 5(c) and (d), respectively. Next, Alice encrypts the digital holograms into the ciphertext $\boldsymbol{c}$ by applying asymmetric method in section 3.2, which has two parts, $\boldsymbol{c_x}$ and $\boldsymbol{c_y}$, as shown in Figs. 5(e) and (f), respectively. Finally, Alice sends Bob $\{\boldsymbol{K_A}, \boldsymbol{c}\}$ where $\boldsymbol{K_A}$ is Alice's public key whose two parts are shown in Figs. 4(c) and (d).

In the decryption stage, Bob uses $\boldsymbol{k_b}$ and $\boldsymbol{K_A}$ to calculate the two pupils $(\boldsymbol{p_1}, \boldsymbol{p_2})$, as shown in Figs. 4(i) and (j). Then Bob decrypts $\boldsymbol{c} = (\boldsymbol{c_x}, \boldsymbol{c_y})$ and obtains the reconstruction cosine and sine holograms, $\boldsymbol{H_{Bc}}$ and $\boldsymbol{H_{Bs}}$, as shown in Figs. 5(g) and (h). Simultaneously, Bob can obtain the pinhole hologram $\boldsymbol{H_{pin}}$, as shown in Figs. 5(i) and (j). Finally, the decryption hologram $\boldsymbol{H_{de}}$ is successful decrypted, as shown in Fig. 5(b). The proposed cryptosystem has a simple structure and requires no encoding image into numbers. And it has strong secure strength because it encrypts holograms, not parameters, in ECC stage.



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j)

Fig. 4 All keys in the experiment (a) Alice's private key $\boldsymbol{k_a}$; (b) Bob's private key $\boldsymbol{k_b}$; (c) and (d) are two parts of Alice's public key $\boldsymbol{K_A} = (\boldsymbol{K_{Ax}}, \boldsymbol{K_{Ay}})$, respectively; (e) and (f) are two parts of Bob's public key $\boldsymbol{K_B} = (\boldsymbol{K_{Bx}}, \boldsymbol{K_{By}})$, respectively; (g) and (h) are $(\boldsymbol{p_1}, \boldsymbol{p_2})$, generated by $\boldsymbol{k_a} \otimes \boldsymbol{K_B}$ in Alice's encryption; (i) and (j) are $(\boldsymbol{p_1}, \boldsymbol{p_2})$, generated by $\boldsymbol{k_b} \otimes \boldsymbol{K_A}$ in Bob's decryption.

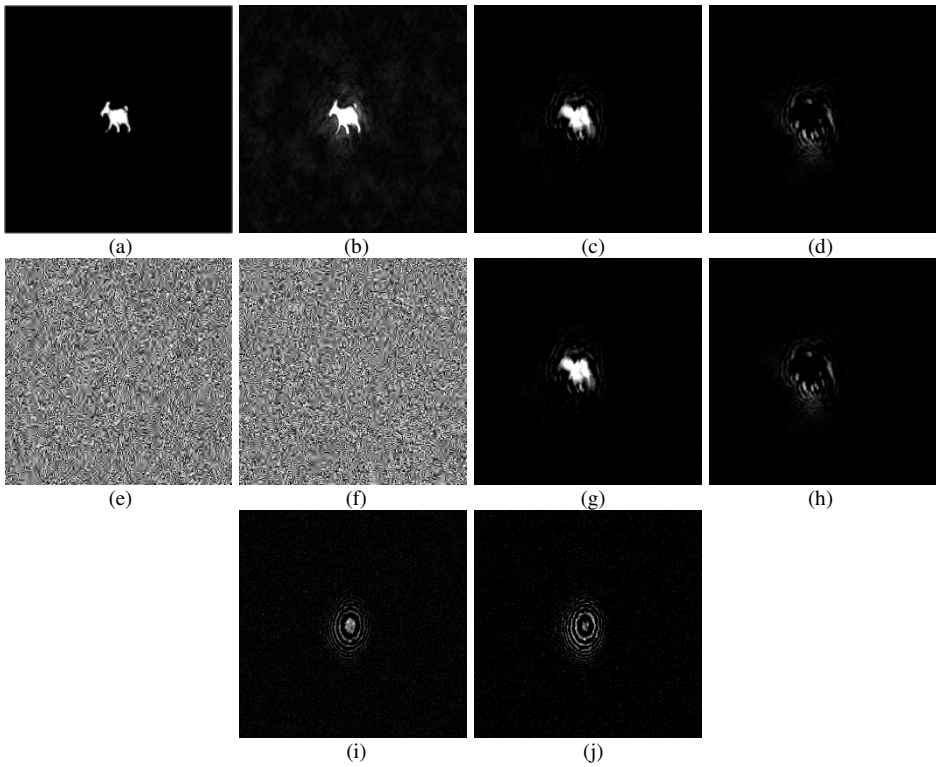
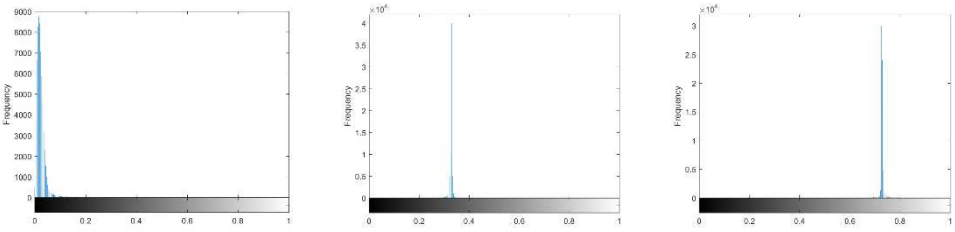
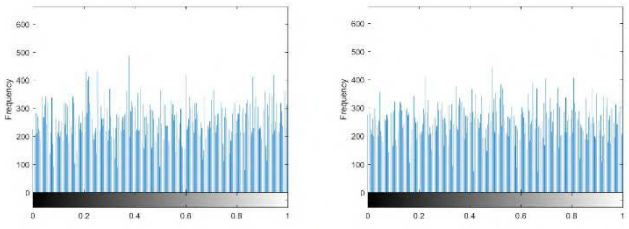


Fig. 5 (a) Image to be encrypted, $\boldsymbol{g}$; (b) final decrypted image $\boldsymbol{H_{de}}$; (c) and (d) are two parts of the mapped hologram of 'goat', i.e., $\boldsymbol{H_{Bc}}$ and $\boldsymbol{H_{Bs}}$ respectively; (e) and (f) are encrypted images, $\boldsymbol{c_x}$ and $\boldsymbol{c_y}$, respectively; (g) reconstruction cosine hologram $\boldsymbol{H_{Bc}}$; (h) reconstruction sine hologram $\boldsymbol{H_{Bs}}$; (i) and (j) are cosine and sine pinhole holograms $\boldsymbol{H_{Bc}}$ and $\boldsymbol{H_{Bs}}$, respectively.

Next, we include a brief analysis of the proposed method. First, the histogram of an image plots the pixel values against its frequency of occurrence. It is an important trait for ciphertext to distribute pixel values uniformly. Histogram of plaintext and its corresponding ciphertext using the proposed method is given in Fig. 6. Most of the pixel values of the "goat" are less than 0.1 in the histogram of Fig. 6(a). After optical encryption, pixel values of the cosine and sine holograms distribute around 0.3 and 0.7, as shown in Figs. 6(b) and (c), respectively. So, it may leak out information about plaintext. However, as shown in Figs. 6(d) and (e), histograms of ciphertext are distributed equally and hence it is hard to obtain information from the ciphertext. It shows demonstrates the proposed method works well.



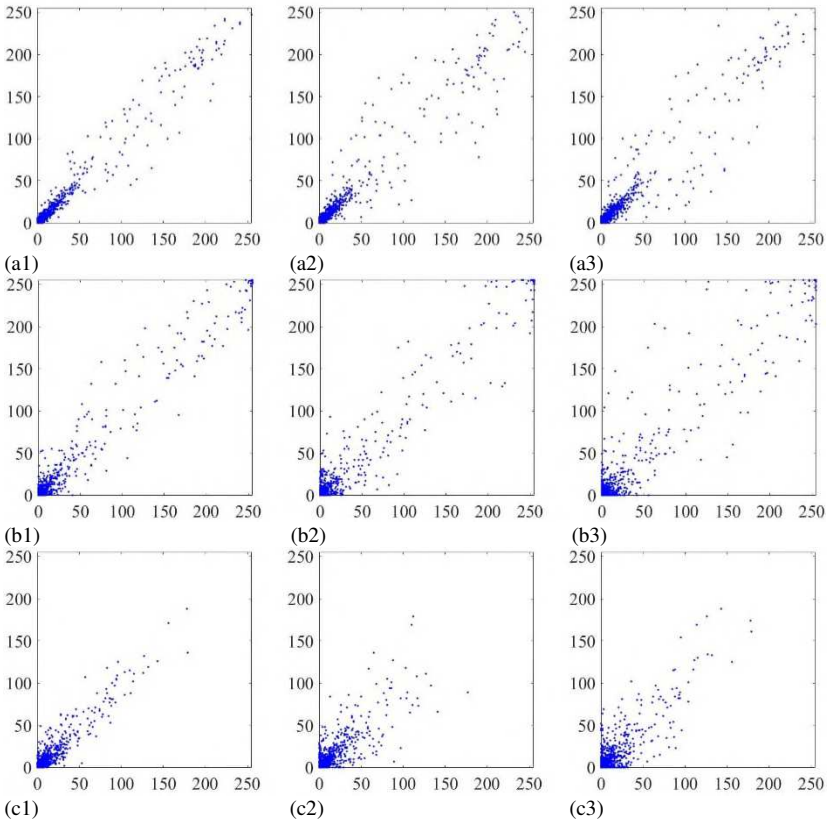
(a) (b) (c)



(d) (e)

Fig. 6 (a) Histogram of plaintext; (b) Histogram of cosine hologram; (c)Histogram of sine hologram; (d) histogram of $\boldsymbol{c_x}$; (e) histogram of $\boldsymbol{c_y}$.

Second, it is necessary to analyze the correlation of adjacent pixels, which reflects the correlation of pixel values in adjacent positions. If the correlation is large, it means that the difference of gray value in the larger area of the image is small, which will affect the security of the image. Therefore, we analyze the correlation between 2000 adjacent pixels randomly selected in three directions of these images. The correlation of adjacent pixels of plaintext and its corresponding ciphertext using the proposed method is given in Fig. 7. After optical encryption, the correlation between the adjacent pixels of cosine holograms and the adjacent pixels of sine holograms are still very high, as shown in Figs. 7(b1)-(b3) and (c1)-(c3), respectively. However, as shown in Figs. 7(d1)-(d3) and (e1)-(e3), the correlation of adjacent pixels of ciphertext are very low and hence the security of ciphertext are relatively high. In addition, the correlation coefficients of these images in three directions are shown in Table 1. It is proved that the method is very effective.



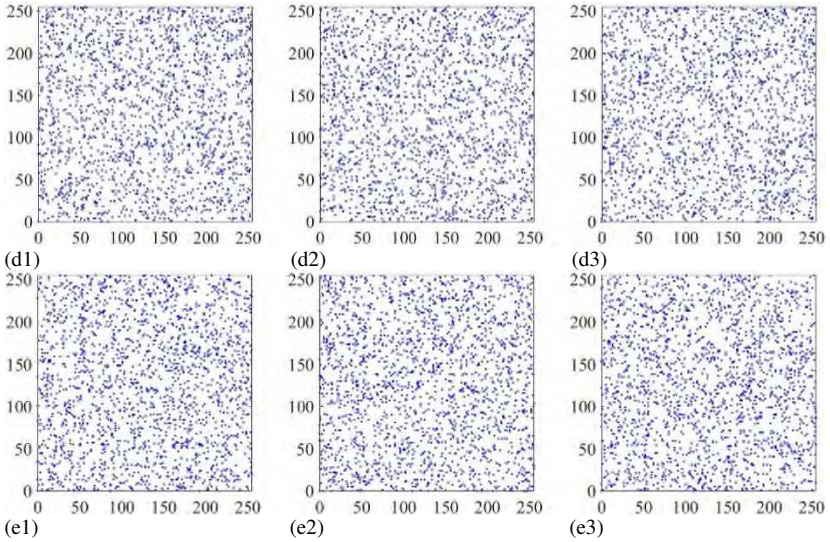


Fig. 7 (a1), (a2) and (a3) The adjacent pixel distributions of plaintext in the horizontal, vertical and diagonal directions; (b1), (b2) and (b3) the adjacent pixel distributions of cosine hologram in the horizontal, vertical and diagonal directions; (c1), (c2) and (c3) the adjacent pixel distributions of sine hologram in the horizontal, vertical and diagonal directions; (d1), (d2) and (d3) the adjacent pixel distributions of $\boldsymbol{c_x}$ in the horizontal, vertical and diagonal directions; (e1), (e2) and (e3) the adjacent pixel distributions of of $\boldsymbol{c_y}$ in the horizontal, vertical and diagonal directions.

Table 1 Correlation coefficients of adjacent pixels

Correlation coefficients	Plaintext	Cosine hologram	Sine hologram	Ciphertext	
				$\boldsymbol{c_x}$	$\boldsymbol{c_y}$
Horizontal	0.9804	0.9853	0.9278	0.0016	0.0064
Vertical	0.9637	0.9764	0.8375	-0.0042	-0.0014
Diagonal	0.9578	0.9706	0.8374	0.0169	0.0131

Third, image information entropy expresses the average amount of information in the image, which is defined by the following equation:

$$H(x) = -\sum_{i=0}^{255} P(x_i) \log_2 P(x_i) \tag{28}$$

where $P(x_i)$ is the probability of a gray value appearing in the image. If an image is very safe, the probability of all gray values should be equal, then according to the Eq. (28), $H(x)$ is equal to 8. And the information entropy of these images are shown in Table 2. The information entropy of ciphertext is extremely close to 8, which shows that our method is very safe.

Table 2 The information entropy

Plaintext	Cosine hologram	Sine hologram	Ciphertext	
			$\boldsymbol{c_x}$	$\boldsymbol{c_y}$
1.9577	1.1599	3.3125	7.9528	7.9608

Fourth, let us consider that the ciphertext is transferred through a channel. It is possible that the receiver receives the cipher image with salt-and-pepper noise. When receiver decrypts ciphertext with salt-and-pepper noise of 0.01 density which is the percentage of noise point that is in the total number of pixels. The reconstruction cosine and sine holograms are shown in Figs. 8(a) and (b), respectively, and the corresponding recovered plaintext is shown in Fig. 8(c). Figs. 8(d), (e) and (f) are shown with noise of 0.05 density. Finally, figs. 8(g) (h) and (i) are shown with noise of 0.1 density. In addition, we draw the curve between salt-and-pepper noise with different densities and image

reconstruction rate, as shown in Fig. 9. These results demonstrate that the proposed cryptosystem has fairly good robustness.

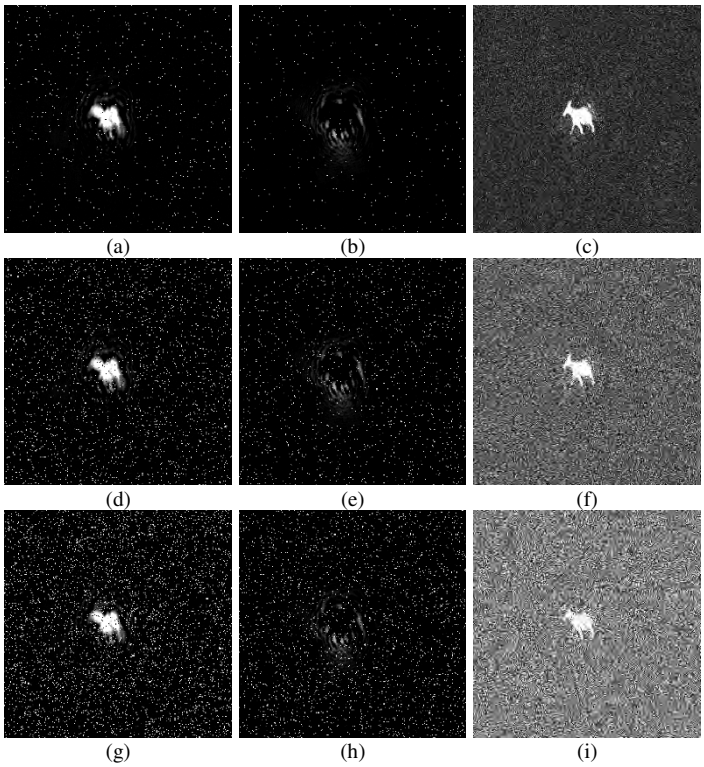


Fig. 8 Decrypted images with salt and pepper noise (a), (b) and (c) are reconstruction cosine and sine holograms and recovered image with 0.01 density, respectively; (d), (e) and (f) are images with 0.05 density; (g), (h) and (i) are images with 0.1 density.

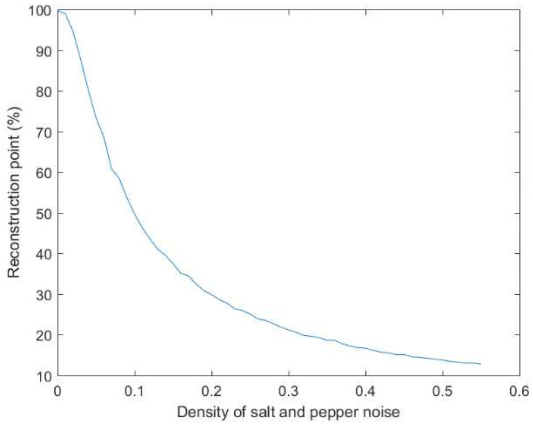
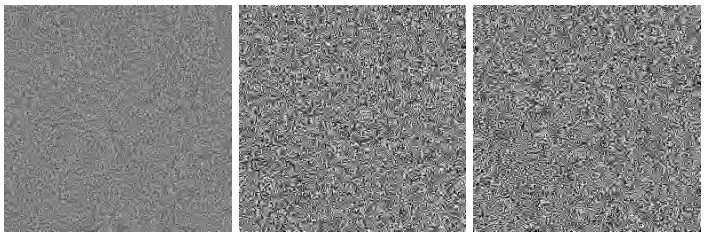


Fig. 9 Decrypted images reconstruction rate with salt and pepper noise.

Fifth, we should discuss known plaintext attack to further prove the security of our cryptosystem. According to the Eq. (20), $\boldsymbol{K_B} = \left(\boldsymbol{K_{Bx}}, \boldsymbol{K_{By}}\right)$ as shown in Figs. 4(e) and (f) determine the cryptosystem's ability to resist known plaintext attack. If the public and fixed $\boldsymbol{K_B}$ is used, it will be vulnerable to known plaintext attack, but changing the value of $\boldsymbol{K_B}$ frequently will make our cryptosystem more complicated. In order to solve this problem, Bob can randomly generate a secret key $\boldsymbol{k_b}'$ and transmit $\{\boldsymbol{k_b}' \otimes \boldsymbol{P}, (\boldsymbol{K_B} \oplus \boldsymbol{k_b}' \otimes \boldsymbol{K_A})\}$ to Alice, as shown in the Fig. 10. Then Alice calculates the following equation:

$$\boldsymbol{K_B} \oplus \boldsymbol{k_b}' \otimes \boldsymbol{K_A} \ominus \boldsymbol{k_A} \otimes \boldsymbol{k_b}' \otimes \boldsymbol{P} = \boldsymbol{K_B} \tag{29}$$

where $\boldsymbol{K_A} = \boldsymbol{k_A} \otimes \boldsymbol{P}$. Therefore, $\boldsymbol{K_B}$ will be hidden and our cryptosystem can resist known plaintext attack.



(a) (b) (c)

Fig. 10 (a) Bob's secret key $\boldsymbol{k_b}'$; (b) and (c) are $(\boldsymbol{K_B} \oplus \boldsymbol{k_b}' \otimes \boldsymbol{K_A})$, generated in Bob's decryption.

Conclusion

We have proposed a novel asymmetric cryptosystem that combines optical scanning cryptography (OSC) with the elliptic curve public-key cryptographic algorithm. It has the following advantages. First, the system realizes asymmetric encryption because the ways to obtain the encryption and decryption keys are different and the dispatch of keys does not need to be considered. Second, the cosine and sine holograms are nonlinearly encrypted simultaneously, so its security level is better than the OSC system alone. Third, the overall system has good robustness and its ciphertext will not leak information of the plaintext. Experimental results have shown that feasibility of this method has been verified through histogram and noise analysis.

Ethical approval

The authors confirmed that all experiments (taking fingerprints of an individual) were performed in accordance with relevant guidelines and regulations. The individual explicitly allowed the authors to use the data in the present publication. Aimin Yan

Statement confirming that informed consent

In this study, we only used fingerprints, not involving other human participants. The fingerprint used in this study is taken from Aimin Yan. Aimin Yan performed the optical experiments in optical laboratory. Aimin Yan

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

1. P. Refregier, B. Javidi, Optical image encryption based on input plane and fourier plane random encoding. Optics Letters. **20**, 767-769 https://doi.org/10.1364/OL.20.000767 (1995).

2. G. Situ, J. Zhang. Double random-phase encoding in the Fresnel domain. Optics Letters. **29**, 1584-1586 https://doi.org/10.1364/OL.29.001584 (2004).

3. H. Li, Y. Wang. Double-image encryption based on iterative gyrator transform. Optics Communications. **281**, 5745-5749 https://doi.org/10.1016/j.optcom.2008.09.001 (2008).

4. L. Sui, M. Xin, A. Tian. Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain. Optics Letters. **38**, 1996-1998. https://doi.org/10.1364/OL.38.001996 (2013).

5. P. Singh, A. K. Yadav, K. Singh. Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. Optics and Lasers in Engineering. **91**, 187-195. https://doi.org/10.1016/j.optlaseng.2016.11.022 (2017).

6. B. Javidi, T. Nomura. Securing information by use of digital holography. Optics Letters. **25**, 28-30 https://doi.org/10.1364/OL.25.000028 (2000).

7. L. Chen, D. Zhao. Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography. Optics Express. **15**, 16080-16089 https://doi.org/10.1364/OE.15.016080 (2007).

8. S. K. Rajput, O. Matoba. Optical voice encryption based on digital holography. Optics Letters. **42**, 4619-4622. https://doi.org/10.1364/OL.42.004619 (2017).

9. T. Nomura, B. Javidi. Optical encryption using a joint transform correlator architecture. Optical Engineering. **39**, 2031-2035 https://doi.org/10.1117/1.1304844 (2000).

10. A. V. Zea, J. F. B. Ramirez, R. Torroba. Three-dimensional joint transform correlator cryptosystem. Optics Letters. **41**, 599-602 https://doi.org/10.1364/OL.41.000599 (2016).

11. J. M. Vilardy, M. S. Millán, E.Pérez-Cabré. Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain. Optics and Lasers in Engineering. **89**, 88-94. https://doi.org/10.1016/j.optlaseng.2016.02.013 (2017).

12. P. Clemente, V. Durán, E. Tajahuerce, J. Lancis. Optical encryption based on computational ghost imaging. Optics Letters. **35**, 2391-2393 https://doi.org/10.1364/OL.35.002391 (2010).

13. M. Tanha, R. Kheradmand, S. Ahmadikandjani. Gray-scale and color optical encryption based on computational ghost imaging. Applied Physics Letters. **101**, 101108 https://doi.org/10.1063/1.4748875(2012).

14. F. Wang, H. Wang, H. Wang, G. Li, G. Situ. Learning from simulation: An end-to-end deep-learning approach for computational ghost imaging. Optics Express. **27**, 25560-25572 https://doi.org/10.1364/OE.27.025560 (2019).

15. T.-C. Poon, T. Kim, K. Doh. Optical scanning cryptography for secure wireless transmission. Applied optics. **42**, 6496-6503 https://doi.org/10.1364/AO.42.006496 (2003).

16. T.-C. Poon. Optical Scanning Holography with MATLAB. **21**, New York, NY: Springer, 2007. https://doi.org/10.1007/978-0-387-68851-0

17. A. Yan, J. Sun, Z. Hu, J. Zhang, L. Liu. Novel optical scanning cryptography using Fresnel telescope imaging. Optics Express. **23**, 18428-18434. https://doi.org/10.1364/OE.23.018428 (2015).

18. A. Yan, T.-C. Poon, Z. Hu, J. Zhang. Optical image encryption using optical scanning and fingerprint keys. Journal of Modern Optics. **63**, S38-S43 https://doi.org/10.1080/09500340.2016.1206981 (2016).

19. A. Yan, Y. Wei, Z. Hu, J. Zhang, P. W. M. Tsang, T.-C. Poon. Optical cryptography with biometrics for multi-depth objects. Scientific Reports. **7**, 12933 https://xs.scihub.ltd/https://doi.org/10.1038/s41598-017-12946-8 (2017).

20. W. Qin, X. Peng. Asymmetric Cryptosystem based on Phase-Truncated Fourier Transforms. Optics Letters. **35**, 118-120 https://doi.org/10.1364/OL.35.000118 (2010).

21. W. Diffie, M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory. **22**, 644-654 https://doi.org/10.1109/TIT.1976.1055638 (1976).

22. S. Vanstone. Next generation security for wireless: elliptic curve cryptography. Computers & Security. **22**, 412-415 https://doi.org/10.1016/S0167-4048(03)00507-8 (2003).

23. D. Hankerson, A. Menezes. Elliptic curve cryptography. (Springer US, 2011).

24. S. Yuan, X. Zhou, D. H. Li, D. F. Zhou. Simultaneous transmission for an encrypted image and a double random-phase encryption key. Applied Optics. **46**, 3747-3753 https://doi.org/10.1364/AO.46.003747 (2007).

25. X. F. Meng, X. Peng, L. Z. Cai, A. M. Li, Z. Gao, Y. R. Wang. Cryptosystem based on two-step phase-shifting interferometry and the RSA public-key encryption algorithm. Journal of Optics A: Pure and Applied Optics. **11**, 085402 https://doi.org/10.1088/1464-4258/11/8/085402(2009).

26. V. S. Miller. Use of elliptic curves in cryptography. Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg https://doi.org/10.1007/3-540-39799-X_31 (1985).

27. N. Koblitz. Elliptic curve cryptosystems. Mathematics of computation. **48,** 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5 (1987).

28. D. Fan, X. Meng, Y. Wang, X. Yang, X. Peng, W. He, H. Chen. Asymmetric cryptosystem and software design based on two-step phase-shifting interferometry and elliptic curve algorithm. Optics Communications. **309,** 50-56 https://doi.org/10.1016/j.optcom.2013.06.044 (2013).

29. A. A. Abd El-Latif, X. Niu. A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU-International Journal of Electronics and Communications. **67**, 136-143 https://doi.org/10.1016/j.aeue.2012.07.004 (2013).

30. H. Liu, Y. Liu. Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. Optics & Laser Technology. **56,** 15-19 https://doi.org/10.1016/j.optlastec.2013.07.009 (2014).

31. L. Tawalbeh, M. Mowafi, W. Aljoby. Use of elliptic curve cryptography for multimedia encryption. IET Information Security. **7**, 67-74 https://doi.org/10.1049/iet-ifs.2012.0147 (2013).

32. D. S. Laiphrakpam, M. S. Khumanthem. Medical image encryption based on improved ElGamal encryption technique. Optik. **147**, 88-102 https://doi.org/10.1016/j.ijleo.2017.08.028 (2017).

33. M. S. Khoirom, D. S. Laiphrakpam, T. Themrichon. Cryptanalysis of multimedia encryption using elliptic curve cryptography. Optik. **168**, 370-375 https://doi.org/10.1016/j.ijleo.2018.04.068(2018).

34. G. Li, W. Yang, D. Li, G. Situ. Cyphertext-only attack on the double random-phase encryption: Experimental demonstration. Optics Express. **25**, 8690-8697 https://doi.org/10.1364/OE.25.008690 (2017).

35. X. Chang, A. Yan, H. Zhang. Ciphertext-only attack on optical scanning cryptography. Optics and Lasers in Engineering. **126**, 105901. https://doi.org/10.1016/j.optlaseng.2019.105901(2020).

Competing interests

The authors declare no competing interests.

Acknowledgements

This work was supported by the National Nature Science Foundation of China under grant (No.62075134)

Author information

Affiliations

Shanghai Normal University, College of Mathematics and Science, Shanghai 200234, China
Xiangyu Chang, Wei Li, Aimin Yan

City University of Hong Kong, Department of Electronic Engineering Hong Kong, SAR China
Peter Wai Ming Tsang

Virginia Tech, Bradley Department of Electrical and Computer Engineering, Blacksburg, VA 24061, USA
Ting-Chung Poon

Author contributions

A. Y. (corresponding author) developed the proposed method and conceived the experiments. X. C. performed the theoretical analysis and prepared the manuscript. W. L. participated in the preparation of manuscript. P. T. (corresponding author) provided suggestions in the proposed ECC method, and participation in the preparation of the manuscript. T. P. provided suggestions in the proposed OSC method and participation in the preparation of the manuscript. All authors reviewed the manuscript.