Journal of Modern Optics

ISSN: 0950-0340 (Print) 1362-3044 (Online) Journal homepage: https://www.tandfonline.com/loi/tmop20

Optical image encryption using optical scanning and fingerprint keys

Aimin Yan, Ting-Chung Poon, Zhijuan Hu & Jingtao Zhang

To cite this article: Aimin Yan, Ting-Chung Poon, Zhijuan Hu & Jingtao Zhang (2016) Optical image encryption using optical scanning and fingerprint keys, Journal of Modern Optics, 63:sup3, S38-S43, DOI: 10.1080/09500340.2016.1206981

To link to this article: https://doi.org/10.1080/09500340.2016.1206981

Published online: 07 Jul 2016.

JOURNAL OF MODERN OPTICS, 2016
VOL. 63, NO. S3, S38–S43
http://dx.doi.org/10.1080/09500340.2016.1206981

Taylor & Francis
Taylor & Francis Group

Optical image encryption using optical scanning and fingerprint keys

Aimin Yan[a], Ting-Chung Poon[b], Zhijuan Hu[a] and Jingtao Zhang[a]

[a]Key Laboratory of Optoelectronic Material and Device, College of Mathematics and Science, Shanghai Normal University, Shanghai, P.R. China; [b]Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, USA

ABSTRACT

Fingerprint authentication is a preferable biometric technique for securing images. Optical scanning cryptography (OSC) is a hybrid optical/digital method to encrypt and decrypt an image using optical scanning technique. In this paper, we propose a new strategy to combine OSC with fingerprints to enhance security. We have verified the effectiveness of the proposed idea in simulations. Subsequently practical implementation of the idea has also been performed with optical heterodyning to confirm the results from simulations. We have also discussed the added security and flexibility of implementation when optical heterodyning is employed in cryptography.

ARTICLE HISTORY
Received 18 May 2016
Accepted 24 June 2016

KEYWORDS
Image and image processing; optical security and encryption; digital holography; fingerprint keys; optical scanning; biometric security

1. Introduction

Optical encryption techniques have attracted significant interest because optical systems can offer the possibility of high speed processing and provide many degrees of freedom to handle optical parameters such as amplitude, phase, wavelength and polarization (*1–5*). A popular optical encryption technique is based on double-random-phase encoding in a well-known 4-f coherent system (*6*), and many other optical encryption techniques, such as the use of fractional Fourier transform (*7, 8*), Fresnel transform (*9, 10*), gyrator transform (*11, 12*), polarization (*13*) and diffractive imaging (*14*), have been investigated. Owing to the need to extract the amplitude and phase information, digital holography is often used to implement some of these ideas in a coherent system (*15–19*). One of the major issues using linear optical systems for encryption and decryption is that if the encryption machine is asked to encrypt a point source, i.e. finding its point spread function (PSF), it will produce the decryption key at the output (*20*). Some recent works have addressed this major issue with encryption scheme using randomized lens-phase functions (*21*). Whereas most investigated optical encryption techniques have been coherent optical systems, there are very few incoherent optical techniques, which inherently have better signal-to-noise ratio (*S/N*) compared to its coherent counterpart. In conventional incoherent optical systems, intensity of the object is manipulated and only real and positive PSFs can be obtained (*22*), which highly limit the way one can process information. In any case, there are few techniques that have been investigated in incoherent optical encryption systems (*22–25*). In this paper, we present a practical implementation of optical scanning cryptography (OSC) using heterodyne scanning. In addition, we investigate the use of amplitude fingerprint keys for encryption and decryption. We have demonstrated its flexibility and pointed out that the PSF of the encryption machine is not straightforward to obtain as in other linear optical systems, which brings the security level higher.

In Section 2, we briefly summarize some of the important results from optical scanning cryptography. In Section 3, we show simulations to clarify the proposed idea of using amplitude fingerprint keys and illustrate the effectiveness and advantages of the proposed technique. In Section 4, we demonstrate the proposed idea with a practical implementation and finally we make some concluding remarks in Section 5.

2. Optical scanning cryptography using fingerprint keys

In this section, we summarize the basic theory of encryption and decryption in optical scanning cryptography. We see that the manipulation of the two pupils in the optical

CONTACT Aimin Yan yanaimin@shnu.edu.cn

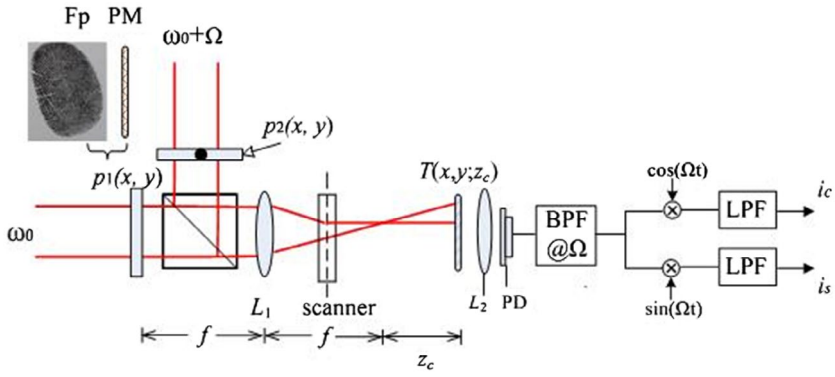

Figure 1. Encryption machine by a two-pupil optical heterodyne scanning system: PD = photodetector; BPF @ Ω = electronic bandpass filter tuned at frequency Ω; LPF = lowpass filter; ⊗ = electronic multiplier.

system will allow us to implement cryptography efficiently. The idea of encryption will first be discussed, which is followed by the description of decryption.

2.1. Encryption

The encryption machine is shown in Figure 1, which is based on a two-pupil heterodyne scanning system (*22*). Two pupils, $p_1(x, y)$ and $p_2(x, y)$, located in the front focal planes of lens L_1 with focal length f, are illuminated by two collimated laser beams of angular frequencies of ω_0 and $\omega_0 + \Omega$, respectively. The two beams are then combined by a beam splitter (BS). The combined beam passes through a lens L_1 and is used for 2-D scanning of the object to be encrypted with amplitude $T(x, y; z_c)$, located at a coding distance z_c away from the back focal plane of lens L_1. The photo-detector (PD) collects all the light transmitted and after a bandpass filter tuned at frequency Ω, delivers a heterodyne current $i_\Omega(x, y; z_c)$ for immediate demodulation. The current is demodulated by an electronic multiplier and a lowpass filter, which can be implemented in practice using a lock-in amplifier in the experimental section to be reported in the next section. By multiplying the incoming signal $i_\Omega(x, y; z_c)$ by $\cos(\Omega t)$ and $\sin(\Omega t)$, and through low-pass filtering, we obtain two signals, $i_c(x, y; z_c)$ and $i_s(x, y; z_c)$, respectively, which can be added in a complex way in a computer to give a final encrypted image, $i(x, y; z_c)$, given by

$$\begin{aligned} i(x,y;z_c) &= i_c + ji_s \\ &= \mathfrak{F}^{-1}\left\{\mathfrak{F}\{|T(x,y;z_c)|^2\} \times \mathrm{OTF}(k_x,k_y;z_c)\right\} \\ &= |T(x,y;z_c)|^2 \otimes \mathfrak{F}^{-1}\{\mathrm{OTF}(k_x,k_y;z_c)\}, \end{aligned} \quad (1)$$

where $\mathfrak{F}^{-1}$ and $\mathfrak{F}$ denote the inverse and forward Fourier transforms, respectively; ⊗ denotes the operation of 2-D convolution, and $\mathrm{OTF}(x, y; z_c)$ is the optical transfer function of the encryption stage at the coding distance z_c, which can be expressed in terms of the two pupil functions as

$$\begin{aligned} \mathrm{OTF}(k_x,k_y;z_c) = e^{j\frac{z_c}{2k_0}(k_x^2+k_y^2)} \\ \iint p_1^*(x',y')p_2\left(x'+\frac{f}{k_0}k_x, y'+\frac{f}{k_0}k_y\right) \\ e^{j\frac{z_c}{2k_0}(x'k_x+y'k_y)}\mathrm{d}x'\mathrm{d}y', \end{aligned} \quad (2)$$

where k_0 is the wave number of the laser light used. Note that in Equation (1), only the intensity of the pattern, $|T(x, y; z_c)|^2$, is processed and hence the system is an incoherent optical system. We can see that the object can be encrypted by $\mathrm{OTF}(x, y; z_c)$ and the OTF is determined by pupil functions $p_1(x, y)$ and $p_2(x, y)$. In our proposed scheme that we will present in the next section, the function $p_1(x, y)$ chosen is the encryption key, which consists of a fingerprint image (*Fp*) and a random phase mask (PM). In reality, the PM can be permanently set on the pupil plane and whenever encryption is taking place, fingerprints can be inputted, thereby allowing user-dependent identity code. The use of an amplitude fingerprint is also convenient and direct as there is no need to change it into a phase image. We will demonstrate that the use of amplitude codes (keys) is as efficient as the use of phase codes. As for the other pupil function, $p_2(x, y)$, in the system, it is taken to be a pin hole for simplicity in the present scheme.

2.2. Decryption

The decryption machine is illustrated in Figure 2. The system is basically the same as that in the encryption stage except the laser beams now scan a pinhole as an object, located a decoding distance z_d away from the back focal plane of lens L_1. Essentially, we are finding the PSF of the optical system. We can use the results in Equation (1) but with z_c replaced by z_d and $T(x, y; z_c) = \delta(x, y; z_d)$. The current collected by the PD is passed to the bandpass filter for the similar processing as in the encryption stage, which gives

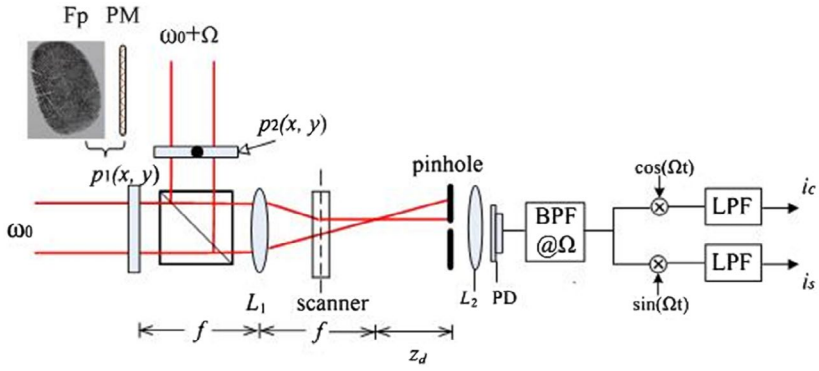

Figure 2. Decryption machine: PSF measurement.

two outputs $i_c(x, y; z_d)$ and $i_s(x, y; z_d)$. After complex construction in the computer, i.e. $i(x, y; z_d) = i_c + ji_s$, we obtain

$$i(x, y; z_d) = \mathfrak{F}^{-1}\left\{\mathfrak{F}\{\delta(x, y; z_d)\} \times \mathrm{OTF}(k_x, k_y; z_d)\right\} \propto \mathfrak{F}^{-1}\left\{\mathrm{OTF}(k_x, k_y; z_d)\right\}, \quad (3)$$

which is considered as a PSF of the optical system. The coded information $i(x, y; z_c)$ and the PSF of the system $i(x, y; z_d)$ generated at the encryption stage and decryption stage, respectively, can be stored in the computer to be used to decrypt the original image. Decryption of the encrypted image, can be performed digitally in the computer as follows:

$$i_0(x, y) \propto \mathfrak{F}^{-1}\left\{\mathfrak{F}\{i(x, y; z_c)\} \times \mathfrak{F}^*\{i(x, y; z_d)\}\right\} = \mathfrak{F}^{-1}\left\{\mathfrak{F}\{|T(x, y; z_c)|^2\} \times \mathrm{OTF}(k_x, k_y; z_c) \times \mathrm{OTF}^*(k_x, k_y; z_d)\right\} = |T(x, y; z_c)|^2 \quad (4a)$$

when the following condition is met:

$$\mathrm{OTF}(k_x, k_y; z_c) \times \mathrm{OTF}^*(k_x, k_y; z_d)\} = 1, \quad (4b)$$

where '*' denotes the complex conjugate.

3. Fingerprints as biometric keys and simulation results

In the last section, we have summarized the overall crypto-system in terms of general pupil functions p_1 and p_2. We have a freedom to choose the type of pupils to be used. For encryption, we propose the use of biometric pupil with $p_1(x, y) = Fp(x, y) \exp[jM(x, y)]$, where $Fp(x, y)$ is the amplitude of a fingerprint image and $M(x, y)$ is a function of numbers randomly distributed in a range of $[0, 2\pi]$. The other pupil is chosen to be $p_2(x, y) = \delta(x, y)$, which is a pinhole. Numerical simulations are first employed to verify the robustness of our biometric authentication idea.

With the proposed pupils, the encryption OTF from Equation (2) is then reduced to

$$\mathrm{OTF}(k_x, k_y; z_c) = e^{\frac{-jz_c}{2k_0}(k_x^2+k_y^2)} Fp\left(-\frac{f}{k_0}k_x, -\frac{f}{k_0}k_y\right) e^{-jM\left(-\frac{f}{k_0}k_x, -\frac{f}{k_0}k_y\right)}. \quad (5)$$

The first term in the above equation is the holographic recording term. Putting Equation (5) back into Equation (1), we have

$$i(x, y; z_c) = \mathfrak{F}^{-1}\left\{\mathfrak{F}\{|T(x, y; z_c)|^2\} e^{\frac{-jz_c}{2k_0}(k_x^2+k_y^2)} Fp\left(-\frac{f}{k_0}k_x, -\frac{f}{k_0}k_y\right) e^{-jM\left(-\frac{f}{k_0}k_x, -\frac{f}{k_0}k_y\right)}\right\}. \quad (6)$$

If we ignore the last two terms of Equation (6), we have standard holographic recording of the object, $|T(x, y; z_c)|^2$, and the resulting coded information is called the complex hologram of the object. Now with the last two terms included, we interpret Equation (6) as the complex hologram of an encrypted object, i.e. the hologram of the object has been encrypted by the last two terms. We call $i(x, y; z_c)$ as the encrypted complex hologram of the object.

Figure 3 shows the simulation results: the fingerprint image (a), the image to be encrypted (b) and (c) the intensity of the encrypted image. It can be seen that the information of the 'goat' image can be completely hidden and encrypted using the proposed amplitude fingerprint as the encryption key. According to Equation (4a), the output generated at the decryption stage $i_o(x, y)$ is shown in Figure 3(d). We can see that the encrypted image in Figure 3(c) can be decrypted but with some noise. The reason is that we have used an amplitude fingerprint, $Fp(x, y)$, in Equation (4a), which does not satisfy Equation (4b), i.e. $\mathrm{OTF} \times \mathrm{OTF}^* = |Fp|^2 \neq 1$. However, we can process $i_0(x, y)$ by dividing $|Fp|^2$ within the inverse transform in Equation (4a); then Equation (4b) will be

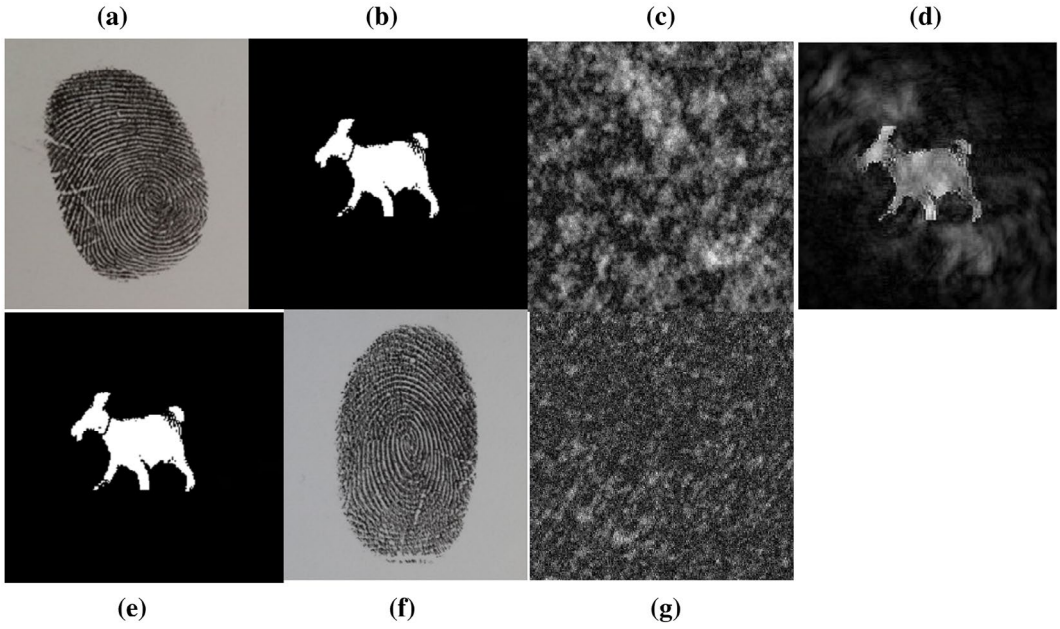

Figure 3. Simulation results: (a) fingerprint image; (b) image to be encrypted; (c) encrypted image; (d) decrypted image with matched key; (e) the decrypted image after processing, meeting the requirement of Equation (4b); (f) wrong fingerprint image used in the decryption machine; (g) decrypted image with wrong decryption key.

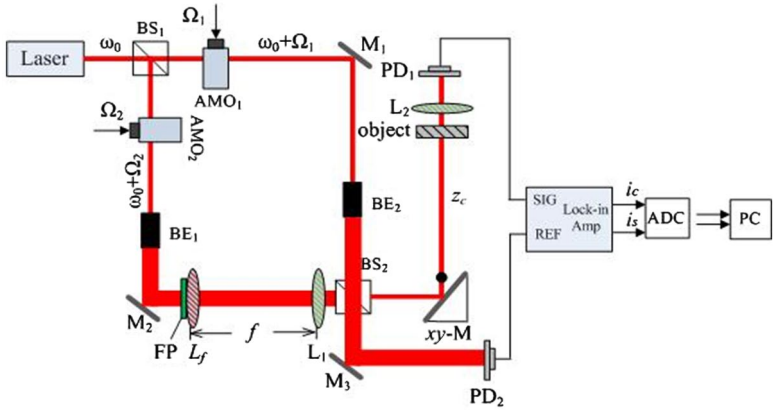

Figure 4. Practical implementation of optical scanning cryptography using heterodyne detection with two AOMs: BS_1 and BS_2, beam splitters; AOM_1 and AOM_2, acousto-optic modulators; *Fp*, fingerprint image; M_1, M_2 and M_3, reflective mirrors; *xy*–*M*, *x*–*y* scanner; PD_1 and PD_2, photo-detectors; BE_1 and BE_2, beam expanders; ADC, analogue-to-digital converter.

satisfied. Figure 3(e) gives the corresponding decrypted image after such processing. When the decryption was performed using the matched decryption key and the correct decoding distance, i.e. $z_d = z_c$, the decrypted image can be completely reconstructed. We also have performed decryption using a wrong fingerprint image in the decryption machine. Figure 3(f) shows a different fingerprint image and the corresponding decrypted image is shown in Figure 3(g). A correct decrypted image cannot be obtained using the wrong amplitude fingerprint key which is different from the fingerprint key in the encryption stage.

4. Practical implementation and experimental results

We have performed some simple experiments to demonstrate the feasibility and effectiveness of the proposed method using fingerprint keys. Figure 4 shows the experimental set-up of the proposed method. The laser wavelength is 632.8 nm. AOM_1 and AOM_2 are acousto-optic modulators with frequencies 40.25 and 40 MHz, which can generate heterodyne frequency $\Omega/2\pi = (\Omega_1 - \Omega_2)/2\pi = 25$ kHz. Note that the use of two AOMs in the actual implementation has added security

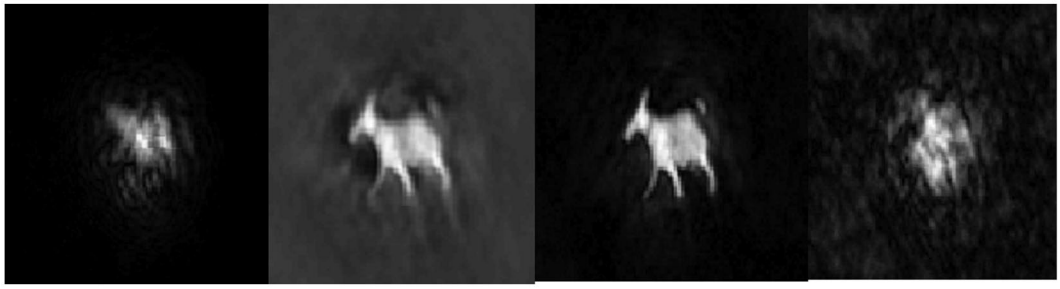

Figure 5. (a) Intensity of encrypted image using amplitude fingerprint in Figure 3(a), (c) decrypted image using the same fingerprint in Figure 3(a) and (c) processed output meeting the requirement of Equation (4b); (d) decrypted image using wrong fingerprint shown in Figure 3(f).

to the overall system. There are three 'secret frequencies', namely the two AOM central operating frequencies at 40.25 and 40 MHz, and the heterodyne frequency at 25 kHz in contrast to the highly idealized case shown in Figure 1 where only one frequency Ω is employed.

BE_1 and BE_2 are two beam expanders. $p_1(x, y)$ is on the front focal plane of lens L_1, which consists of a fingerprint image $Fp(x, y)$ and a positive lens L_f with focal length f_0 and hence $p_1(x, y) = Fp(x, y)\exp[jk_0(x^2 + y^2)/2f_0]$. Therefore, we have chosen $M(x, y) = \exp[jk_0(x^2 + y^2)/2f_0]$ instead of a random phase mask used in the simulations because that is something convenient to find in a laboratory. We have used the fingerprint image, shown in Figure 3(a), as a cipher key. The other pupil used is a pinhole, i.e. $p_2(x, y) = \delta(x, y)$ and with that kind of a pupil function, it will produce a uniform beam on the object, and hence the output of BE_2 now goes directly to the object to effectuate the condition of $p_2(x, y) = \delta(x, y)$. The two beams coming from BE_1 and BE_2 are then combined by beam splitter BS_2 and projected to the object through an x–y scanner (xy–M) as shown in Figure 4. The transmitted light from the object is then finally collected by lens L_2 onto photo-detector PD_1 to provide a signal to the lock-in amplifier.

The other part of the combined beam from beam splitter BS_2 will be reflected by mirror M_3 to photo-detector PD_2, which produces a reference electrical signal for the lock-in amplifier. The coding distance z_c and decoding distance z_d are the same, z_c = 30 cm. The focal length f_0 of L_f and f of L_1 is 75.6 and 300 mm, respectively. The object to be encrypted is a 5 mm × 6 mm transparency of a goat image, as shown in Figure 3(b). Figure 5(a) shows the intensity of the encrypted complex hologram of the goat image, i.e. the output given by Equation (1), $i(x, y; z_c)$, using the knowledge of the in-phase current $i_c(x, y; z_c)$ and the quadrate current $i_s(x, y; z_c)$ from the lock-in amplifier (see Figure 4). It can be seen that the pattern is seriously disturbed and no useful information about the original image can be identified. Therefore, the object can be encrypted using the amplitude fingerprint image as the encryption key in the system.

In the decryption stage, we have used a pinhole to replace the object and obtain the pinhole hologram, $i(x, y; z_d)$, i.e. the PSF of the encryption machine, to decrypt the encrypted image. The corresponding decrypted image, using Equation (4a), is shown in Figure 5(b). We can see that the object pattern is successfully decrypted. However, the image is blurred and of low contrast. The reason is that Equation 4b) is not met with amplitude keys.

To compensate this blurring effect, we have digitally processed the decrypted image by dividing $|Fp|^2$ within the inverse transform in Equation (4a) as discussed in the last section. Figure 5(c) shows the processed output. We have also obtained another pinhole hologram, which corresponds to the wrong decryption key, to decrypted the original image, namely $p_1(x, y) = Fp(x, y)$ by removing the positive lens L_f in the experiment and therefore only the fingerprint image is left to be used in the decryption system. The corresponding decrypted image using the wrong key is shown in Figure 5(d). Because the measured PSF, i.e. the pin hole hologram, is not exactly the same as that obtained from the encryption stage, the decrypted image is seriously distorted. Therefore, in the decryption process, the decryption pupil parameter, namely the decrypted key, should be completely the same as that used for encryption.

5. Conclusion

In summary, we have proposed optical scanning cryptography with amplitude fingerprint images as a cipher key. Biometric information cannot be retrieved directly from templates and offers a reliable and convenient solution to the problem of user authentication. While other novel implementation of optical scanning cryptography has been proposed, we feel the practical implementation of the idea presented in the present paper offers additional merits in terms of increased security. The increased security comes

from the use of extra parameters in the implemented system in additional to the amplitude fingerprint key. These extra parameters are the 'secret frequencies' mentioned in the last section. If one gets hold of the encryption machine, the decryption key cannot be easily retrieved by asking it to encrypt a point source which is not the case with all existing linear encryption systems. In the present practical implementation, two acousto-optic modulators (AOMs) are used to provide heterodyne detection in the overall crypto-system. AOMs have centre frequencies ranging from MHz to GHz which is difficult to identify concurrently. In addition, the heterodyne frequency can be in the range even down from kHz to GHz. In the present implementation, we have used two AOMs to obtain heterodyne frequency of the order of kHz. These three secret frequencies (two center frequencies plus the heterodyne frequency) can be considered as extra keys to the overall hybrid crypto-system. Besides, when one is trying to obtain the PSF with the encryption machine, the pin hole must be placed correctly, i.e. the value of z_d must be at z_c, the coding distance. Therefore, the encrypted image is a function of additional four parameters in addition to the random phase function on the pupil plane and the biometric amplitude fingerprint key. The proposed practical implementation therefore can provide a new strategy for optical cryptography and information security applications. We have provided the first experimental results on optical scanning cryptography using heterodyning technique. Subsequent extensive evaluation of the technique should be performed to illustrate the effectiveness and applicability of the technique. We plan to investigate this aspect in the near future.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Shanghai Municipal Natural Science Foundation under [grant number 14ZR1430700] and the National Nature Science Foundation of China under [grant number 61307008, 11174304, 61575124, 61475168).

References

(1) Matoba, O.; Nomura, T.; Perez-Cabre, E.; Millan, M.Í.S.; Javidi, B. *Proc. IEEE* **2009**, *97*, 1128–1148.
(2) Shi, L.; Guo, C.; Sheridan, J.T. *Opt. Laser Technol.* **2014**, *57*, 327–342.
(3) Sanpei, T.; Shimobaba, T.; Kakue, T.; Endo, Y.; Hirayama, R. *Opt. Commun.* **2016**, *361*, 138–142.
(4) Shi, Y.; Li, T.; Wang, Y.; Gao, Q.; Zhang, S.; Li, H. *Opt. Lett.* **2013**, *38*, 1425–1427.
(5) Yan, A.; Hu, Z.; Poon, T.-C. *J. Shanghai Normal Univ.* **2015**, *44*, 25–32.
(6) Refregier, P.; Javidi, B. *Opt. Lett.* **1995**, *20*, 767–769.
(7) Kong, D.; Shen, X. *Opt. Laser Technol.* **2014**, *57*, 343–349.
(8) Unnikrishnan, G.; Joseph, J.; Singh, K. *Opt. Lett.* **2000**, *25*, 887–889.
(9) Situ, G.; Zhang, J. *Opt. Lett.* **2004**, *29*, 1584–1586.
(10) Liu, J.; Xu, X.; Wu, Q.; Sheridan, J.T.; Situ, G. *Opt. Lett.* **2015**, *40*, 859–861.
(11) Muhammad, R.A. *Appl. Opt.* **2012**, *51*, 3006–3016.
(12) Liu, Z.; Xu, L.; Lin, C.; Liu, S. *Appl. Opt.* **2010**, *49*, 5632–5637.
(13) Zhu, N.; Wang, Y.; Liu, J.; Xie, J.; Zhang, H. *Opt. Exp.* **2009**, *17*, 13418–13424.
(14) Chen, W.; Chen, X.D.; Sheppard, C.J.R. *Opt. Lett.* **2010**, *35*, 3817–3819.
(15) Javidi, B.; Nomura, T. *Opt. Lett.* **2000**, *25*, 28–30.
(16) Li, J.; Zheng, T.; Liu, Q.; Li, R. *Opt. Commun.* **2012**, *285*, 1704–1709.
(17) Chang, H.T.; Tsan, C.L. *Appl. Opt.* **2005**, *44*, 6211–6219.
(18) Li, J.; Li, H.; Li, J.; Pan, Y.; Li, R. *Opt. Commun.* **2015**, *344*, 166–171.
(19) Seok, H.J.; Sang, K.G. *J. Opt. Soc. Korea* **2012**, *16*, 263–269.
(20) Carnicer, A.; Montes-Usategui, M.; Arcos, S.; Juvells, I. *Opt. Lett.* **2005**, *30*, 1644–1646.
(21) Kumar, P.; Kumar, A.; Joseph, J.; Singh, K. *Opt. Lett.* **2009**, *34*, 331–333.
(22) Poon, T.-C; Kim, T; Doh, K. *Appl. Opt.* **2003**, *42*, 6496–6503.
(23) Tajahuerce, E.; Lancis, J.; Javidi, B.; Andrés, P. *Opt. Lett.* **2001**, *26*, 678–680.
(24) Zang, J.; Xie, Z.; Zhang, Y. *Opt. Lett.* **2013**, *38*, 1289–1291.
(25) Bondareva, A.P.; Evtikhiev, N.; Krasnov, V. *Radiophy. Quantum Electron.* **2015**, *57*, 619–626.