Optics Communications 420 (2018) 34–39

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Computational ghost imaging encryption based on fingerprint phase mask

Jinan Zhu [a], Xiulun Yang [a,*], Xiangfeng Meng [a], Yurong Wang [a], Yongkai Yin [a], Xiaowen Sun [a], Guoyan Dong [b]

[a] *Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China*

[b] *College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China*

ARTICLE INFO

Keywords:
Computational ghost imaging encryption
Fingerprint phase mask
Digital holography

ABSTRACT

A computational ghost imaging encryption method based on fingerprint phase mask is proposed. In this work, we introduce one's fingerprint information into computational ghost imaging for the first time. The phase mask key in computational ghost imaging encryption is generated by a fingerprint image using digital holography method. As the phase key links to one's fingerprint which is uniqueness, this method offers a significant improvement for the security of computational ghost imaging encryption. Furthermore, because a fingerprint can verify one's identity, the proposed method can combine identity authentication with image decryption. In addition, the distances of recording and reconstruction during digital holography can be saved as additional keys which make the encryption system more secure. To verify the feasibility, security and ability to resist noise attack, some computer simulations are performed.

1. Introduction

Ghost imaging has drawn more and more attention since Pittman [1] proposed optical imaging using two-photon quantum entanglement in 1995. In 2002, Bennink [2] proved that coincidence imaging can be achieved experimentally with a classical source which opened possibility to practical applications of ghost imaging. In ghost imaging with thermal light, a beam of thermal light is divided into two beams, one of which is signal beam and the other is reference beam. The signal beam illuminates an object and then is detected by a bucket detector (BD) while reference beam is detected by a Charge Coupled Device (CCD) directly. The information of the object can be reconstructed by correlating the intensities detected by BD and CCD [3,4]. To simplify the system of ghost imaging, Shapiro proposed computational ghost imaging in 2008 [5] in which only a signal beam is needed and reference intensities can be calculated by computer but not are detected by a CCD. In 2009, Katz applied compressive sensing to ghost imaging reducing the number of measurements for image recovery [6].

Ghost imaging has been applied to optical image encryption recently as it can transfer images to real vectors instead of complex images comparing to traditional optical image encryption methods based on double random phases. Clemente proposed computational ghost imaging for optical encryption in 2010 [7] in which the information of an object is encrypted into the intensities of signal light. There were also many other achievements in ghost imaging encryption [8–15]. In 2011, Duran applied compressive ghost imaging to optical encryption which overcome the limitation that it required high acquisitions times in conventional ghost imaging encryption [16]. The key technology of ghost imaging encryption is the management and transmission of phase mask keys which are used to encrypt and decrypt images. For the security of phase keys, there were some papers in which phase keys were linked to ones fingerprint. In 2012, Takeda combined fingerprint image with double random phase encoding [17] in which the second phase key of optical encryption system was the phase generated by a fingerprint image using Fourier transform. This method improved the security of encryption system a lot as the fingerprint is unique. Verma proposed the generation of biometric phase mask in 2016 [18] in which biometric phase masks were generated by digital holography method with one's fingerprint image, and the randomness of biometric phase mask was proved. Then in 2017, Sinha applied the optically generated biometric phase mask to double random phase encryption [19] which allows for decrypting information together with user authentication.

As far as we are concerned, there is no published paper applying fingerprint to ghost imaging encryption. In this paper, we first introduced one's fingerprint phase into computational ghost imaging encryption in which the secret image can be encrypted into real intensity values. In the encryption process, a defocus reconstructed image linked to ones

[*] Corresponding author.
E-mail address: xlyang@sdu.edu.cn (X. Yang).

https://doi.org/10.1016/j.optcom.2018.03.014
Received 20 October 2017; Received in revised form 6 March 2018; Accepted 7 March 2018

fingerprint can be obtained by off-axis digital holography. The reconstructed information contains DC term with separated real and virtual image. So the real fingerprint image can be easily cut out and the phase information of the real fingerprint can be extracted [20,21]. The phase can be used as the fingerprint phase mask key (FPM) in computational ghost imaging encryption. As the phase keys link to one's fingerprint which is unique, the security of the encryption system gets improved greatly. However, thousands of phases are needed in computational ghost imaging, so we applied logistic map into ghost imaging which can generate other phases with only one initial phase. So the keys storage space can be reduced a lot. Furthermore, the distances of recording and reconstruction during off-axis digital holography can also be saved as additional keys which improve the security of encryption system. In the decryption process, the authorized user can decrypt the image correctly with his fingerprint and correct distance keys. The rest of the paper is organized as follows. First, the system principles are described in Section 2 which contains the generation of FPM, computational ghost imaging encryption with FPM and decryption process. Then computer simulations of computational imaging encryption with FPM are performed to verify the feasibility, security, resistance to noise attack in Section 3. Finally, we draw our conclusion.

2. System principles

2.1. The generation of FPM

In this method, we generate FPM using a fingerprint image by off-axis digital holography. The generation process of FPM is shown in Fig. 1. In this paper, we set the distance positive when light propagates forward along z-axis. A Fingerprint image is putted on the object plane, a CCD locates on the recording plane which is z_0-distance away from the object plane, and the reconstructed image can be calculated by computer on the reappearance plane. First, a beam of plane wave light illuminates a fingerprint image. According to the Fresnel diffraction theory [22,23], the complex amplitude distribution *U(x, y)* which is the object light field on the recording plane can be written as:

$$U(x,y) = \frac{1}{i\lambda z_0}\exp(i\frac{2\pi}{\lambda}z_0)\iint U_0(x_0,y_0) \times\exp\left\{\frac{i\pi}{\lambda z_0}\left[(x-x_0)^2+(y-y_0)^2\right]\right\}dx_0dy_0, \tag{1}$$

where λ is the wave length of the object light, and $U_0(x_0,\ y_0)$ is the amplitude distribution of fingerprint image. Then, a reference beam light which is not parallel with object beam interferes with object beam on recording plane. The interference pattern $I\ (x,\ y)$ which is called hologram can be obtained on the recording plane [24,25] and it is shown as:

$$I(x,y) = \left|U(x,y)+U_r(x,y)\right|^2, \tag{2}$$

in which, $U_r(x, y)$ denotes reference light which can be written as:

$$U_r(x,y) = A_r\exp(i\varphi_r), \tag{3}$$

where A_r and φ_r is the amplitude and the phase of reference light respectively. And φ_r can be denoted as:

$$\varphi_r = \frac{2\pi}{\lambda}(x\cos\alpha + y\cos\beta + z\cos\gamma), \tag{4}$$

where α, β, γ is the angle between reference light and x-axis, y-axis and z-axis, respectively.

We set z_1 as the distance from recording plane to the reappearance plane. According to off-axis digital holography, we can get the focused reconstructed virtual object image for $z_1 = -z_0$, where the original object was located. When $z_1 = z_0$, the focused conjugated real image of the original object image can be obtained. The reconstructed image which includes DC term and separated virtual and real image can be reconstructed by simulating the Fresnel diffraction of hologram on the reappearance plane [26]. The reconstructed complex amplitude U' (ξ, η) can be written as:

$$U'(\xi,\eta) = \frac{1}{i\lambda z_1}\exp(i\frac{2\pi}{\lambda}z_1)\iint I(x,y) \times\exp\left\{\frac{i\pi}{\lambda z_1}\left[(\xi-x)^2+(\eta-y)^2\right]\right\}dxdy. \tag{5}$$

The real fingerprint image including amplitude and phase information cut out from the reconstructed image can be expressed as:

$$U''(\xi,\eta) = A\exp(i\varphi), \tag{6}$$

in which, A denotes the amplitude of reconstructed real fingerprint while φ denotes the phase of it. And the fingerprint phase which ranges in $(-\pi,\ \pi)$ can be extracted using following equation:

$$\varphi = \arg(U''(\xi,\eta)). \tag{7}$$

2.2. Computational ghost imaging encryption with FPM

In computational ghost imaging, we first generate FPM as initial phase using off-axis digital holography method described in Section 2.1. So the fingerprint used in the generation of FPM can be used as main key. Besides, the recording distance and reconstruct distance in digital holography can be saved as additional keys for decryption. In conventional ghost imaging encryption, the key technology is the transmission and management of the phase keys. However, it needs big storage space to store the phase keys. In this paper, we adopt logistic map to generate M phase keys P_j which are shown as:

$$P_j = \mu P_{j-1}(E-P_{j-1}), (j = 1,2,3,\ldots,M). \tag{8}$$

j is the jth measurement of computation ghost imaging, μ is the control parameter of logistic map, E is a matrix whose element values are one and dimension is the same as P_0, and P_0 is the initial FPM generated by off-axis digital holography which is the normalization of φ. P_0 can be calculated by

$$P_0 = \frac{\varphi-\min(\varphi)}{\max(\varphi)-\min(\varphi)}, \tag{9}$$

in which, min (φ) denotes the minimum value of φ, and max(φ) is the maximum value of φ. According to the property of logistic map, the obtained phase masks P_j range in (0, 1) randomly when μ rang in (0.37, 4.0) [27,28]. In this way, only the initial FPM and the control parameter of logistic map are needed to decrypt the image.

Fig. 2 shows the process of computational ghost imaging encryption with FPM, in which the phase masks generated by FPM with logistic map are uploaded to SLM and modulate the phase of collimated signal plane wave. The object plane is z-distance from SLM. According to Fresnel diffraction theory, the light field distribution of signal light in front of object plane is the same as reference light calculated by computer which can be shown as:

$$I_j(x,y) = \left|\mathrm{FrT}_z\left\{\exp\left[i2\pi P_j\right]\right\}\right|^2. \tag{10}$$

FrT_z denotes Fresnel diffraction transform of z-distance. The signal light intensities detected by BD after the object can be written as [3]:

$$B_j = \sum_{y=1}^{m}\sum_{x=1}^{n} T(x,y)\,I_j(x,y), \tag{11}$$

in which $T\ (x,\ y)$ is the amplitude distribution of the plaintext image on object plane whose dimension is $m\times n$. Finally, the $m\times n$-dimension image is encrypted into an $M\times 1$-dimension vector and is conveyed to the legal user with the distance keys which are adopted during the generation process of FPM.