Optics Communications 365 (2016) 180–185

Contents lists available at ScienceDirect

Optics Communications

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

Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging

Sheng Yuan [a],*, Jianbin Yao [a], Xuemei Liu [a], Xin Zhou [b], Zhongyang Li [a]

[a] Department of Information and Engineering, North China University of Water Resources and Electric Power, Zhengzhou 450011, China
[b] Department of Opto-electronics Science and Technology, Sichuan University, Chengdu 610065, China

ARTICLE INFO

Article history:
Received 29 October 2015
Received in revised form
1 December 2015
Accepted 11 December 2015

Keywords:
Optical cryptography
Chosen-plaintext attack
Computational ghost imaging

ABSTRACT

Optical cryptography based on computational ghost imaging (CGI) has attracted much attention of researchers because it encrypts plaintext into a random intensity vector rather than complexed-valued function. This promising feature of the CGI-based cryptography reduces the amount of data to be transmitted and stored and therefore brings convenience in practice. However, we find that this cryptography is vulnerable to chosen-plaintext attack because of the linear relationship between the input and output of the encryption system, and three feasible strategies are proposed to break it in this paper. Even though a large number of plaintexts need to be chosen in these attack methods, it means that this cryptography still exists security risks. To avoid these attacks, a security enhancement method utilizing an invertible matrix modulation is further discussed and the feasibility is verified by numerical simulations.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Optical processing techniques have been widely applied in the field of information security since the pioneering work reported by Refregier and Javidi on the double random-phase encoding (DRPE), owing to its inherent advantages such as high-speed parallel processing capability and muti-dimensional operation [1–14]. Furthermore, optical procedures are the natural medium to deal with images or holograms and benefit from continuous advantages in electro-optic devices. As the accompanying complementary opposites, the corresponding security analyses have also been carried out and promoted the further development of optical encryption techniques [15–20]. However, most of these existed optical cryptosystems based on the random-phase encoding encrypt the plaintext image into a complex-valued function, which will bring inconvenience in data transmission and storage.

On the contrary, optical encryption scheme based on the computational ghost imaging (CGI) has noticeably reduced the number of bits required to transmit the image, because the encryption of the object image is not a complex-valued matrix but simply an intensity vector [21]. In the CGI-based encryption scheme, a spatially coherent laser beam is modified by a set of random-phase masks and repeatedly illuminates on a secret image, then the transmitted lights are recorded by a bucket detector (a single-pixel sensor without spatial resolution) to obtain a ciphertext. A sequence of random seeds used to generate the random-phase masks are taken as the key. The secret image is retrieved by correlating the ciphertext with the intensity patterns computed by the key in the reference beam. In the past few years, the CGI-based security technique has achieved rapid development and some new schemes are also derived [22–26]. For examples recently, a higher security and better robustness optical encryption based on CGI with QR code has been proposed [23]. To improve the efficiency for data storage or transmission and enhance the security of the system, CGI-based encryption techniques using labyrinth-like phase modulation patterns and compressive sensing has also been investigated [24–26]. All these encryption techniques derived from Ref. [21] have effectively enlarged the application domain of CGI for optical security. However, we find that the CGI-based encryption scheme is vulnerable to chosen-plaintext attack because of the linear relationship between the input and output of the encryption system. As long as enough plaintexts are chosen, the key can be retrieved by solving a set of linear equations. In order to overcome this security risk, a security enhancement strategy utilizing an invertible matrix modulation is further investigated. The feasibility and security of the proposed scheme

* Corresponding author.
E-mail address: shn.yuan@sohu.com (S. Yuan).

http://dx.doi.org/10.1016/j.optcom.2015.12.013
0030-4018/© 2015 Elsevier B.V. All rights reserved.

are verified by numerical simulations.

2. CGI-based encryption scheme

The schematic diagram of the CGI-based encryption scheme [21] is shown in Fig. 1. A collimated laser beam is generated for illumination. The light firstly passes through a spatial light modulator (SLM), which is controlled by computer to introduce a series of independent random-phase profiles as the secret keys of the encryption scheme. Then, the source is splitted into two beams, object and reference, which are measured by a bucket detector (without spatial resolution) and a charge coupled device (CCD), respectively.

For one random-phase profile $\phi_k(x, y)$ ($k = 1, 2, 3, \cdots, K$) generated by the SLM, the free-space propagation field at the distance z from the SLM can be described by

$$E_k(\xi, \eta) = \exp\left[j\phi_k(x, y)\right] \otimes h(x, y; z) \tag{1}$$

where (ξ, η) denotes the coordinate on the CCD plane, $j = \sqrt{-1}$, $\otimes$ represents the convolution operation, and $h(x, y; z)$ is the point pulse function of the Fresnel transform which can be described by

$$h(x, y; z) = \frac{\exp(j2\pi z/\lambda)}{j\lambda z} \exp\left[\frac{j\pi}{\lambda z}\left(x^2 + y^2\right)\right] \tag{2}$$

where z is the Fresnel propagation distance between the SLM and the CCD plane (or the object plane), λ denotes wavelength of the laser. Thus, the intensity pattern detected by CCD can be calculated by

$$I_k(\xi, \eta) = |E_k(\xi, \eta)|^2 \tag{3}$$

Actually as the CGI notes, the intensity patterns at the reference arm are unnecessary to be detected by CCD, which can be replaced with a “virtual detector” by calculating the propagation of the field of the reference beam (indicated by the dashed box in Fig. 1).

In the object beam, the light illuminates the object with the transmission function $T(\xi, \eta)$, and the collected intensities measured by the bucket detector can be described by

$$B_k = \int d\xi d\eta I_k(\xi, \eta) T(\xi, \eta) \tag{4}$$

The operation is repeated K times for K different phase profiles $\phi_k(x, y)$. Thus, the object information is encoded in a vector of K components $\{B_k\}$, i.e., ciphertext.

In order to reconstruct the object, the computed intensity patterns at the object plane $\{I_k(\xi, \eta)\}$ are cross-correlated with the intensities measured by the bucket detector $\{B_k\}$, i.e.,

$$\tilde{T}(\xi, \eta) = \frac{1}{K}\sum_{k=1}^{K}\left(B_k - \langle B\rangle\right) I_k(\xi, \eta) \tag{5}$$

where $\tilde{T}(\xi, \eta)$ is the reconstructed object image, and $\langle B\rangle$ is the average value for the measured intensity sequence $\{B_k\}$.

3. Vulnerability of the CGI-based encryption scheme

Chosen-plaintext attack is an attack mode in cryptanalysis. In this method, the attacker can choose a certain number of plaintexts in advance, encode them by the encryption scheme, and get the corresponding ciphertexts. The purpose for the attacker is to obtain some information about the encryption scheme through this process, so that they can effectively decrypt the ciphertexts encoded by the same encryption scheme (as well as the related key) in the future.

For the CGI-based encryption scheme proposed in Ref. [21], as can be seen from Eq. (5), the decryption key is the series of intensity patterns $\{I_k(\xi, \eta)\}$ computed by the encryption key $\{\phi_k(x, y)\}$. In other words, as long as attacker acquires the intensity patterns $\{I_k(\xi, \eta)\}$ through a certain means, the CGI-based encryption scheme will be broken. According to the chosen-plaintext attack mode, there may be three strategies to break the encryption scheme.

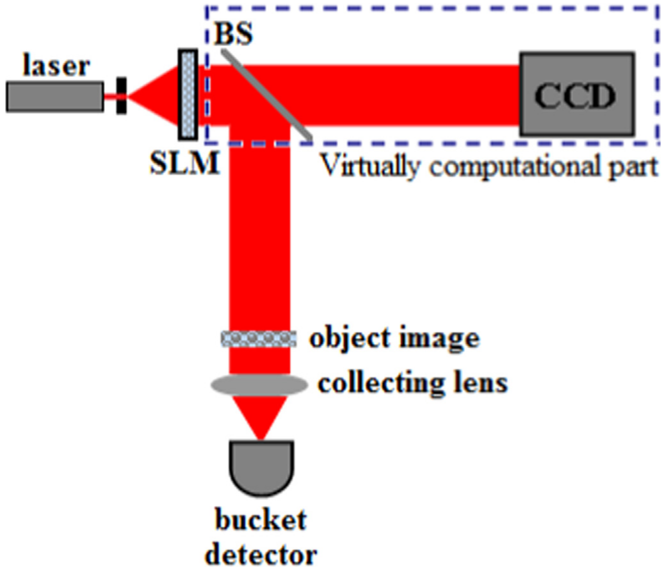

Fig. 1. Schematic of the CGI-based encryption scheme. SLM: spatial light modulator, BS: beam splitter, CCD: charge coupled device (CCD).

Strategy 1. In the CGI-based encryption scheme, the sequence $\{B_k\}$ is the linear superposition of the product of $\{I_k(\xi, \eta)\}$ and $T(\xi, \eta)$ (known from Eq. (4)), which forms a set of linear equations. If a series of linearly independent matrices with real-valued elements are selected as the plaintexts to be encrypted, the relationship between the input and output of the encryption system will be described by a set of nonhomogeneous linear equations, which can be solved by conventional linear least-squares methods [27]. The solutions of the equations are indeed the intensity patterns $\{I_k(\xi, \eta)\}$. Thus, the encryption scheme will be broken.

Strategy 2. As can be seen from Eqs. (4) and (5), $I_k(\xi, \eta)$ and $T(\xi, \eta)$ are symmetrical and they play the same role in ghost imaging. If one chooses a series of random real-valued masks $\{T_k(\xi, \eta)\}$ to modulate the intensity pattern $I_k(\xi, \eta)$, thus Eq. (4) becomes

$$B'_k = \int d\xi d\eta I_k(\xi, \eta) T_k(\xi, \eta) \tag{6}$$

and $I_k(\xi, \eta)$ can be ghostly imaged by

$$\tilde{I}_k(\xi, \eta) = \frac{1}{K}\sum_{k=1}^{K}\left(B'_k - \langle B'\rangle\right) T_k(\xi, \eta) \tag{7}$$

where $\tilde{I}_k(\xi, \eta)$ is the reconstructed intensity pattern of $I_k(\xi, \eta)$, and $\langle B'\rangle$ is the average value for the measured intensity sequence $\{B'_k\}$. Then the encryption scheme can also be broken.

Strategy 3. For a spatial case, if one chosen plaintext T_k only has a pixel valued 1 and other 0 (schematically shown in Fig. 2), B_k measured by the bucket detector is the intensity of $\{I_k(\xi, \eta)\}$ in the position of the 1-valued pixel (known from Eq. (4)). All the values of the intensity pattern $I_k(\xi, \eta)$ can be acquired by removing the 1-valued pixel in turns in the whole chosen plaintext, which is shown schematically in Fig. 2. Thus the decryption key $\{I_k(\xi, \eta)\}$

Download English Version:

https://daneshyari.com/en/article/1533461

Download Persian Version:

https://daneshyari.com/article/1533461

Daneshyari.com