Optics and Lasers in Engineering 111 (2018) 58–64

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical encryption based on ghost imaging and public key cryptography

Kang Yi, Zhang Leihong*, Zhang Dawei

University of Shanghai for Science and Technology, Shanghai, China

ARTICLE INFO

Key Words:
Ghost imaging
Optical encryption
Phase object
Public key cryptography

ABSTRACT

In this paper, according to the phase object in the ghost imaging has a stealth effect, we proposed an optical encryption method based on compressive ghost imaging and public key cryptography. This method solves the key distribution problem of ghost imaging encryption, and reduces the additional cost of establishing security channels. The simulation results verify the feasibility, security and robustness of the proposed encryption scheme. This technique can be immediately applied to encryption and data storage with the advantages of high-safety, high-robustness and low-cost.

1. Introduction

The development of modern communication technologies has led to increased attention being paid to information security. In the past 20 years, many optical imaging technologies have been applied to encrypt images, as they can offer the capability of high speed and the possibility of hiding data in multiple dimensions (such as phase, wavelength, spatial frequency, or polarization) [1]. The classical double random-phase encoding (DRPE) based on the 4f optical setup has aroused great enthusiasm of scholars for the study of optical information security. Various algorithms, such as phase truncation, phase retrieval and phase place have been further developed [2–6]. However, recent reports point out that the DRPE systems are vulnerable to chosen-ciphertext, known-plaintext and chosen –plaintext attacks. [7–10]

Ghost imaging (GI) offers great potentiality, with respect to standard imaging, to obtain the imaging of objects located in optically harsh or noisy environment. Since 1995, Pittamn achieved GI with entangled photon pairs. The GI technology has suffered a rapid development [11–14]. In 2010, Pere Clemente applied GI to optical security [15]. In the past few years, optical encryption based GI has achieved rapid development. Duran et al combined GI with compressive sensing (CS) to encrypt and transmit 2D images to a remote party. This compressive sensing ghost imaging (CSGI) optical encryption technique is robustness to eavesdropping attacks preserving high-quality image fidelity and high speed operation [16]. In paper [17], this approach has the capability of encrypting ghost images by flexibly manipulating the position correlation of a pair of “signal” and “idler” beams. Chen et al. proposed a series of methods for optical encryption and information authentication based on GI, which broadened the application of GI [18–21]. Zhao et al. proposed a high performance optical encryption scheme based on computational GI with Quick Response (QR) Code and CS technique. The high error tolerance of QR code greatly improved the reconstructed image quality [22]. In the other paper [23], an optical image transformation and encryption scheme is proposed based on double random-phase encoding and CSGI techniques. It overcame the blurring defect of the decryption image in the GI-based encryption. Sun et al. proposed a novel optical image encryption scheme utilizing computational GI based on a series of the specially designed phase-only masks [24]. In another study [25], a novel technique for the simultaneous fusion, imaging and encryption of multiple objects using a single-pixel detector is proposed. Meng et al. proposed a multiple-image encryption method via lifting wavelet transform and exclusive OR (XOR) operation, which is based on a row scanning CSGI scheme [26]. However, optical methods based on GI are symmetric encryption schemes, that is to say decryption and encryption require the same key. The security of information is threatened if the key is stolen. At the same time, in order to ensure the key security, whether establishes security channels or takes additional security measures will increase costs.

In this paper, according to the phase object in the GI system has a stealth effect, we propose an optical encryption method based on CSGI and public key cryptography. In the encryption system, Alice is and encipherer, Bob is a receiver. Bob uses RSA algorithm to generate the public key and the private key, and transfers the public key to Alice. Alice adds a phase object to the GI system and uses this system to encrypt plaintext. The phase object and its location information are keys, and Alice uses the public key to encrypt them. Alice transfers encrypted information to Bob through the common channel. Bob uses the private key to decrypt the encrypted phase object information, and finally uses CS to decrypt the encrypted plaintext information. The simulation results verify the feasibility, security and robustness of the proposed encryption scheme. This scheme solves the problem of key distribution, and reduces the additional cost of establishing security channels. This scheme

* Corresponding author.
E-mail address: lhzhang@usst.edu.cn (Z. Leihong).

https://doi.org/10.1016/j.optlaseng.2018.07.014
Received 6 June 2018; Received in revised form 17 July 2018; Accepted 25 July 2018

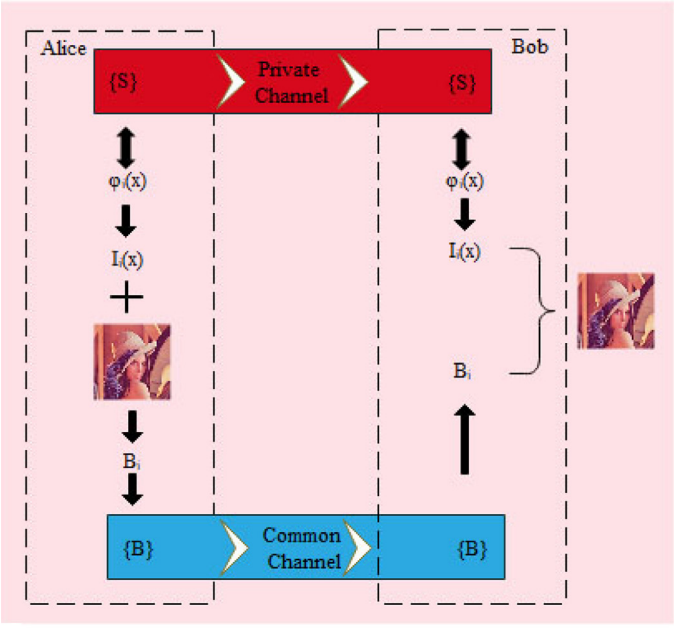

Fig. 1. Scheme of the encryption method based on GI. (a) Block diagram showing encryption/decryption procedure. (b) Experimental setup for GI.

combines the advantages of the RSA public key algorithm and GI encryption techniques and bring security and convenience for efficient information transmission.

2. Theory analysis

2.1. Optical encryption based on ghost imaging

In optical encryption based on computational GI, the scheme is illustrated in Fig. 1(a). Alice wants to transmit an encrypted imaging to Bob. Alice encrypted the image with the aid of GI illustrated in Fig. 1(b). A laser beam passes through a spatial light modulator (SLM), which

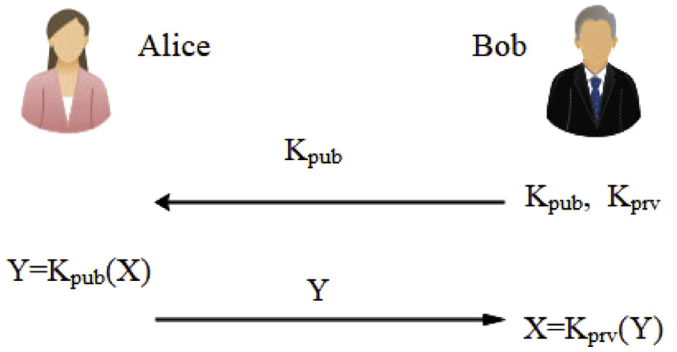

Fig. 2. The flowchart of the proposed public key cryptography.

introduces an arbitrary phase-only mask$\varphi_i(x)$. The modified beam illuminates the object $T(x)$, and the transmitted laser is collected by a bucket detector. This operation is repeated N times for N different phase profiles$\varphi_i(x)$. These phase profiles form the secret key$\{S\}$. Thus, the object information is encrypted in a vector of N components, containing the corresponding intensity values detected by the bucket detector,$\{B\}$. Next Alice transmits $\{B\}$ to Bob through a common channel, and transmits $\{S\}$ through a private channel (i.e. not necessarily secure).

In order to simplify calculating, we use one-dimensional coordinates. The corresponding intensity value B_i can be expressed as:

$$B_i = \int I_i(x)T(x)dx \tag{1}$$

where $I_i(x)$ denotes the intensity distribution, it can be calculated by $\varphi_i(x)$

$$I_i(x) = \left|E_{in}(x)\exp\left[j\varphi_i(x)\right] \otimes h_z(x)\right|^2 \tag{2}$$

here, $E_{in}(x)$is the complex field of the coherent light beam,$h_z(x)$ is the Fresnel propagation kernel at a distance $z$and $\otimes$ denotes the 2D convolution operation.

According to the conventional GI algorithm, Bob can recover the object information through following linear operation. Where $I_i(x)$ can be easily computed by Bob according to formula (2).

$$T'(x) = \langle I_i(x)B_i\rangle - \langle I_i(x)\rangle\langle B_i\rangle \tag{3}$$

In order to improve the reconstruction quality of ciphertext, CS algorithm can be used for decryption. The process is shown in formula (4). The CS theory states that it allows the recording an image consisting of N pixels using much fewer than N measurements if it can be transformed to a basis where most pixels have negligibly small values [27].

$$T'(x) = \arg\min : \|T(x)\|_{L1} \quad s.t.\ B_i = \int I_i(x)T(x)dx \tag{4}$$

2.2. Public key cryptography principle

Conventional optical encryption schemes are symmetrical, and thus the problem is that if the key is stolen, the security of the plaintext information is threatened. At the same time, the establishment of security channels or additional security measures will increase the cost of the system. The emergence of public-key cryptography provides us with new ideas for solving these problems.

In public key cryptography principle, the key is divided into a public key and a private key. Alice encrypts plaintext with a public key, and the Bob decrypts the ciphertext with a private key. Take the RSA algorithm in public key cryptography as an example [28]. As shown in Fig. 2. The specific procedure is as follows:

(1) Bob uses RSA algorithm to generate a pair of key(K_{pub}, K_{prv}). The private keyK_{prv} is kept by Bob and the public key $K_{pub}$is sent to Alice.