Optics Communications 426 (2018) 325–332

Contents lists available at ScienceDirect

Optics Communications

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

Authentication-based optical cryptosystem with noise-free information retrieval

Yi Qin [a,*], Qiong Gong [a], Hongjuan Wang [a], Zhipeng Wang [b]

[a] College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China
[b] College of Physical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China

ARTICLE INFO

Keywords:
Optical information encryption
Authentication
Diffractive-imaging-based encryption

ABSTRACT

It is widely recognized that the main challenges facing the optical cryptosystem are the speckle noise and the linearity-induced security leak. In this paper, we report, for the first time to our best knowledge, a novel approach to cope with these two problems. The original information is firstly transformed into a series of images by aid of an image-character map (ICM), where the one to one relationship between the 26 characters and 26 images is predefined Then, these images are encrypted in the diffractive-imaging-based encryption (DIBE) scheme and the multiple ciphertexts corresponding to them finally merge into a synthetic ciphertext (SC) via space multiplexing. For decryption, the recovered images are unrecognizable but can be authenticated by nonlinear correlation. The authenticated images are converted back to characters with the help of the ICM, and thus the primary information can be exactly retrieved. Numerical results are presented to demonstrate the practicality of the proposed security system.

1. Introduction

Optical information security techniques have received increasingly attention in the past several decades for their distinguished advantages, including multiple dimensions and parallel processing [1–3]. Optical cryptosystems supported by experimental results [4–6] or numerical simulations [7–10] have both made great progress in the past several years. A well-known optical encryption technique is double random phase encoding (DRPE) [11]. It places two random phase masks in the input and Fourier planes of an optical 4f scheme, and successfully transforms an arbitrary image into stationary white noise. The invention of DRPE revealed the huge potential for applying optical techniques to information security. Thereafter, variations of DRPE using Fresnel [12] or fractional Fourier [13] transforms are further developed. Besides DRPE, a lot of classical optical principles, such as interference [14], joint transform correlator (JTC) [15], diffractive imaging [16], had been explored for optical encoding and decoding. Recently, computational ghost imaging (CGI) also found its applications in information encryption, which has noticeably reduced the number of bits required to transmit the image in contrast to previous approaches [17–19].

Multiplexing is another marked merit reinforcing optical encryption, which provides the chance to enhance optical cryptosystem capacity without enlarging the ciphertext size. Up to now, several important multiplexing principles, such as wavelength multiplexing [20], polarization state multiplexing [21], and space multiplexing [22], have been investigated. Moreover, Gong et al. propose a flexible multiple-image encryption algorithm by utilizing data compression characteristics of log-polar transform, which explores a novel way for space multiplexing [23]. Recently, Zea et al. demonstrate a new method for cross-talk free selective reconstruction of individual objects from multiplexed optical field data [22]. In particular, Mosso et al. reported an all-optical encrypted movie [24].

Although great progress, as mentioned above, has been made, challenge remains. One disturbing problem is the speckle noise accompanying all the coherent optical cryptosystems [25]. In other words, the decoded results in such schemes are polluted by speckle noise, as a consequence of which potential users are loath to accept the optical protocols concerning the degraded primary inputs. As a solution of this issue, the quick response (QR) code is adopted as the container of the primary information before a standard optical encrypting procedure [25]. After the introduction of the QR code, some interesting applications were reported by integrating it into different optical cryptosystems [26,27]. In particular, based on QR code, Jaramillo et al. presented an optical cryptographic protocol in a multi-user environment [28]. Nevertheless, the QR code is demonstrated to be not an optimal data container from an error-correction coding perspective [29]. More recently, customized

[*] Corresponding author.
E-mail address: 641858757@qq.com (Y. Qin).

https://doi.org/10.1016/j.optcom.2018.05.079
Received 28 April 2018; Received in revised form 20 May 2018; Accepted 24 May 2018

data container emerges as a substitute of QR code and it motivates some new applications [30].

Another intractable issue is the security leak of optical cryptosystems. It is well known that optical propagation is essentially a linear process, and encryption through linear systems is too vulnerable to resist attacks. For instance, DPRE has been cracked by almost all the known types of cryptographic attacks [31–33]. In addition, cryptosystem based on JTC has also been demonstrated to be not robust under several attacks [34–36]. In particular, the diffractive-imaging-based encryption (DIBE), which had been believed to be with higher security, is breached by chosen-plaintext attack (CPA) [37]. Recently, nonlinear-correlation-based optical encryption schemes are widely studied. In these methods, the photon-limited [38] or sparse [39,40] version of the ciphertext is reserved and transmitted to the receiver. The recovered image is intended not for visualization but for verification by aid of nonlinear correlation. As a consequence, these schemes are provided with an additional layer of protection and thus become more robust against attacks. More recently, the CGI are combined with authentication to acquire high security encryption in a big data environment [19].

In this paper, we report, for the first time to our best knowledge, a high-security optical cryptosystem for noise-free information retrieval. The cryptosystem is designed based on the nonlinear-correlation-based authentication, space multiplexing and an image-character map (ICM). In traditional authentication system, the authentication is used to judge whether the tested result is coincident with the primary one, and this requires the sender and the receiver share the same database [38–40]. In this regard, all the currently available authentication schemes do not support freely information encryption. In order to get rid of this limit, we establish an ICM to endow the information of the 26 characters to 26 grayscale images, respectively. Since all the information can be expressed by the combination of the 26 characters, the encryption of information is translated into the authentication of images. We employ the DIBE scheme as a platform to carry out this new strategy. Numerical results show that the proposal not only possesses high security, but also enables lossless information retrieval. The proposal may pave a new way for overcoming the troublesome speckle noise in coherent optical cryptosystems.

2. Principle

2.1. The diffractive-imaging-based encryption and decryption

DIBE is a widely studied optical encryption scheme, and a typical architecture for illustrating it is shown in Fig. 1. The scheme includes three statistically independent random phase-only masks (POMs) that are used as encryption keys. They are placed in-line along the optical axis, and M2 separates d1 and d2 from M1 and M3 respectively. The input image U and M1 are located at the same plane, attaching to each other. When the input image is illuminated by the coherent light with a wavelength of λ, the diffraction field is successively modulated by M1, M2 and M3, and finally propagates to the output plane, where its intensity is recorded by the intensity-sensitive device (i.e. CCD). For convenience, symbols (x,y), (η,ξ), (p,q) and (μ,ν) are used to denote coordinates of the input image, M2, M3, and the CCD plane, respectively. The diffractive intensity pattern recorded by the CCD camera can be expressed as [41]:

$$I(\mu,\nu) = \Big|\mathrm{FrT}_\lambda\big[\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[U(x,y)\,M_1(x,y);d_1]\,M_2(\eta,\xi);d_2\}\,M_3(p,q);d_3\big]\Big|^2, \tag{1}$$

where FrT_λ means the Fresnel transform with regard to λ. $I(\mu,\nu)$ is treated as the ciphertext, while the POMs, the axis distances as well as the wavelength are regarded as the secret keys.

For decryption, we employ a median-filtering-based phase retrieval algorithm (MPRA) to recover the primary image. In the first step, a constant or random $T_n(x,y), n = 1$ is nominated as the initial estimation of the plaintext, which will then propagate forward to the CCD plane [41]:

$$U_n(\mu,\nu) = \mathrm{FrT}_\lambda\big[\mathrm{FrT}_\lambda\{\mathrm{FrT}_\lambda[T_n(x,y)\,M_1(x,y);d_1]\,M_2(\eta,\xi);d_2\}\,M_3(p,q);d_3\big]. \tag{2}$$

After that, the square root of $I(\mu,\nu)$ is taken as the support constraint of real part of $U_n(\mu,\nu)$ and we can fabricate a new complex wavefront at the CCD plane [41]:

$$\overline{U_n(\mu,\nu)} = I(\mu,\nu)^{1/2}U_n(\mu,\nu)\,/\,|U_n(\mu,\nu)|\,. \tag{3}$$

This new complex amplitude propagates back to the input plane and the calculated intensity at the input plane is [41]

$$\overline{T'_n(x,y)} = \Big|\mathrm{FrT}_\lambda\Big[\mathrm{FrT}_\lambda\Big\{\mathrm{FrT}_\lambda\Big[\overline{U_n(\mu,\nu)};-d_3\Big]\,M_3^*(p,q);-d_2\Big\}\,M_2^*(\eta,\xi);-d_1\Big]\Big|^2, \tag{4}$$

where the superscript * denotes the complex conjugate. Then a low-pass filtering operation is performed on $\overline{T_n(x,y)}$ and we obtain a new estimated plaintext [41]:

$$\overline{T_n(x,y)} = \mathrm{LPFilter}\Big[\overline{T'_n(x,y)}\Big] \tag{5}$$

where LPFilter[ ] indicates the low-pass filtering function. Afterwards, $\overline{T_n(x,y)}$ is used as a new estimate to substitute $T_n(x,y)$ in Eq. (2). This procedure will always continue until the iterative error between $T_{n-1}(x,y)$ and $T_n(x,y)$, which can be expressed by

$$\mathrm{Error}_1 = \sum\big[|T_n(x,y)| - |T_{n-1}(x,y)|\big]^2, \tag{6}$$

becomes smaller than a preset threshold (δ). Once the recycle is terminated, $\overline{T'_n(x,y)}$ is considered as the decrypted image.

2.2. Multiple-image authentication with space multiplexing in DIBE

In 2011, Pérez-Cabré proposed to use photon-counting to record the ciphertext in DRPE. Although the decrypted image turns to be very vague and can hardly be recognized by naked eyes, it contains enough information of the primary image and can be successfully authenticated by nonlinear correlation [38]. The nonlinear correlation between the primary image and the decrypted image, which are respectively denoted by f_p and f_d, is defined as

$$NC(x,y) = IFT\left\{\left|FT\left(f_p\right)FT\left(f_d\right)\right|^{\omega-1}\times FT\left(f_p\right)FT(f)\right\}, \tag{7}$$

where FT denotes the Fourier transform and IFT denotes the inverse Fourier transform, ω defines the strength of the applied nonlinearity. The subsequent research [39] indicates that the sparse data of the ciphertext, which is a randomly selection from it, can also produce similar certifiable decrypted result. Inspired by these contributions, we infer that the decrypted result in DIBE can also be verified if a small contiguous area of the ciphertext is retained for decryption. To demonstrate this, we choose Peppers (256×256 pixels) as the image for test, which is shown in Fig. 2(a). Fig. 2(b) is the encoded result in the DIBE depicted in Fig. 1. Hereinafter, the simulations are all performed on the platform of MATLAB R2011a. The wavelength of the illumination is set as 632.8um. The axial distances d1, d2, and d3 all equal 100 mm. The threshold δ controlling the iteration number is predefined as 0.005. The selected partial ciphertext for decryption, which is a stripe containing 3% of the whole pixels, is displayed in Fig. 2(c). Since in such cases the iteration will not always converge, the calculation will stop if the maximum number of iteration reaches 1000. By using the MPRA, the decrypted result after 1000 iterations is shown in Fig. 2(d). Although it looks apparently different from the primary image, the nonlinear correlation result shown in Fig. 2(e) reveals its validity. So it can be claimed that an image verification method in DIBE has been described and demonstrated.