Optics Communications 346 (2015) 124–132

Contents lists available at ScienceDirect

Optics Communications

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

Optical interference-based image encryption using circular harmonic expansion and spherical illumination in gyrator transform domain

Qu Wang [a,*], Qing Guo [b], Liang Lei [a], Jinyun Zhou [a]

[a] School of Physics and Optoelectronic Engineering, Guangdong University of Technology, Guangzhou 510006, China
[b] Institute of Remote Sensing and Digital Earth, Chinese Academy of Sciences, Beijing 100094, China

ARTICLE INFO

Article history:
Received 10 January 2015
Received in revised form
13 February 2015
Accepted 21 February 2015
Available online 23 February 2015

Keywords:
Image encryption
Optical interference
Circular harmonic expansion

ABSTRACT

In this paper, a new optical interference-based encryption method using off-axis circular harmonic component (CHC) expansion and iterative phase retrieval algorithm in gyrator transform (GT) domain is proposed. Off-axis CHC expansion is employed to divide the inverse GT spectrum of primitive image into two parts: the zero-order CHC and the sum of the other CHCs. The sum term of CHCs is further encrypted into a complex image whose amplitude constraint is devised to be the amplitude of zero-order CHC by the iterative retrieval GT algorithm. The amplitude part of CHC is the final ciphertext which has rotation-symmetric distribution. Three phase-only keys, the main keys of this proposal, are also calculated during the digital encryption process. To recover the primitive image correctly, two identical ciphertexts placed in the two interference branch should be illuminated by two spherical waves with required parameters (wavelength and radius). Moreover, rotational center of ciphertexts must be placed in a predefined position, which is off the optical axis. The transform angles of GTs, the propagation parameters of spherical waves and the relative position of rotational center of ciphertext are sensitive additional keys for correct retrieval. Numerical simulation tests have been carried out to verify the effectiveness of the proposed scheme.

1. Introduction

In the past two decades, optical systems have been extensively studied and designed for the applications of information processing, such as pattern recognition and image security due to its parallel ability and high-speed processing [1–3]. One of the most popular optical encryption techniques is double random phase encoding (DRPE) proposed by Refregier and Javidi [1], which enables one to encode a primary image into a stationary white noise by placing two random phase keys in the input and Fourier planes, respectively. Due to its huge key space and robustness against brute force attack, a number of extensions of DRPE in the fractional Fourier domain (FrFT) [4,5], the Fresnel transform (FrT) domain [6] and the gyrator transform [GT] domain [7,8] have also been reported recently to further strengthen the security level with additional keys. Moreover, by combining with wavelength multiplexing based on lensless FrT holograms, a security-strengthened configuration for color image encoding can be easily constructed [9]. To alleviate the strict optical alignment, some DRPE systems based on configuration of joint transform correlator (JTC) [10,11] or joint fractional Fourier transform correlator (JFTC) [12,13] have been proposed. On the other hand, some modified schemes use structured instead of random phase mask to overcome the problem of axis alignment, and to enlarge the key space with some structure parameters [14,15]. These structured phase masks (SPM), generally, have a rotationally symmetric distribution and are made from a spiral phase plate [14] or a devil's vortex Fresnel lens (DVFL) [15].

Recently, Zhang and Wang reported a very simple interference-based method to encode a primitive image into two phase-only masks (POMs) without any time-consuming iterative computation involved [16]. The authorized users can retrieve the primitive image directly in an intensity recording device (CCD) by means of the interference of the two analytically obtained POMs. The earlier interference-based encoding (IBE) algorithm has an inherent problem, in which the silhouette information of the primitive image can be discerned when only one POM is employed for decryption. The silhouette problem is mainly because the phase information of transform spectrum of the primitive image is completely retained in the POMs [17]. To eliminate the silhouette problem, a number of algorithms have been proposed. However, most of them require time-consuming computation for post processing or a greater number of POMs [18,19]. With the expectation to thoroughly resolve this problem at the source, two different

[*] Corresponding author.
E-mail address: wq197893@163.com (Q. Wang).

http://dx.doi.org/10.1016/j.optcom.2015.02.040
0030-4018/© 2015 Elsevier B.V. All rights reserved.

triple-POM based methods have been reported recently, which do not need any time-consuming digital computation or post processing of POMs [17,20]. Furthermore, some IBE schemes have been devised for multiple-image or color image encryption by combining with polarized light encoding [21], POM multiplexing [22], position multiplexing [23] and phase-only encoding techniques [24]. Chen et al. devised a novel IBE scheme using three-dimensional phase retrieval and an FrFT-based IBE scheme [25], in which a series of random and fixed phase-only masks are applied in the optical paths, to enhance the security of conventional IBE algorithms [26,27]. Chen et al. proposed a method to encode pseudo color image using three-beam interference principle and common vector composition [28]. An encryption method based on multiple-beam interference principle and vector composition has also been introduced by them recently [29]. In this scheme, one can retrieve the original image only when all the phase-only keys are known. In addition, to alleviate the optical alignment and stability requirement in the encryption setup, a novel IBE scheme based on single-beam illumination has also been proposed in a recent work [30].

In this paper, we will propose a novel optical IBE scheme based on circular harmonic expansion technique and phase retrieval algorithm in the GT domain. To the best of the authors' knowledge, this is the first time that the circular harmonic expansion is adopted to design the optical IBE algorithms. It is well known that a single order circular harmonic component (CHC) of a reference image is extracted to generate the circular harmonic filter (CHF) for in-plane rotation-invariant pattern recognition [31,32]. It is worthy to be noted that a CHC has a central-symmetric configuration that is advantageous for optical axis alignment. Moreover, these CHCs are strongly related with the choice of the center of circular harmonic expansion. Shifting the coordinates of expansion center slightly, one can get totally different CHCs from the same image, which suggests that the relative position of CHC center to the optical axis of system can be considered as additional key to enhance the security level of encryption.

During the encryption process of our proposal, the primitive image combined with a random phase mask is inverse gyrator transformed digitally. Then the resultant spectrum is expanded into the sum of CHCs by off-axis CHC expansion, in which the CHC expansion center is selected to be at a predefined off-axis position that is only known by authorized user. Zero-order CHC of the inverse GT spectrum, amplitude of which will serve as the ciphertext of the first interference branch, is separated from the other non-zero-order CHCs. Next, using an iterative phase retrieval GT algorithm, we encrypt the rest part of the inverse GT spectrum into a complex field distribution, which will be used in the second interference branch for decryption. To realize the iteration, the amplitude of the target image is constrained to be the amplitude of the zero-order CHC intentionally. Meanwhile, during the above encoding process, we can get three phase-only functions that can be considered as the main decryption keys. For generation of the main phase keys, two spherical propagation factors with specific wavelength and radius are also involved as modulation factor. The encryption procedures should be completed digitally. To recover the secret image, both identical ciphertext (the amplitude of the zero-order CHC) are displayed in the input planes of two interference branches respectively with two phase-only keys placed behind immediately. Two coherent spherical waves with specific parameters are generated to illuminate the ciphtexts. In the second interference branch, the diffraction beam is gyrator transformed at certain transform angle and then modulated by the third phase-only key. The modulated result is combined with the diffraction beam in the first branch by a beam splitter and undergoes the second gyrator transform. The final decryption result is recorded by a CCD in the output plane. The decryption phase keys, the transform angles of GTs, the relative position of the rotational center of CHC to the optical axis, the wavelength and radius of spherical waves are the keys for decryption. The decryption procedures can be implemented at an optoelectronic hybrid platform. Numerical simulations have been conducted to demonstrate the feasibility of the system theoretically.

This article is arranged as follows. The encryption and decryption processes are presented in Section 2. The simulation results and discussions are given in Section 3. A brief conclusion is presented in Section 4.

2. Encryption principle

2.1. Gyrator transform

It is well documented in literature that canonical integral transforms are utilized for image encryption because the transform parameters, as additional keys, can enlarge the key space of encryption system greatly. As one of the canonical transforms, the GT was firstly introduced in the field of optical information processing by Rodrigo et al. [33,34]. The GT of a two-dimensional complex field function $o(x, y)$ can be mathematically expressed as

$$\begin{aligned} O(u, v) &= \mathcal{G}^{\alpha}\{o(x, y)\}(u, v) \\ &= \frac{1}{|\sin\alpha|} \\ &\quad \iint o(x, y)\exp\left(j2\pi\frac{(uv + xy)\cos\alpha - (xv + yu)}{\sin\alpha}\right)dxdy, \end{aligned} \tag{1}$$

where $\mathcal{G}^{\alpha}\{\}$ denotes the GT operator at transform angle α, and (x, y) and (u, v) are the input and output coordinates, respectively. In recent years, the GT has also been used for optical encryption in a variety of ways [7]. The GT can be implemented optically by using a cascaded architecture of three generalized lens [35]. Each generalized lens is a combination of two convergent thin cylindrical lenses of the same power. One can vary the transform angle conveniently by properly rotating the cylindrical lenses. The digital implementation of GT can be found in the studies of Pei [36] and Liu [37].

2.2. Image encryption and decryption

In our optical IBE algorithm, the encryption process is performed digitally while the decryption process can be implemented optically or digitally. Let the function $o(x_0, y_0)$ represent the normalized intensity distribution of the primitive image, which is first modulated by a random POM as below

$$o'(x_0, y_0) = \sqrt{o(x_0, y_0)}\,\exp\left[j2\pi\mathrm{rand}(x_0, y_0)\right], \tag{2}$$

where $\mathrm{rand}(x_0, y_0)$ represents a random function with uniform distribution in the range of [0, 1]. Note that here the origin of coordinate point (0,0) is located in the center of the image. Optical axis of instruments will pass this point at the decryption platform. Then the modulated primitive image $o'(x_0, y_0)$ is processed with an inverse gyrator transform at the transform angle $-\alpha$:

$$m(x_1, y_1) = \mathcal{G}^{-\alpha}\left\{o'(x_0, y_0)\right\} = \left|m(x_1, y_1)\right|\ \exp\left[j\varphi_m(x_1, y_1)\right], \tag{3}$$

where $\|$ denotes the modulus operator and $\varphi(x_1, y_1)$ is the phase of the inverse gyrator transform spectrum. As pointed out by Wang [17], inherent silhouette problem in the previous IBE schemes is mainly due to the phase information of $m(x_1, y_1)$. To smooth away the side effect of $\varphi_m(x_1, y_1)$, we introduce another RPM $\exp\left[j\phi(x_1, y_1)\right]$, where $\phi(x_1, y_1)$ is a random phase distribution