Optics Communications 410 (2018) 468–474

Contents lists available at ScienceDirect

Optics Communications

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

Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding

Jun Wang [a], Xiaowei Li [a], Yuhen Hu [b], Qiong-Hua Wang [a,*]

[a] School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
[b] Department of Electrical & Computer Engineering, University of Wisconsin-Madison, Madison, WI 53706, USA

ARTICLE INFO

Keywords:
Optical encryption
Phase-retrieval attack free cryptosystem
Cylindrical diffraction method
Computer holography

ABSTRACT

A phase-retrieval attack free cryptosystem based on the cylindrical asymmetric diffraction and double-random phase encoding (DRPE) is proposed. The plaintext is abstract as a cylinder, while the observed diffraction and holographic surfaces are concentric cylinders. Therefore, the plaintext can be encrypted through a two-step asymmetric diffraction process with double pseudo random phase masks located on the object surface and the first diffraction surface. After inverse diffraction from a holographic surface to an object surface, the plaintext can be reconstructed using a decryption process. Since the diffraction propagated from the inner cylinder to the outer cylinder is different from that of the reversed direction, the proposed cryptosystem is asymmetric and hence is free of phase-retrieval attack. Numerical simulation results demonstrate the flexibility and effectiveness of the proposed cryptosystem.

1. Introduction

The network globalization and active social networking make the information security technologies increasingly important. Among them, optical information processing is one of the most promising approaches for data securing, encryption, and authentication [1–3]. The field of optical encryption was pioneered by Refregier and Javidi, who used double-random phase encoding (DRPE) in the standard 4f optical system [4,5]. DRPE has developed to one of the most widely used and studied optical encryption techniques. It has been extended to the Fresnel transform [6–8], the fractional Fourier transformation [9,10], gyrator transform [11], and phase truncation operations [12–14] by many researchers. To improve security, DRPE has been combined with other imaging techniques such as iterative computational algorithms [15–17], compressive sensing [18,19], photon-counting imaging [20–22], and so on. These methods have either reinforced the decoding resistance or simplified the implementation of the operation.

Unfortunately, the conventional DRPE encryption approach has vulnerability against specific types of attacks, such as chosen-plaintext attacks and known-plaintext attacks [23–26]. Several cryptosystems have been proposed to improve the weakness of conventional DRPE based approaches. An asymmetric cryptosystem was proposed, which is based on phase-truncated Fourier transforms [27]. Later, an improved asymmetric cryptosystem was developed by using random binary phase modulation and a mixture phase retrieval algorithm [28]. Also, coherent superposition and equal modulus decomposition were proposed for the asymmetric optical cryptosystem [29]. More recently, the distorted wavefront beam illumination was adopted to develop a novel cryptosystem based on double-random phase encoding [30]. And a novel optical image encryption method was proposed by employing divergent illumination [31]. Although they are easy to implement in digital simulation, they are difficult to implement in optical experiments. Moreover, they are generally vulnerable to the collision algorithm [32,33]. This is because these cryptosystems are derived from mathematical formulas and most of them lack a reasonable explanation from an optical viewpoint. Therefore, a cryptosystem with asymmetric diffraction based on optical principles that is practical to implement and exhibits a high resistance against specific attacks is desirable.

Inspired by the aforementioned research, we proposed a phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and DRPE in this paper. It is noticed that the majority of existing schemes of optical image encryption based on DRPE at present are propagations between two or more planers. To the best of our knowledge, it is the first time to apply the cylindrical diffraction to holographic encryption. In this proposal, the plaintext image is abstract as a cylinder, while the observed diffraction and holographic surfaces are concentric

* Corresponding author.
E-mail address: qhwang@scu.edu.cn (Q. Wang).

https://doi.org/10.1016/j.optcom.2017.10.061
Received 28 September 2017; Received in revised form 23 October 2017; Accepted 24 October 2017
0030-4018/

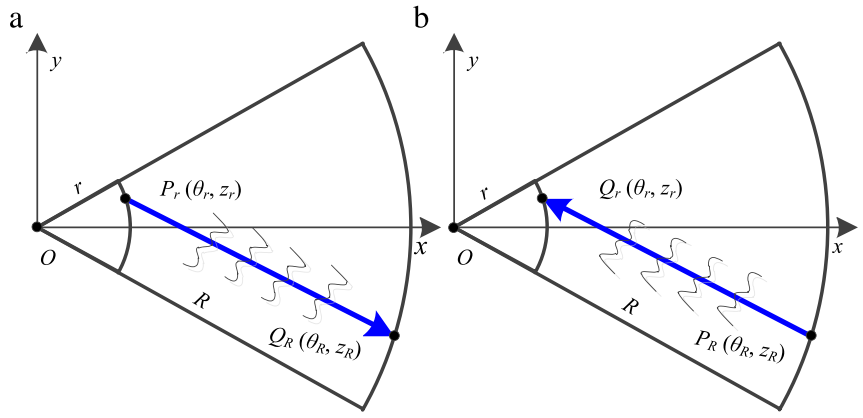

Fig. 1. Illustration of geometrical relation in cylindrical diffraction with top-view. (a) IOP Model, (b) OIP Model.

cylinders. Therefore, the plaintext can be encrypted through a two-step diffraction process with double pseudo random phase masks located on the object surface and the first diffraction surface. The distribution of complex amplitude on the second diffraction surface can be recorded and recovered by the two-step phase-shifting holography. The plaintext image can be reconstructed by inverse diffraction from a holographic surface to an object surface in a decryption process. The initial value and control parameter of double pseudo random phase masks, wavelength of the cylindrical wave, and parameters (inner and outer radii and height) of the cylinders are highly sensitive keys for authorized users. Compared with the conventional DRPE based cryptosystems, our proposed scheme has two additional keys, which enhance the security of the proposed cryptosystem. Since the diffraction calculation of propagation from inner cylinder to outer one is different from that of the reversed direction, the cylindrical diffraction is asymmetric, and hence the proposed cryptosystem is free of phase-retrieval attack. Numerical simulation results demonstrate the effectiveness and flexibility of the proposed cryptosystem.

2. Principle

In this section, the principle of our proposal is descripted. Firstly, the basic diffraction theory between a pair of concentric cylindrical surfaces is introduced. Then, the optical setup of our proposed DRPE with cylindrical asymmetric diffraction is given. Lastly, how to encrypt and decrypt an object image applying the cylindrical diffraction theory is presented.

2.1. Diffraction between two concentric cylinders

In the cylindrical diffraction theory [34,35], the object and the observation surfaces are concentric cylindrical surfaces as shown in Fig. 1, where R and r denote the radii of the inner and outer surfaces, respectively. Obviously, there are two, inside-out and outside-in, propagation models in the cases that object are placed on the inside and outside surfaces as shown in Figs. 1(a) and 1(b), respectively.

In the case of inside-out propagation (IOP) model, the object and observation points are represented by $P_r(\theta_r, z_r)$ and $Q_R(\theta_R, z_R)$ in cylindrical coordinate, respectively. While in the case of outside-in propagation (OIP) model, the object and observation points are represented by $P_R(\theta_R, z_R)$ and $Q_r(\theta_r, z_r)$ in cylindrical coordinate, respectively. Here, z_r and z_R are in range of $-H/2$ to $H/2$, where H is the height of the cylindrical surface. If the distributions on the inner and outer surfaces are represented by $u_r(\theta_r, z_r)$ and $u_R(\theta_R, z_R)$, respectively, the Rayleigh–Sommerfeld integral equation in its form can be written by

$$u_R(\theta_R, z_R) = C \iint_s u_r(\theta_r, z_r) \frac{\exp(ikd_{P_rQ_R})}{d_{P_rQ_R}} d\theta_r dz_r \quad \cdots\cdots\cdots\cdots \text{IOP}, \tag{1}$$

$$u_r(\theta_r, z_r) = C \iint_s u_R(\theta_R, z_R) \frac{\exp(ikd_{P_RQ_r})[r - R\cos(\theta_r - \theta_R)]}{d^2_{P_RQ_r}} d\theta_R dz_R \quad \cdots\cdots \text{OIP}, \tag{2}$$

$$d = d_{P_rQ_R} = d_{P_RQ_r} = [R^2 + r^2 - 2Rr\cos(\theta_R - \theta_r) + (z_R - z_r)^2]^{1/2}, \tag{3}$$

where k and C denote the wavenumber of the incident light and a constant, respectively. The d represents the distance between two points of P and Q on the object and observation surfaces, respectively. The s denotes the object surface. Note that these two equations can be accelerated by FFT algorithm [34,35].

2.2. DRPE with cylindrical asymmetric diffraction

The optical setup for the realization of the DRPE with cylindrical asymmetric diffraction is depicted as Fig. 2. The laser, special filter (SF), and lens (L1) make up a collimating system to generate the uniform plane wave. M1 and M2 are mirrors. The beam splitter (BS1) between two mirrors and the beam splitter (BS2) just before CCD divide the wave light into two beams. The random phase masks (RPM1 and RPM2) are cylindrical surfaces, which have radii of R_1, R_2 and r, respectively. The input object, which is bonded to RPM1, is also cylindrical surface with radius of R_1. The object wave, $u_{R1}(\theta_{R1}, z_{R1})$, modulates by the RPM1 and propagates to the intermediate surface, on which the distributions is $u_r(\theta_r, z_r)$. After reflection and modulation by the RPM2, the wave field continuously propagates to the destination surface, on which the distributions is $u_{R2}(\theta_{R2}, z_{R2})$. Finally, it interferes with the reference light, and the holograms are captured by the CCD. The two-step phase-shifting holography is employed here [36]. The holograms (PSH1 and PSH2) are sent to computer for processing and transmittance. Note that, the optical path lengths of the two wavefront sensing optical paths of the object and reference lights should be equal.

2.3. Encryption and decryption

The flow chart of encryption and decryption can be depicted in Fig. 3. In encryption, the object image is located at the cylindrical surface with radius of R_1 as input and is modulated by the first random phase mark (RPM1). After propagation a distance of d_1 in OIP model, the wavefront reaches the first intermediate surface and is modulated by the second random phase mark (RPM2). After propagation a distance of d_2 in IOP model, the wavefront reaches the destination surface and is captured by