Optics and Lasers in Engineering 105 (2018) 1–5

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Image security based on iterative random phase encoding in expanded fractional Fourier transform domains

Zhengjun Liu[a,*], Hang Chen[b], Walter Blondel[c,d], Zhenmin Shen[e], Shutian Liu[f]

[a] Department of Automatic Test and Control, Harbin Institute of Technology, Harbin 150001, China
[b] Laboratoire Conception Optimisation et Modélisation des Systèms, University de Lorraine, Metz 57070, France
[c] Universit de Lorraine, CRAN, UMR 7039, 54516 Vanduvre-ls-Nancy cedex, France
[d] CNRS, CRAN, UMR 7039, France
[e] Laboratory of Laser Engineering and Technology, Beijing Institute of Space Mechanics & Electricity, Beijing 100094, China
[f] Department of Physics, Harbin Institute of Technology, Harbin 150001, China

ARTICLE INFO

Keywords:
Image hiding
Compound lens
Diffraction
Off-line holography
Phase encoding
Optical transform

ABSTRACT

A novel image encryption method is proposed by using the expanded fractional Fourier transform, which is implemented with a pair of lenses. Here the centers of two lenses are separated at the cross section of axis in optical system. The encryption system is addressed with Fresnel diffraction and phase modulation for the calculation of information transmission. The iterative process with the transform unit is utilized for hiding secret image. The structure parameters of a battery of lenses can be used for additional keys. The performance of encryption method is analyzed theoretically and digitally. The results show that the security of this algorithm is enhanced markedly by the added keys.

1. Introduction

Due to the excellent performance of optical system, such as data processing with high speed and high dimension, optical information security techniques [1–3] have been developed extensively in recent years. In this field, some optical transforms have a significant role during the design of encryption algorithm. Qin et al. reported an optical color image encryption method by using the diffraction imaging [4]. As an application of information security, Lu et al. and Wang et al. proposed an interference-based optical authentication method [5,6] by using a pair of phase-only masks with different diffraction distances. Another type of data security approach based on volumetric light-field imaging at the microscopic scale was explored in [7,8]. A diffraction system with incoherent superposition was considered for optical image conversion and encryption [9]. Fatima et al. proposed an optical image encryption scheme [10] using equal modulus decomposition and multiple diffraction imaging to against some potential attacks. A single-shot imaging system [11] was applied into the field of information hiding for simplifying optical structure. Other optical systems, such as diffraction imaging structure [12], Mach–Zehnder interferometer [13], and joint transform correlator [14], were used for hiding secret image. Multiple-image encryption scheme has been studied by taking single-pixel detector [15], ptychography [16], gyrator transform [17], simultaneous interference [18] and hologram [19]. From the encryption ways mentioned above, new optical principle and framework of transform are beneficial for the development and application of optical information security.

In this paper, a battery of lenses is used for the modulation of beam propagation in an optical information system. Two lenses having different physical sizes are connected together as a unit. The lenses are placed into the optical encryption system composed of extended fractional Fourier transform (eFrFT) [20]. In mathematics, the optical process is expressed by using phase modulation and Fresnel diffraction alternately. The structure parameters of the lenses can serve as additional keys in this encryption system. The random phase encoding is also utilized in the iterative operation of data processing for making a random hidden pattern. The performance of this encryption method is validated by numerical simulation.

The rest of this paper is organized in the following sequence. In Section 2, the proposed encryption algorithm is presented and the eFrFT implemented with the two lenses is explained. In Section 3, some numerical simulation results of encryption, security and robustness, are given to demonstrate the validity of this optical information security approach. Concluding remarks are summarized in the final section.

* Corresponding author.
E-mail address: zjliu@hit.edu.cn (Z. Liu).

https://doi.org/10.1016/j.optlaseng.2017.12.007
Received 23 October 2017; Received in revised form 12 December 2017; Accepted 17 December 2017
0143-8166/

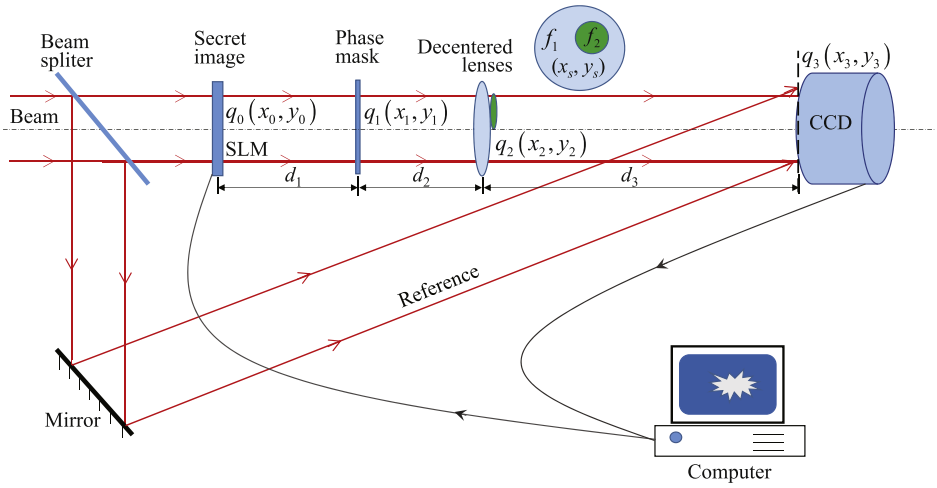

Fig. 1. The optical encryption system composed of iterative eFrFT with a pair of convex lenses.

2. Optical encryption scheme

As shown in Fig. 1, the secret image, $q_0(x_0, y_0)$, encoded by spatial light modulator (SLM) is illuminated by uniform beam and is propagated with the distance d_1 into the random phase mask. Here the light field at the left side of the mask can be expressed as

$$q_1(x_1, y_1) = \exp[\mathrm{i} \cdot p(x_1, y_1)] F_{d_1,\lambda}[q_0(x_0, y_0)], \tag{1}$$

where F denotes Fresnel diffraction operation. The symbol λ is wavelength. The function $p(x_1, y_1)$ represents the phase distribution of the mask, which is a uniform random function. The random field modulated by the mask is converted by eFrFT which composed by two lenses and then finally received by CCD. Here the field $q_2(x_2, y_2)$ is determined as

$$q_2(x_2, y_2) = \exp[\mathrm{i} \cdot s(x_2, y_2)] F_{d_2,\lambda}[q_1(x_1, y_1)], \tag{2}$$

where $s(x_2, y_2)$ is the phase distribution of the unit constituted by two lenses. The function $s(x_2, y_2)$ is defined as follows

$$s(x_2, y_2) = \exp\left[-\mathrm{i}k\frac{x_2^2 + y_2^2}{2f_1} - \mathrm{i}k\frac{(x_2 - x_s)^2 + (y_2 - y_s)^2}{2f_2}\right], \tag{3}$$

where $k = 2\pi/\lambda$ is wavenumber. Here f_1 and f_2 are the focal length of big lens and small lens, respectively. The variables (x_s, y_s) are the shift of the centers of two lenses. The unit composed of two lenses can also be replaced with a SLM achieving phase-only modulation in practical experiment. The field q_3 at the CCD plane is calculated as

$$q_3(x_3, y_3) = F_{d_3,\lambda}[q_2(x_2, y_2)], \tag{4}$$

where the data of complex image q_3 is recorded by using off-line holography technique [21]. Here the data distribution of q_3 is scrambled by Arnold mapping before being sent into SLM from the computer for the next loop of random phase encoding.

The operations mentioned above will be performed iteratively. For simplicity, the structure parameters (x_s, y_s) of two lenses are fixed at the same value in the repeated operations. During the data transmission, the distance parameters d_1, d_2 and d_3, are also unchanged in this optical encryption system. The five parameters related with position and two values of focal length can serve as additional keys to enhance the security of this algorithm. The reverse optical path of the system depicted in Fig. 1 will be employed for the decryption of secret pattern. The conjugate phase mask and two concave lenses having the values of focal length, $-f_1$ and $-f_2$, respectively, are used for inverse process when recovering original information. Moreover the positions of the mask and two lenses should be switched to make an inverse process in the optical decryption system.

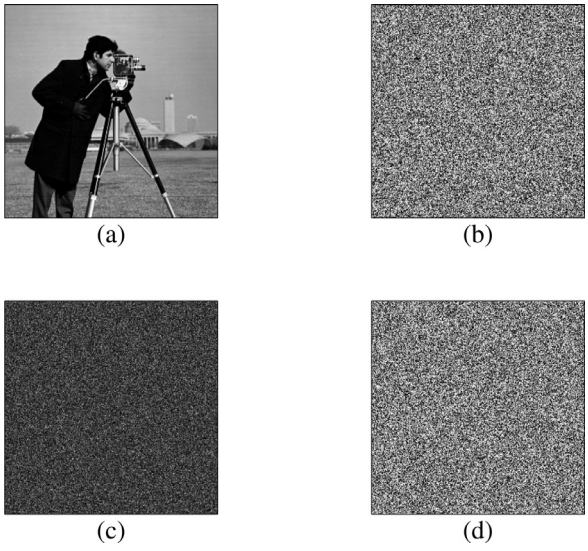

Fig. 2. The tested result of image encryption: (a) original image, (b) random phase, (c) amplitude pattern, (d) phase pattern.

3. Numerical simulation

3.1. Performance of the proposed method

Numerical simulation is considered for validating the performance of this optical encryption method. The parameters are taken as follows: (a) $\lambda = 632.8$ nm, $f_1 = 10$ cm, $f_2 = 3$ cm, $x_s = 2.3$ mm, $y_s = 2$ mm, $d_1 = 6$ cm, $d_2 = 5$ cm, $d_3 = 9$ cm, (b) the radius of small lens is $R_2 = 1.8$ mm, (c) the physical size of original image is 1 cm × 1 cm. The encryption operation is performed 4 times iteratively. A gray-level image having 256 × 256 pixels is regarded as secret image and is shown in Fig. 2 (a). The phase distribution of the phase mask is given in Fig. 2 (b). The amplitude pattern and the phase pattern of encrypted result are illustrated in Fig. 2(c) and (d), respectively. These output pictures clearly show that the image hiding scheme is effective in hiding the secret pattern. The original image can be recovered completely, when all correct values of keys are used in the decryption computation. The corresponding image is displayed in Fig. 3. The calculated images have validated that the encryption method is performed successfully.