Available online at www.sciencedirect.com
SCIENCE DIRECT®
Optics Communications 260 (2006) 449–453
OPTICS COMMUNICATIONS
www.elsevier.com/locate/optcom

Image encryption based on extended fractional Fourier transform and digital holography technique

Xiaogang Wang, Daomu Zhao *, Linfei Chen

Department of Physics, Zhejiang University, Hangzhou 310027, China

Received 10 September 2005; received in revised form 31 October 2005; accepted 2 November 2005

Abstract

We present a new optical image encryption algorithm that is based on extended fractional Fourier transform (FRT) and digital holography technique. We can perform the encryption and decryption with more parameters compared with earlier similar methods in FRT domain. In the extended FRT encryption system, the input data to be encrypted is extended fractional Fourier transformed two times and random phase mask is placed at the output plane of the first extended FRT. By use of an interference with a wave from another random phase mask, the encrypted data is stored as a digital hologram. The data retrieval is operated by all-digital means. Computer simulations are presented to verify its validity and efficiency.

PACS: 42.30.−d; 42.30.Kq; 42.30.Va

Keywords: Image encryption; Decryption; Fractional Fourier transform; Digital holography

1. Introduction

Nowadays information security is becoming more and more important. Many methods based on optical techniques play an important role in information security applications. Optical encryption provides a high security against counterfeiting and unauthorized access. A number of optical image encryption systems have been proposed in recent years.

The earlier optical image encryption systems [1–4] are based on general Fourier transforms. And by use of fractional Fourier transform (FRT), a generalization of Fourier transform, optical image encryption techniques have been developing steadily [5–9]. Hua et al. [10] introduced the extended FRT with more parameters compared with the conventional FRT. Several optical image encryption systems based on extended FRT have also been proposed [11–13]. In recent years, digital holography has been noticed and can be used on the information security [9,14–16]. Data encryption algorithms combined FRTs and digital holography techniques not only provide many degrees of freedom, but also enable us to store, transmit and decode the encoded data digitally.

In this paper, we propose a fully digital encryption system based on extended FRT and digital holography technique. The parameters of the extended FRT give an enhancement on security compared with the conventional FRT. The input image is extended fractional Fourier transformed two times and encrypted by use of a random phase mask in the extended FRT encryption system. By use of an interference with a wave from another phase mask, the data is encrypted again and recorded as a digital hologram. The decryption key can also be recorded as the key hologram as described in the following section. The parameters, the random phase code and the key hologram form the keys to the encrypted image. The retrieval is carried out by all-digital means. Theoretical explanation and numerical simulations show the algorithm proposed is feasible.

* Corresponding author. Tel./fax: +86 57 188863887.
E-mail address: zhaodaomu@yahoo.com (D. Zhao).

0030-4018/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2005.11.006

2. Image encryption and decryption

The proposed encryption and decryption system based on extended FRT and digital holography technique is shown in Fig. 1. By use of an interference with a wave from a random mask, the data passed through the extended FRT encryption system is recorded and simultaneously encrypted. Although the images are two-dimensional, we follow a one-dimensional representation for convenience. Let $f(x_1)$ denote the original amplitude image to be encrypted. As shown in Fig. 2, the original image multiplied by a random mask $p_1(x_1)$, represented by function $\exp[i\phi_1(x_1)]$, where $\phi_1(x_1)$ is a random function distributed uniformly in the interval $[0,2\pi]$, is extended fractional Fourier transformed firstly

$$g(x_2) = K \int f(x_1) \exp[i\phi_1(x_1)] \times \exp\left[i\pi \frac{(a_1^2 x_1^2 + b_1^2 x_2^2)}{\tan\varphi_1} - i2\pi \frac{a_1 b_1}{\sin\varphi_1} x_1 x_2\right] dx_1, \quad (1)$$

where x_1 and x_2 are the coordinates of the input plane and output plane of the first extended FRT, respectively. a_1, b_1 and φ_1 are the three parameters of the extended FRT and K is a complex constant. For the sake of simplicity, we use two lenses with the same focal length f in the system. The parameters a_1, b_1 and φ_1 are related to the distances l_1, l_1', the wavelength λ, the focal length f and given by:

$$a_1^2 = \frac{1}{\lambda} \frac{\sqrt{f - l_1'}}{\sqrt{f - l_1}} \frac{1}{[f^2 - (f - l_1)(f - l_1')]^{1/2}}, \quad (2)$$

$$\varphi_1 = \arccos\left(\frac{\sqrt{f - l_1}\sqrt{f - l_1'}}{f}\right), \quad (3)$$

$$b_1^2 = \frac{1}{\lambda} \frac{\sqrt{f - l_1}}{\sqrt{f - l_1'}} \frac{1}{[f^2 - (f - l_1)(f - l_1')]^{1/2}}. \quad (4)$$

Then it goes into the second extended FRT operation, the distribution $g(x_2)$ is encoded by random phase mask $p_2(x_2)$, mathematically expressed as phase function $\exp[i\phi_2(x_2)]$, where $\phi_2(x_2)$ is a random function distributed uniformly in the interval $[0,2\pi]$ and statistically independent of $\phi_1(x_1)$. The distribution at the output plane is given by

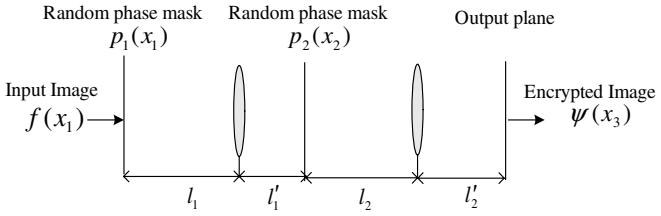

Fig. 2. The extended FRT encryption system.

$$\psi(x_3) = K \int g(x_2) \exp[i\phi_2(x_2)] \times \exp\left[i\pi \frac{(a_2^2 x_2^2 + b_2^2 x_3^2)}{\tan\varphi_2} - i2\pi \frac{a_2 b_2}{\sin\varphi_2} x_2 x_3\right] dx_2, \quad (5)$$

where the values of the parameters a_2, b_2, φ_2 are related to the physical parameters l_2, l_2', f. One can obtain the values of these parameters by substituting l_2, l_2' for l_1, l_1', respectively, into Eqs. (2)–(4).

With a wave from another random phase mask $q(u)$ represented by phase function $\exp[i\phi(u)]$, where $\phi(u)$ is a random white sequence uniformly distributed in the interval $[0,2\pi]$ and statistically independent of $\phi_1(x_1)$ and $\phi_2(x_2)$, one can record the interference signal as the digital hologram of the encrypted data by use of a CCD camera as shown in Fig. 1. The intensity $P(u)$ of the digital hologram created by the interference between these two waves is given by

$$P(u) = |\psi(x_3) + q(u)|^2 = |\psi(x_3)|^2 + |q(u)|^2 + \psi^*(x_3)q(u) + \psi(x_3)q^*(u), \quad (6)$$

where the first and second terms on the right-hand side of Eq. (6) can be known a priori by obtaining the power spectrum of the encrypted data and reference beam [9,14–16]. By removing both the original object, the transforming lens and illuminating with a plane wave of uniform unitary amplitude [9,16], the key hologram $k(u)$ is given by

$$k(u) = |1 + q(u)|^2 = |1|^2 + |q(u)|^2 + q^*(u) + q(u). \quad (7)$$

One can see that the exact key hologram $k(u)$ cannot be obtained without knowledge of $q(u)$. When extracting the holographic data from Eqs. (6) and (7), retaining the fourth

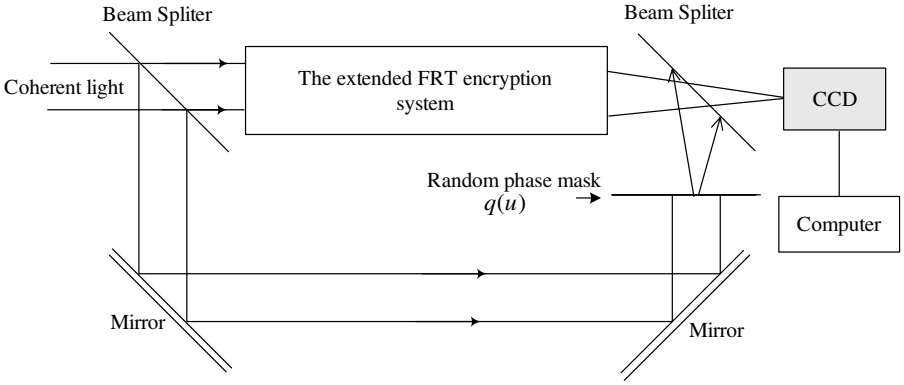

Fig. 1. The schematic of the optical image encryption–decryption system.