Optics Communications 286 (2013) 123–129

Contents lists available at SciVerse ScienceDirect

Optics Communications

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

Security-enhanced interference-based optical image encryption

Wen Chen*, Xudong Chen

Department of Electrical and Computer Engineering, National University of Singapore, 4 Engineering Drive 3, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 23 December 2011
Received in revised form
31 August 2012
Accepted 4 September 2012
Available online 18 September 2012

Keywords:
Optical image encryption
Optical interference
Security enhancement
Fractional fourier transform

ABSTRACT

Interference-based optical image encryption has triggered much current attention due to its marked advantages, such as non-iterative operation. Although interference-based optical image encryption is an effective approach, cryptosystem security is still a great concern from a cryptanalysis point of view and higher security is always desirable. In this paper, we propose a novel method to enhance the security for conventional interference-based optical image encryption in the fractional Fourier transform (FrFT) domain. A series of random and fixed phase-only masks is used in the optical paths, and subsequently interference principle is applied to extract two phase-only masks (i.e., ciphertexts) during image encryption. Feasibility and effectiveness of the proposed method are demonstrated by computer simulations.

1. Introduction

With the rapid development of computer and internet technologies, unauthorized information usage and distribution become a serious problem, which results in a stringent demand of various encryption techniques. In recent years, optical encryption technique [1] is considered as an important research topic for information security. Optical image encryption has attracted more and more attention due to its marked advantages, such as parallel processing and multiple-parameter characteristic. Since double random phase encoding [1] was proposed, various algorithms and infrastructures [2–9], such as virtual optics [2,3], digital holography [4], polarization [5], Fresnel transform [6], gyrator transform [7] and fractional Fourier transform (FrFT) [8,9], have been further developed in order to enhance cryptosystem security. However, it was found that some cryptosystems could not effectively endure the attacks [10–13], such as known-plaintext attack [11]. Optical asymmetric cryptosystems, such as phase-truncated Fourier transform [14], have been proposed to resolve the problem inherent in conventional symmetric cryptosystems. In addition, it is also found that when diffractive imaging [15–17] is applied in optical image encryption, the attack algorithms cannot work.

In recent years, the phase retrieval algorithm [18–20] is considered as one of the most important technologies for optical image encryption. Wang et al. [18] and Li et al. [19] first proposed phase retrieval algorithm which can iteratively encrypt the plaintext into two phase-only masks (i.e., one mask fixed and another mask extracted). Subsequently, Chang et al. [20] developed phase retrieval algorithm which can embed the plaintext into multiple phase-only masks. The phase-only masks generated are stored or transmitted to the authorized receivers, and either a digital or optical approach can be applied during image decryption. However, an iterative operation is usually required for extracting the phase-only masks during image encryption. Recently, Zhang and Wang [21] proposed a phase retrieval algorithm based on interference principle for optical image encryption. It was illustrated [21] that iterative operations can be avoided during image encryption, and interference strategy could be easily implemented during image decryption. However, there is a silhouette problem in the conventional interference-based optical encryption [22,23]. Some algorithms [22,23], such as exchanging strategy [22] and jigsaw transform [23], have been proposed to remove the silhouette. In addition to the silhouette problem, higher security is always desirable for interference-based optical image encryption [21].

In this paper, we propose a novel method to enhance the security for conventional interference-based optical image encryption. A series of fixed phase-only masks (i.e., principal security keys) is used in the optical paths, and interference principle is applied to extract two phase-only masks (i.e., ciphertexts) during image encryption. Since a series of random and fixed phase-only masks is applied as principal security keys, more key space is generated and higher security can be achieved in the proposed optical cryptosystem compared with conventional interference-based optical encryption method [21].

2. Theoretical analysis

The optical encryption scheme based on interference [21–27] is briefly summarized. Fig. 1 shows a schematic setup for interference-based optical image encryption in the FrFT domain.

* Corresponding author. Tel.: +65 65166855; fax: +65 67791103.
E-mail address: elechenw@nus.edu.sg (W. Chen).

0030-4018/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2012.09.014

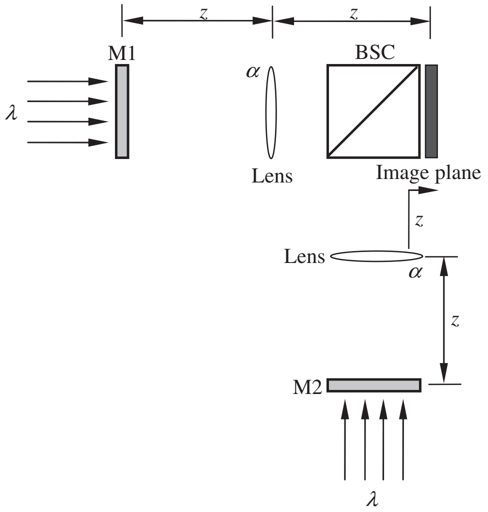

Fig. 1. A schematic experimental setup for conventional interference-based optical image encryption [21] in the FrFT domain: M_1 and M_2, extracted phase-only masks (i.e., ciphertexts); BSC beam splitter cube; z axial distance; α FrFT function order and λ the wavelength of plane waves.

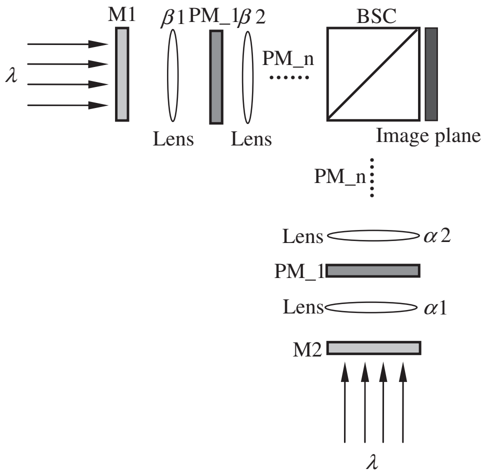

Fig. 2. A schematic experimental setup for security-enhanced interference-based optical image encryption in the FrFT domain: M_1 and M_2, the extracted phase-only masks based on the proposed method; *PM_n* a series of fixed phase-only masks placed in the optical paths; $\alpha1$, $\alpha2$, $\beta1$ and $\beta2$, FrFT function orders. Circular dots are used to illustrate that a series of random and fixed phase-only masks can be applied in the optical paths.

To obtain the input image (i.e., plaintext) in the image plane, a digital approach is used to encrypt the plaintext into two phase-only masks, i.e., M_1 and M_2. In this study, FrFT function orders are the same at the corresponding propagation intervals in the two optical paths. When a plane wave is generated to simultaneously illuminate phase-only masks M_1 and M_2, interference in the image plane can be described by [21–27]

$$\sqrt{O(x,y)}\exp[jH(x,y)] = FrFT_{\alpha,\alpha}\{\exp[jM_1(\xi,\eta)]\} + FrFT_{\alpha,\alpha}\{\exp[jM_2(\xi,\eta)]\}, \tag{1}$$

where $O(x,y)$ denotes a plaintext, $j=\sqrt{-1}$, and $H(x,y)$ is a map randomly distributed in the range of $[0,2\pi]$. Note that the plaintext is first normalized before image encryption. For simplicity, an one-dimensional FrFT is analyzed, and FrFT with an order α can be described by [8,9,28,29]

$$FrFT_{\alpha}\{\exp[jM_1(\xi)]\} = \int_{-\infty}^{+\infty}\{\exp[jM_1(\xi)]\}T_{\alpha}(x,\xi)d\xi, \tag{2}$$

where

$$T_{\alpha}(x,\xi) = \begin{cases} R\exp\left\{j\pi\left[x^2\cot(\alpha\pi/2)+\xi^2\cot(\alpha\pi/2)-2x\xi\csc(\alpha\pi/2)\right]\right\} & \text{if } \alpha \neq 2m \\ \delta(x-\xi) & \text{if } \alpha = 4m \\ \delta(x+\xi) & \text{if } \alpha = 4m \pm 2 \end{cases},$$

m is an integer, and $R=\sqrt{1-j\cot(\alpha\pi/2)}$,

Hence, the plaintext can be encrypted into two phase-only masks M_1 and M_2 (i.e., ciphertexts) as [21–27]

$$M_1(\xi,\eta) = ang(D) - \arccos\{[abs(D)]/2\}, \tag{3}$$

$$M_2(\xi,\eta) = ang\{D - \exp[jM_1(\xi,\eta)]\}, \tag{4}$$

where $D = FrFT_{-\alpha,-\alpha}\left\{\sqrt{O(x,y)}\exp[jH(x,y)]\right\}$, $-\alpha$ denotes function order in the inverse FrFT, and ang and abs denote arc-tangent and modulus operations, respectively. In Eq. (3), values of $\left[abs(D)\right]/2$ are thresholded, and values larger than one are set as 1. When spatial light modulators are used in real experiments, constant values, such as 2π, can be simultaneously added to the extracted phase-only masks M_1 and M_2. Although the plaintext can be encrypted into two phase-only masks, key space is small in the conventional encryption method and cryptosystem security is limited to some extent [21].

In this study, a series of random and fixed phase-only masks (i.e., principal security keys) is used in the optical paths to enhance cryptosystem security as shown in Fig. 2. It is worth noting that the corresponding FrFT function orders in two optical paths are the same. For instance, FrFT function order $\alpha1$ in one optical path is the same as $\beta1$ in another optical path (see Fig. 2). Similarly, the same phase-only masks (i.e., *PM_n*) are placed in the two optical paths. The fixed phase-only masks *PM_n* are 2D maps randomly distributed in the range of $[0,2\pi]$. When a plane wave is generated to simultaneously illuminate phase-only masks M_1 and M_2, optical interference in the image plane can be described by

$$\sqrt{O(x,y)}\exp[jH(x,y)] = FrFT_{\alpha2,\alpha2}[(FrFT_{\alpha1,\alpha1}\{\exp[jM_1(\xi,\eta)]\})PM_1(\mu,v)] + FrFT_{\beta2,\beta2}[(FrFT_{\beta1,\beta1}\{\exp[jM_2(\xi,\eta)]\})PM_1(\mu,v)], \tag{5}$$

where $\alpha1$, $\alpha2$, $\beta1$ and $\beta2$ are FrFT function orders, and $PM_1(\mu,v)$ denotes the phase-only mask *PM_1*. In the interference-based optical encryption, function order $\alpha1$ is numerically equal to $\beta1$, and function order $\alpha2$ is equal to $\beta2$. The different symbols are used to illustrate that the function orders are generated in the different optical paths.

Hence, the plaintext can be encrypted into two phase-only masks $M_1$and M_2 (i.e., ciphertexts) as

$$M_1(\xi,\eta) = ang(W) - \arccos\{[abs(W)]/2\}, \tag{6}$$

$$M_2(\xi,\eta) = ang\{W - \exp[jM_1(\xi,\eta)]\}, \tag{7}$$

where $W = FrFT_{-\alpha1,-\alpha1}[(FrFT_{-\alpha2,-\alpha2}\left\{\sqrt{O(x,y)}\exp[jH(x,y)]\right\})/PM_1(\mu,v)]$, and the FrFT function orders in the symbol W can be replaced by $(-\beta1,-\beta1)$ and $(-\beta2,-\beta2)$, respectively. In Eq. (6), values of $\left[abs(W)\right]/2$ are thresholded, and values larger than one are set as 1. When a series of random phase-only masks *PM_n* is used, the symbol W can be described by

$$W = FrFT_{-\alpha1,-\alpha1}\{\cdots\cdots\{FrFT_{-\alpha(n),-\alpha(n)}\left[(FrFT_{-\alpha(n+1),-\alpha(n+1)}\left\{\sqrt{O(x,y)}\exp[jH(x,y)]\right\})/PM_n(\mu_n,v_n)\right]\}/PM_{n-1}(\mu_{n-1},v_{n-1})\cdots\cdots\}, \tag{8}$$

where n is an integer 1,2,3,…, and the circular dots are used to denote the operations based on a series of fixed phase-only masks *PM_n* in the FrFT domain.

Encryption process should be digitally implemented, and either an optical or digital approach can be applied for image