Optics & Laser Technology 57 (2014) 327–342

Contents lists available at ScienceDirect

Optics & Laser Technology

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

A review of optical image encryption techniques

Shi Liu [a,b,c], Changliang Guo [a,b,c], John T. Sheridan [a,b,c,*]

[a] School of Electrical, Electronic and Communication Engineering, College of Engineering and Architecture, University College Dublin, Belfield, Dublin 4, Ireland
[b] Communications and Optoelectronic Research Centre, University College Dublin, Belfield, Dublin 4, Ireland
[c] The SFI-Strategic Research Cluster in Solar Energy Conversion, University College Dublin, Belfield, Dublin 4, Ireland

ARTICLE INFO

Available online 9 July 2013

Keywords:
Optical image processing
Optical encryption
Information security

ABSTRACT

In this paper we review a number of optical image encryption techniques proposed in the literature inspired by the architecture of the classic optical Double Random Phase Encoding (DRPE) system. The optical DRPE method and its numerical simulation algorithm are first investigated in relation to the sampling considerations at various stages of the system according to the spreading of the input signal in both the space and spatial frequency domains. Then the several well-known optically inspired encryption techniques are examined and categorized into all optical techniques and image scrambling techniques. Each method is numerically implemented and compared with the optical DRPE scheme, in which random phase diffusers (masks) are applied after different transformations. The optical system used for each method is first illustrated and the corresponding unitary numerical algorithm implementation is then investigated in order to retain the properties of the optical counterpart. The simulation results for the sensitivities of the various encryption keys are presented and the robustness of each method is examined. This overview allows the numerical simulations of the corresponding optical encryption systems, and the extra degree of freedom (keys) provided by different techniques that enhance the optical encryption security, to be generally appreciated and briefly compared and contrasted.

1. Introduction

With the rapid development of modern communication techniques, both information security and intellectual property protection are of great concern. This has led to extensive study of data encryption, digital signature, authentication, and watermarking methods [1]. Optical encryption techniques have attracted significant interest as they offer the possibility of high-speed parallel processing of 2D image data, of hiding information in many different dimensions, i.e. of multiple degrees of freedom [2]. One important optical encryption scheme, dubbed "Double Random Phase Encoding (DRPE)", involves multiplication of the image by random phase diffusers (masks) both in the input (space) and Fourier (spatial frequency) domains [3]. The encrypted image can be shown to be a stationary white noise if the two random phases are statistically independent white noises. Digital holography [4,5] provides a convenient form of recording the complex encrypted images after passing through the optical DRPE systems. The second random phase diffuser located at the Fourier domain serves as the key in this encryption system. Following the introduction of this technique, several other optically inspired encryption methods have been proposed in the literature including digital optical stream cipher [6], optical XOR image encryption [7], phase-shifting interferometry [8], polarization encoding [9,10], and information security verification techniques involving the joint transform correlators [11–13]. The theoretical and experimental results reported indicate that the security level of the optical encryption systems can be improved significantly using such methods.

The DRPE method opened new fields of research in optical image and signal processing and has been the focus of many studies. Many variations of this approach have been developed involving extra degrees of freedom. The fractional Fourier transform (FRT) [14–24] and the Fresnel transform (FST) [25–28] have been utilized in encryption algorithms and systems, in which the fractional order and the propagation distance are introduced and served as additional keys. It has been argued that these extra keys could improve the security of the optical encryption system since they provide additional difficulties for the attackers of the system. Since the Fourier transform (FT), the fractional Fourier transform (FRT), and the Fresnel transform (FST) are all special cases of the linear canonical transform (LCT), the use of the LCT has also been proposed for the optical encryption techniques using a quadratic

* Corresponding author at: School of Electrical, Electronic and Communication Engineering, College of Engineering and Architecture, University College Dublin, Belfield, Dublin 4, Ireland. Tel.: +353 17161927.
E-mail address: John.Sheridan@ucd.ie (J.T. Sheridan).

0030-3992/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.05.023

phase system (QPS) [29]. In this case the QPS transformation parameters provide extra keys for the encryption system. The Gyrator transform (GT), which also belongs to the class of the linear canonical transforms, has been used for optical encryption systems [30–40], where the rotation angle parameter provides the extra key of the encryption system. The Hartley transform (HT), which is effectively a real Fourier transform without any phase information, has also been proposed for the use in optical DRPE systems [41–45]. In addition, the DRPE has been investigated for use in multiple-image encryption [46–48] and color image encryption [49–56]. The image scrambling techniques, which can be viewed as computer based numerical preprocessing procedure, have also been applied in conjunction with theDRPE system using the Jigsaw transform (JT) [57–59] and the Arnold transform (ART) [60–64]. Recently, the computational ghost imaging technique has been proposed for encrypting and transmitting information, where the encrypted image appears to be an intensity vector instead of a complex-valued matrix in the typical DRPE system [65,66]. Another alternative optical imaging method, i.e. the diffractive imaging, has also been developed in the optical encryption field. It involves using an iterative phase retrieval algorithm for decrypting the original image from the recorded diffraction patterns [67–70]. Furthermore, two dimensional optical encryption processing has been extended into a three dimensional space-based encryption processing, where each pixel of the image is axially considered as one particle and phase-shifting digital holography technique is applied to the diffraction of all pixels in space (particles) [71–74]. In the context of cryptography and cryptoanalysis, both chosen-plaintext [60] and known-plaintext attack [75–77] on DRPE have been examined, as have several other attacking methods [78–82] and the key space of DRPE technique itself [83–86] has also been analysed.

In this paper we review a number of optical image encryption methods proposed in the literature based on the architecture of the classic optical Double Random Phase Encoding (DRPE) system. The optical DRPE method is first recalled and its ability to randomly spread the energy of the input signal in both the space and spatial frequency domains is discussed in Section 2. After considering this ability, a recent proposed numerical simulation method of the DRPE based on the physical sampling considerations is then reviewed in Section 3. This method is based on a discrete model of the DRPE system that retains the properties of its optical counterpart. With this in mind, each optical encryption method studied in this paper is investigated both optically and numerically in terms of the DRPE architecture. We assign these optically encryption approaches to two categories: (I) all optical techniques and (II) image scrambling techniques, which are discussed in Sections 4 and 5, respectively. The all optical methods are generalized using various linear canonical transforms, which are applied to change the FT, (in the original DRPE scheme), into the FRT, the FST, the LCT, the GT, and the HT. The image scrambling techniques, including the Jigsaw transform (JT) and the Arnold transform (ART), are employed in order to randomly scramble the input (or intermediate) plane images. For the purpose of comparison, identical random phase diffusers (masks) are used for all cases examined. The robustness of each method is demonstrated by exploring the sensitivities of decryption to errors in the encryption keys. In general, the review process is discussed and organized systematically for each optical encryption method in the following way: (i) the optical implementation is illustrated, (ii) the numerical algorithms of the corresponding optical system are explored, (iii) the method is implemented numerically based on DRPE scheme, and (iv) the robustness performance is investigated based on the sensitivities of the extra key always using the same random diffusers and same input image. In all cases an attempt is made to quantify the robustness. The final section contains a brief conclusion.

2. Optical double random phase encoding (DRPE)

In this section we review the classical optical DRPE system as proposed in Ref. [3]. In the context of categorizing and investigating different types of optical encryption techniques in this paper, it is critically important to discuss the encryption and decryption processes of the optical DRPE architecture. In what follows we refer to the optical Fourier transform (OFT), the Fourier transform (FT) and the discrete Fourier transform (DFT) in Ref. [87].

2.1. DRPE encryption

The standard optical DRPE system is illustrated in Fig. 1(a). An input image wave field first passes through a random diffuser $D1(x,y)$, then a 2D OFT, and the second diffuser $D2(x,y)$, and finally a second 2D OFT. The two diffusers described by their transmission functions, $D1(x,y)$ and $D2(x,y)$, are statistically independent random phase functions positioned in the space and spatial frequency domains, respectively. $D1(x,y)$ is described as $\exp\{j2\pi\theta_1(x,y)\}$ and $D2(x,y)$ is given by $\exp\{j2\pi\theta_2(x,y)\}$, where the functions $\theta_1(x,y)$ and $\theta_2(x,y)$ denote two independent sequences uniformly distributed in $[0,1]$. The encrypted image field, $E(x,y)$, can be represented as follows:

$$E(x,y) = DRPE\{I(x,y), D1(x,y), D2(x,y)\} = \mathcal{OFT}\{\mathcal{OFT}\{I(x,y)\times D1(x,y)\}\times D2(x,y)\}, \quad (1)$$

where $DRPE\{-\}$ denotes the complete encryption process, $\times$ denotes multiplication and $\mathcal{OFT}\{-\}$ is the 2D optical Fourier transform [88]. The encrypted image, $E(x,y)$, can be shown to be a stationary white noise due to the statistical properties of the two diffusers [3]. $D1(x,y)$ is in the space domain and makes the input image $I(x,y)$ white, while $D2(x,y)$ is in the Fourier or spatial frequency domain and makes it stationary and encoded. We note that the optical DRPE uses the Fourier transforming property of a thin lens, and it is linear due to the linearity theorem of the FT [88]. Since the encrypted image $E(x,y)$ is complex valued, it is necessary to capture both the amplitude and phase information of $E(x,y)$ in the optical implementation described in Fig. 1(a). Digital holographic techniques must be used to extract the full complex wave field information [4,5].

We assume finite bandwidths for both $D1(x,y)$ and $D2(x,y)$ as defined in Table 1 [We note in the case of $D2(x,y)$, the width and

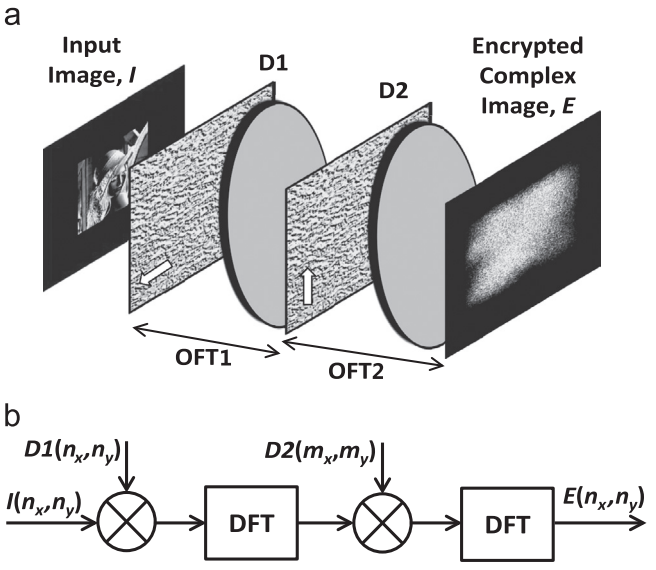

Fig. 1. The illustration of the DRPE: (a) the standard optical DRPE system; (b) the discrete counterpart of the optical DRPE system.