Optics Communications 321 (2014) 61–72

Contents lists available at ScienceDirect

Optics Communications

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

# Optical double image encryption employing a pseudo image technique in the Fourier domain

Changliang Guo, Shi Liu, John T. Sheridan *

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

ARTICLE INFO

*Article history:*
Received 31 October 2013
Received in revised form
19 January 2014
Accepted 21 January 2014
Available online 5 February 2014

*Keywords:*
Optical image processing
Optical encryption
Double Random Phase Encoding
Information security
Pseudo image

ABSTRACT

A novel optical encryption method is proposed involving double image encryption in which one image is introduced as the pseudo image while the other is the original object image. The Double Random Phase Encoding technique is used to encrypt both the pseudo and object images into complex images. A unique binary image is then employed to first generate the random phase key for the object image encryption and then to embed the encrypted object image into the encrypted pseudo image, which acts as host image. Both the second random phase mask used for encoding the pseudo image and the binary image act as encryption keys. If an attacker attempts to crack the random phase key and decrypt the original object image, the pseudo image will be obtained instead. Simulation results and robustness tests are performed which demonstrate the feasibility of the algorithm.



## 1. Introduction

In recent years, information security has received increasing attention. Optical systems offer the potential advantage of being able to process 2-D complex data in parallel and at great speeds. In 1995, Refregier and Javidi proposed The Double Random Phase Encoding (DRPE) method, involving two random phases screen keys in the input and Fourier domains [1]. It can be shown that if the two random phases are statistically independent then the encrypted image output is a stationary white noise. Several variations on the original DRPE technique [2] using the fractional Fourier transform (FRT) [3,4,5], gyrator transform (GT) [6], Fresnel transform (FST) [7], linear canonical transform (LCT) [8], or using polarized light [9], or pixel scrambling techniques [10] have been proposed and studied. Double image encryption (DIE) can be used to encrypt more information simultaneously in a single image [11], and can be implemented using the DRPE. In this case the information of the two images is combined into one complex valued image as part of the encryption process.

In this paper we proposed a new double image encryption method to encrypt two images, with one image acting as a pseudo image and the other acting as the object image. A pseudo image is an image used to deceive the attacker by covering the object image to be transmitted. Both the pseudo and object images are encrypted using the DRPE technique. Then, the encrypted object image is embedded in the encrypted pseudo image (using specific binary position information) to obtain the final encrypted image. Both the second random phase used for the pseudo image encryption and the position information serve as keys in our proposed encryption system. If the attacker attempts to decrypt the final encrypted image using the inverse DRPE system, the pseudo image is decrypted and can be mistakenly taken as the object image transmitted.

This information hiding technique reinforces data security by hiding the encrypted object information (plain-text) within the encrypted pseudo message. Thus, not only is the image encrypted but also the encrypted image is hidden in an uncorrelated encrypted image which is used as a 'cover'. This provides extra security during information exchange [12,13,14].

The paper is organized as follows. In Section 2 we present the general scheme of our proposed optical encryption algorithm. Section 3 describes the algorithm proposed, including descriptions of: (i) the DRPE method; (ii) the encryption of the pseudo image; (iii) the encryption of the object image, and (iv) the method of embedding the encrypted object image into the encrypted pseudo image. In Section 4 we analyze the robustness of the decryption process by simulating a blind attack in comparison to correct decryption. Section 5 describes a proposed optical implementation of the algorithm. In Section 6, simulation results, testing the robustness of the method to blind decryption and noise are presented. The last section gives a brief conclusion.

* Corresponding author. Tel.: +353 1 716 1927; fax: +353 1 283 0921.
*E-mail address:* john.sheridan@ucd.ie (J.T. Sheridan).

0030-4018/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2014.01.061

## 2. Principle of our algorithm: encryption

### 2.1. Encryption scheme

In this section we outline the general scheme of our encryption/decryption system. Figs. 1 and 2 illustrate the proposed pseudo technique which is then discussed in detail.

#### 2.1.1. Encryption of the pseudo image

The size of the pseudo image is larger than that of the object image, as indicated in Fig. 1. In our simulation, the size of the pseudo image is chosen to be $2N \times 2N$, while the size of object image is $N \times N$. Therefore the size of the object image is one quarter the size of the pseudo image. This facilitates the embedding process during the last stage of the encryption procedure. The classical DRPE system is then applied to encrypt the pseudo image using two random phase masks, denoted by $D1(x,y)$ and $D2(x,y)$. Since only the intensity of the pseudo image is of interest, the DRPE method used is an Amplitude Encoding (AE) system [1]. In Amplitude Encoding (AE), the second mask $D2(x,y)$ serves as the only key in the encryption system.

#### 2.1.2. Encryption of the object image

To encrypt the object image, the DRPE method is again utilized with two different random phase masks, denoted by $D3(x,y)$ and $D4(x,y)$. In our approach, in order to reduce the quantity of data to be transmitted and ensure higher security, the second random phase mask $D4(x,y)$ is generated using a subset, i.e., one quarter, of the $D2(x,y)$ mask pixels. Information regarding the location of this extracted subset is defined using a binary image, in our case an image of the head of a well-known cartoon character. This location information is crucially important in our method and must also be transmitted to the receiver in order to decrypt the object image correctly. Therefore, $D2(x,y)$ provides all the random phase key information in our pseudo encryption system.

#### 2.1.3. Embedding the encrypted object image into the encrypted pseudo image

In order to obtain the final encrypted image, we embed the encrypted object image into the encrypted pseudo image. The location within the encrypted pseudo image into which the encrypted object image is embedded is determined in the same way that the locations of the $D4(x,y)$ pixel values are determined within $D2(x,y)$. First we remove part of the encrypted pseudo

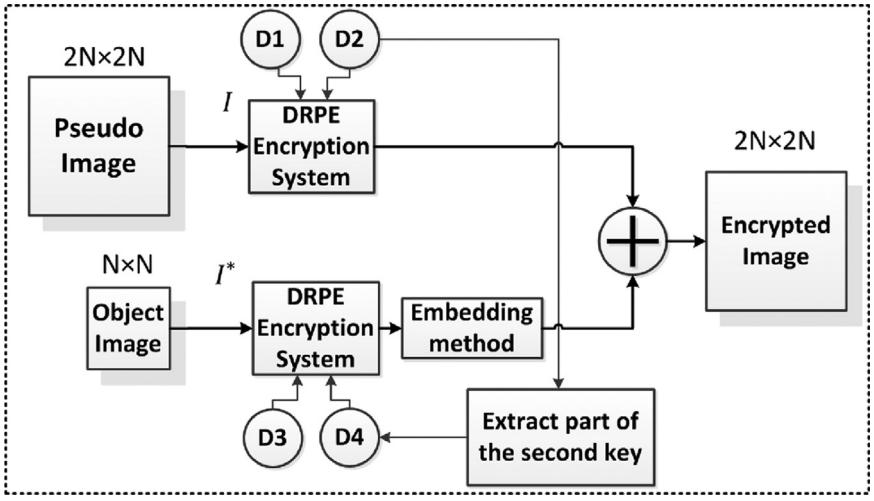


**Fig. 1.** Illustration of the encryption process.

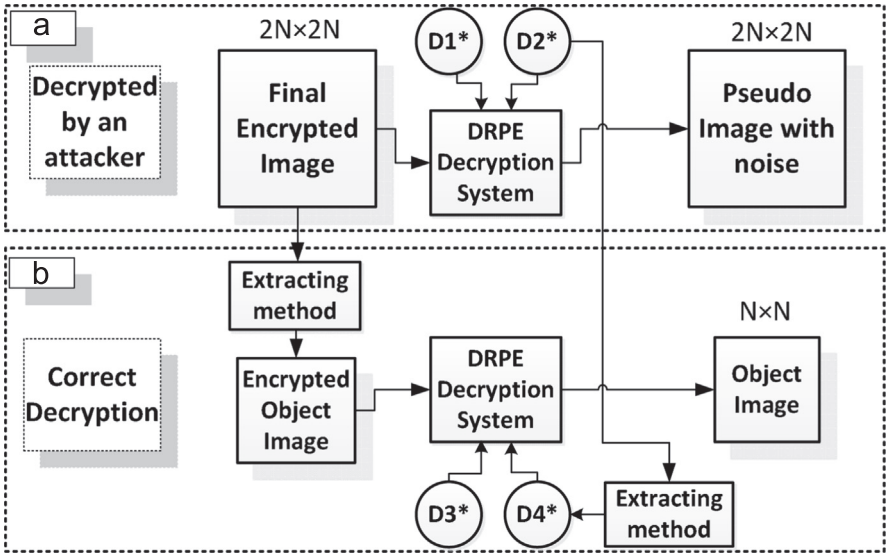


**Fig. 2.** Illustration of both (a) an incorrect (TOP) and (b) correct decryption process.