Optics Communications 310 (2014) 69–74

Contents lists available at ScienceDirect

Optics Communications

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

# Optical information encryption based on incoherent superposition with the help of the QR code

Yi Qin*, Qiong Gong

*College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China*

ARTICLE INFO

*Article history:*
Received 18 June 2013
Received in revised form
14 July 2013
Accepted 26 July 2013
Available online 8 August 2013

*Keywords:*
Optical encryption
Incoherent superposition
QR code

ABSTRACT

In this paper, a novel optical information encryption approach is proposed with the help of QR code. This method is based on the concept of incoherent superposition which we introduce for the first time. The information to be encrypted is first transformed into the corresponding QR code, and thereafter the QR code is further encrypted into two phase only masks analytically by use of the intensity superposition of two diffraction wave fields. The proposed method has several advantages over the previous interference-based method, such as a higher security level, a better robustness against noise attack, a more relaxed work condition, and so on. Numerical simulation results and actual smartphone collected results are shown to validate our proposal.



## 1. Introduction

Optical technology has been widely used in information encryption and decryption application, owing to its multiple parameters and parallel processing ability. In the past decade, various algorithms and systems about optical information encryption and security have been proposed [1–8]. The pioneering work was devoted by Refregier and Javidi, who proposed the double random phase encoding (DRPE) technique in 1995 [6]. After that, DRPE techniques in the fractional Fourier and Fresnel domains were explored successively [7,8], which enhanced the security of the technique with extra keys such as distance and wavelength. The security of DRPE has also been thoroughly analyzed and a few weaknesses have started to appear [9,10]. Besides, the DRPE technique involves a complex ciphertext, which is not very convenient for optical decryption, since spatial light modulators (SLMs) are not able to modify the amplitude and the phase simultaneously. To address this issue, researchers proposed lots of methods with which one can encrypt images into phase only masks (POMs) [11–13]. Nevertheless, phase retrieval algorithms must be used to obtain the POMs in the above-mentioned works. To remove the disadvantage of iterative computations, Zhang et al. [14] proposed an interference-based optical encryption (IBOE) scheme to encode the image into two pure phase masks based on the optical interference. With the aid of the two POMs calculated analytically in the encryption process, authorized users can record the decrypted image directly in the output plane by using an intensity device. Although this method is simple and does not have the problem of time-consuming computation, it suffers the silhouette problem, which is considered as one serious security vulnerability [15–17].

As stated above, optical encryption method has gained great success in information security. However, an important question remains concerning the quality of the decryption results. Since the light sources employed by most of the encryption schemes are coherent, the optically decrypted outcomes are always polluted by the speckle noise and hence degraded in quality. In this regard, potentials user are reluctant to accept the optical protocols in view of the degraded original inputs. Recently, Barrera et al. successfully settled the problem by merging the Quick Response Code (QR code) to the optical encryption [18]. In their approach, the information was transformed into the corresponding QR code before a standard optical encrypting procedure. Therefore the original information could be retrieved without quality loss, as QR codes are tolerant to speckle noise.

In this paper, with the help of the QR code and by utilizing the characteristic of the IBOE method, a novel method based on the incoherent superposition is proposed. The silhouette problem, which was treated as a safe flaw of the IBOE scheme, plays an important role in this proposal. In our method, the QR code of the original information to be encrypted is first divided equally into two parts, thereafter each part is encoded into a POM by using a particular illuminating wavelength. For decryption, the superposition of the intensity of the diffraction fields of the two POMs will regenerate the QR code and hence the original information.

This paper is organized as follows. The encryption and decryption procedure is presented in Section 2. The simulation results together with discussions are given in Section 3 and a brief conclusion is included in Section 4.

* Corresponding author. Tel.: +86 135 692 23036.
*E-mail address:* 641858757@qq.com (Y. Qin).

0030-4018/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.optcom.2013.07.062

## 2. Principle of the system

### 2.1. The IBOE method and the silhouette problem

In this section, we will first review IBOE method [14] and study the performance of the silhouette problem when binary images are encrypted. The system is schematically shown in Fig. 1. The distance between the phase mask $M_1$ and output plane is $l$, which is equal to the distance between $M_2$ and the output plane. Thus two beams interfere with each other at the output plane and generate a complex filed whose amplitude is exactly the original image encrypted in the two POMs.

To encrypt the target image into the two phase-only masks, the normalized amplitude image $f(x_o,y_o)$ is first multiplied by a random phase mask to construct a complex value image as [14]

$$f'(x_o,y_o)=\sqrt{f(x_o,y_o)}\exp[i2\pi \mathrm{rand}(x_o,y_o)], \tag{1}$$

where $\mathrm{rand}(x_o,y_o)$ generates a random distribution with the range [0,1]. According to the principle of decryption process, we have [14]

$$f'(x_o,y_o)=\mathrm{F}^{-1}\{\mathrm{F}[\exp(iM_1)+\exp(iM_2)]\times H(f_x,f_y)\}, \tag{2}$$

where $F[]$ denotes the Fourier transform and $\mathrm{F}^{-1}[]$ denotes the inverse Fourier transform, and [19]

$$H(f_x,f_y)=\exp\left[i\frac{2\pi l}{\lambda}\sqrt{1-(\lambda f_x)^2-(\lambda f_y)^2}\right], \tag{3}$$

indicates the transfer function. $f_x$ and $f_y$ are spatial frequencies and $\lambda$ is the wavelength of the incident light. By the use of Fourier transform theory, Eq. (2) can be rewritten as [14]

$$\exp(iM_1)+\exp(iM_2)=D, \tag{4}$$

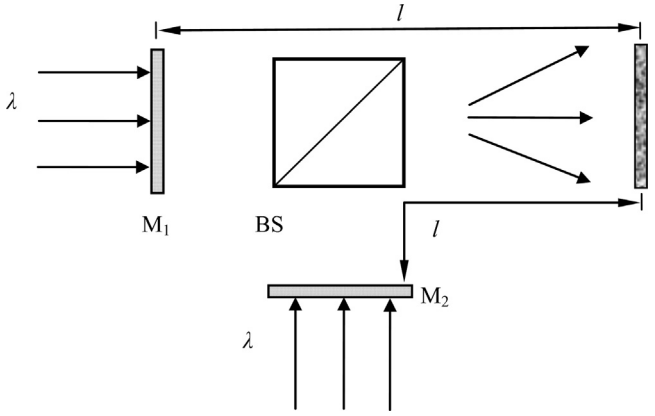


**Fig. 1.** Schematic of the decryption setup of the IBOE method.

where $D=F^{-1}\{F[f'(x_o,y_o)]/H(f_x,f_y)\}$. Since two masks are phase-only elements, we have [14]

$$[\exp(iM_1)][\exp(iM_1)]^*=[\exp(iM_2)][\exp(iM_2)]^*=1, \tag{5}$$

where the superscript * denotes the complex conjugate. Finally, we could obtain the phase distributions of the two masks as [14]

$$M_1=\arg(D)-\arccos[\mathrm{abs}(D)/2], \tag{6}$$

$$M_2=\arg[D-\exp(iM_1)], \tag{7}$$

For brevity, we mathematically denote the whole encryption process as

$$M_1=\psi[f(x_o,y_o),\lambda;l], \tag{8}$$

$$M_2=\phi[f(x_o,y_o),\lambda;l], \tag{9}$$

As has been investigated in depth in previous works [15–17], this encryption scheme has an inherent silhouette problem. Recently, several effective methods have been proposed to resolve this problem [20–22]. For instance, Chen has proposed to introduce a series of random and fixed phase only masks into the optical paths to eliminate it [20]. Chen also devoted a three-dimensional processing strategy to suppress the silhouette problem [21], to name a few. The silhouette problem was considered as an important security leak of the IBOE scheme since any one of the two POMs can provide considerable information of the primary image even though the object tested is a grayscale image. So it would be expected that the silhouette will give more information about the primary image if a binary one is employed in the IBOE scheme, since binary images have better robustness against noise compared with grayscale images. Computer simulations are carried out to show validity of this deduction. A normalized amplitude binary image with the size of $300\times300$ pixels, as shown in Fig. 2(a), is chosen as the target image. Fig. 2(b) and (c) show the decryption results reconstructed from one of the two POMs and the other, respectively. It can be seen that there is a strong resemblance between the silhouette and the original image. To objectively estimate these decryption results, we calculate the correlation coefficient (CC) between the recovered image $\hat{f}(x_o,y_o)$ and the primary image $f(x_o,y_o)$. It is defined as

$$\mathrm{CC}=\frac{E\{[f-E(f)][\hat{f}-E(\hat{f})]\}}{\sqrt{E\{[f-E(f)]^2\}E\{[\hat{f}-E(\hat{f})]^2\}}}, \tag{10}$$

where E[] is the expectation value. The coordinates are omitted here for brevity.

The CC values for Fig. 2(b) and (c) are calculated to be 0.9329 and 0.9316, which indicates that the silhouette is almost a reproduction of the original image. In other words, the diffraction of any one of the two POMs is able to regenerate the original binary image successfully. In the subsequent section, this character will be utilized and a novel encryption method will be proposed

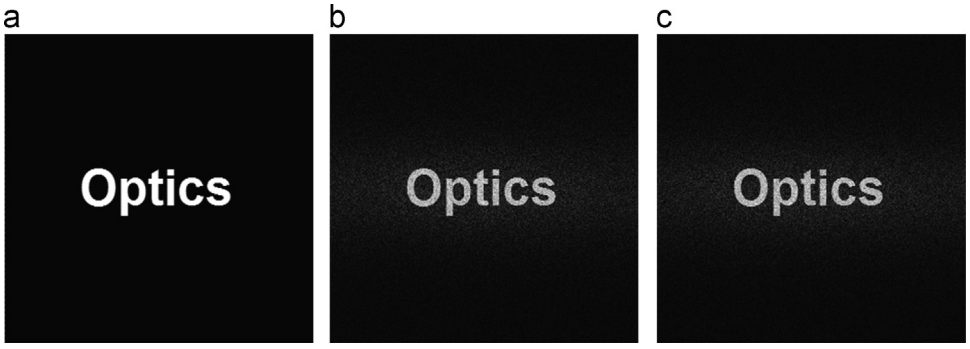


**Fig. 2.** The original image (a) and the decryption results with (b) one POM and (c) the other.