Optics and Lasers in Engineering 84 (2016) 62–73

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal

Yi Qin [a,*], Hongjuan Wang [a], Zhipeng Wang [b], Qiong Gong [a], Danchen Wang [c]

[a] College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China
[b] College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China
[c] Sichuan Information Security Testing Evaluation Center, Chengdu 610000, China

ARTICLE INFO

Article history:
Received 1 February 2016
Received in revised form
25 March 2016
Accepted 29 March 2016
Available online 12 April 2016

Keywords:
Optical encryption
QR code
Silhouette problem

ABSTRACT

In optical interference-based encryption (IBE) scheme, the currently available methods have to employ the iterative algorithms in order to encrypt two images and retrieve cross-talk free decrypted images. In this paper, we shall show that this goal can be achieved via an analytical process if one of the two images is QR code. For decryption, the QR code is decrypted in the conventional architecture and the decryption has a noisy appearance. Nevertheless, the robustness of QR code against noise enables the accurate acquisition of its content from the noisy retrieval, as a result of which the primary QR code can be exactly regenerated. Thereafter, a novel optical architecture is proposed to recover the grayscale image by aid of the QR code. In addition, the proposal has totally eliminated the silhouette problem existing in the previous IBE schemes, and its effectiveness and feasibility have been demonstrated by numerical simulations.

1. Introduction

Along with the rapid development of Internet, information security has become an increasingly serious problem. Image encryption methods originated from computer science have been extensively studied and numerous new algorithms are invented [1–6]. Some representative examples include algorithms based on one-time keys [7], mathematical model [8], bit-level scrambling [9] and DNA computing [10], which have been demonstrated to have high security. However, the speed performance of them mainly depend on the computer, and thus people search for alternative methods with higher time efficiency.

Recently, optical image encryption has aroused widely interest due to its remarked parallel data processing ability [11–19]. The most famous work in this field is the double random phase encoding (DRPE) technique invented in 1995 [20]. The DRPE is constructed by introducing two random phase only masks (POMs) into the optical 4f system, which are located at the input plane and the Fourier plane [20]. The DRPE has fully exhibited the merits of optical security techniques over the traditional methods, such as high speed and parallelism. Thereafter, various other approaches based on modern optical techniques, such as optical transform [21], diffraction [22], and polarization [23], are further developed for optical image encryption. In particular, Zhang and Wang described a novel interference-based encryption (IBE) method to analytically encrypt an image into two phase-only masks [24]. It is regarded as an breakthrough of the previous methods which must employ iterative algorithms to encrypt an image into phase only masks [25,26]. Moreover, the decryption procedure of this method is also very simple, because the decrypted image can be directly recorded by CCD camera. Afterwards, the IBE method is extensively studied and many new approaches based on it are presented [27–32]. Unfortunately, it is found to have an inherent silhouette problem. That is, if one of the two POMs is utilized in the decryption architecture, the silhouette of the primary image can be observed. Since the silhouette divulges sufficient information about the plaintext and hence becomes a security leak, people developed a lot of methods to remove it [28–31].

Recently, in order to enhance the efficiency of secret-information transmission, many approaches for achieving multiple-image encryption in optical architecture are invented. For instance, Situ and Zhang showed that wavelength multiplexing [33] can be exploited for multiple binary-image encryption in DRPE scheme. Barrera taken advantage of polarization multiplexing to encrypt multiple images in a holographic framework [34]. With regard to the IBE scheme, Wang et al. [35] and Chen et al. [36] successively hide two and multiple image into POMs in it. However, these two methods both have to endure a time-consuming iterative process to finish the encryption, and this drawback restrict their application to low-speed information encryption. Although a recent

* Corresponding author.
E-mail address: 641858757@qq.com (Y. Qin).

http://dx.doi.org/10.1016/j.optlaseng.2016.03.028
0143-8166/

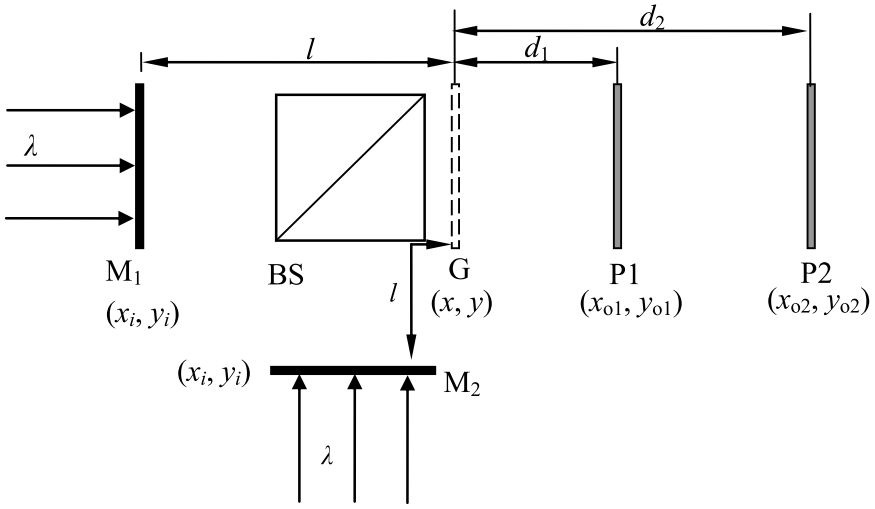

Fig. 1. The optical setup for illustrating position multiplexing in IBE scheme. M, phase only mask; λ, wavelength; BS, beam splitter.

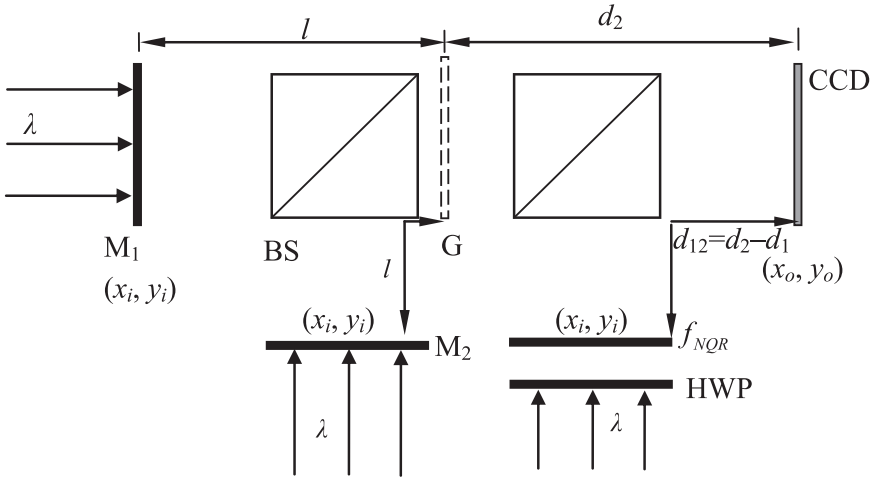

Fig. 2. The optical scheme for retrieving the grayscale image. M, phase only mask; λ, wavelength; BS, beam splitter; HWP: half wave plate.

proposal [37] can abstain the time-consuming iterative process, it can only be used to encrypt binary images due to the vexatious cross-talk. In this paper, we propose a novel method to encrypt two images (QR code and grayscale image) in the IBE scheme by position multiplexing. The encryption process is analytical, and the decryption can be performed optically. Especially, the carefully designed decryption method ensures the primary images can be retrieved without any crosstalk. Meanwhile, the silhouette problem, which has been considered as an important risk to the IBE scheme, is also eliminated.

2. Principle

2.1. QR code

A QR code is a special type of barcode that allows its content to be decoded at high speed. It consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera, scanner, etc.) The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity. An important character of QR codes is its function of error correction. In other words, when the QR code is generated, some redundant data, which will help a QR reader accurately read the code even if part of it is unreadable, is also created. Consequently, information can be correctly scanned even though localized contamination pollutes the QR code. Barrera et al. first propose to employ QR as a "container" of information to resist speckle noise [38,39]. More details about QR code could be found in [40]. In recent years, the encryption approaches using QR code have been widely studied [41–43].

2.2. Encryption

Our task is to encrypt a QR code as well as a grayscale image into two POMs. The position multiplexing technique described in [37] is employed, but the whole encryption process is obviously different from that of [37]. Let $f_{QR}(x_{o1}, y_{o1})$ and $f_{GS}(x_{o2}, y_{o2})$ respectively stand for the QR code and the grayscale image. First of all, a new image $f_{NQR}(x_{o1}, y_{o1})$ is created by using the following method:

$$f_{NQR}(x_{o1}, y_{o1}) = \begin{cases} f_{QR}(x_{o1}, y_{o1}) + \mathrm{RAM}(x_{o1}, y_{o1}) & \text{if} \quad f_{QR}(x_{o1}, y_{o1}) = 0 \\ f_{QR}(x_{o1}, y_{o1}) & \text{if} \quad f_{QR}(x_{o1}, y_{o1}) = 1 \end{cases}$$
$$\text{with} \quad \mathrm{RAM}(x_{o1}, y_{o1}) = \mathrm{rand}(x_{o1}, y_{o1}) \tag{1}$$