Optics and Lasers in Engineering ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Discussion and a new method of optical cryptosystem based on interference

Dajiang Lu, Wenqi He *, Meihua Liao, Xiang Peng *

College of Optoelectronic Engineering, Key Laboratory of Optoelectronics Devices and Systems, Education Ministry of China, Shenzhen University, Shenzhen 518060, China

ARTICLE INFO

Article history:
Received 30 November 2015
Received in revised form
29 February 2016
Accepted 5 April 2016

Keywords:
Optical information security
Hierarchical authentication
Interference

ABSTRACT

A discussion and an objective security analysis of the well-known optical image encryption based on interference are presented in this paper. A new method is also proposed to eliminate the security risk of the original cryptosystem. For a possible practical application, we expand this new method into a hierarchical authentication scheme. In this authentication system, with a pre-generated and fixed random phase lock, different target images indicating different authentication levels are analytically encoded into corresponding phase-only masks (phase keys) and amplitude-only masks (amplitude keys). For the authentication process, a legal user can obtain a specified target image at the output plane if his/her phase key, and amplitude key, which should be settled close against the fixed internal phase lock, are respectively illuminated by two coherent beams. By comparing the target image with all the standard certification images in the database, the system can thus verify the user's legality even his/her identity level. Moreover, in despite of the internal phase lock of this system being fixed, the crosstalk between different pairs of keys held by different users is low. Theoretical analysis and numerical simulation are both provided to demonstrate the validity of this method.

1. Introduction

Information security receives more and more attention in this information age. With the development of diverse communication, security problem of information exchanging plays an important role in communication platform in which images are widely used as the information carriers. In 1995, Javidi proposed a novel method to encrypt an image through an optical way, that's now what we call double-random-phase encoding (DRPE) [1]. Since then, optical information security technology has experienced an extensive investigation and development due to its parallelism, multiple dimensions, and high degree of freedom compared with traditional security systems. Besides extending DPRE technique to various transform domains, e.g., fractional Fourier transform domain [2–4], Fresnel transform domain [5], many other methods are based on digital holography [6,7], virtual optics [8], diffractive imaging [9–11], two-beam interference [12], ghost imaging [13], integral imaging [14,15], ptychography [16,17], etc.

In fact, most of these optical information security techniques tend to be utilized for optical image encryption systems. Nevertheless, many researchers have also contributed to optical authentication systems [18–21]. In general, these authentication systems involve two core components: one, the lock, is always fixed inside the system; the other, the key(s), is (are) held by the legal users. Mostly, if the key is correctly presented in the verification stage, it will interact with the lock by some specific means, (e.g., correlation, interference), leading to a correlated peak or a significant image at the output plane.

Actually, some optical encryption methods could also transfer their functions to optical authentication. The optical image encryption based on principle of interference proposed by Zhang et al. in 2008 [12] is just such a method which could be taken advantage for optical authentication system. In Zhang's method, an image is analytically encoded into two phase-only masks (POMs). Only if these two POMs were correctly placed at the input plane could the image be obtained at the output plane. In terms of encryption scheme, any one of the POMs could be considered as the ciphertext while the other as the decryption key. And from the view of authentication, any one of the POMs can be regarded as the system's lock and the other as the key held by legal user. Zhang's method has aroused many researchers' concern since its structure is quite simple and the algorithm does not require any iteration. However, it has an inherent drawback: a silhouette of the desired image would be revealed if only one of the two POMs is employed in the verification process. Thereby, many researchers

* Corresponding authors.
E-mail addresses: ludajiang@outlook.com (D. Lu), he.wenqi@qq.com (W. He), xpeng@szu.edu.cn (X. Peng).

http://dx.doi.org/10.1016/j.optlaseng.2016.04.004
0143-8166/

have attempted to vanquish the silhouette problem. One solution is to utilize pixel scrambling techniques [22,23], yet results in time-consuming. By using of phase retrieval algorithm (PRA), the silhouette can be also removed [24,25]. Nevertheless, PRA, likewise, would increase the computational load to the system. Some other proposals suggest encoding the original image into three POMs [26–28], of which any one would not reveal the silhouette of the image, yet two would. Yuan et al. proposed an information hiding method [29], which allows an image to be encoded into one predefined amplitude only mask (host image) and one complex amplitude (key). However, the silhouette of the image to be hidden could be also observed when only the key or the phase of the key is presented in the input. Recently, Cai et al. proposed a new optical cryptosystem based on equal modulus decomposition and interference principle [30]. Due to introducing two more amplitude modulations to the marks, the silhouette problem has been weakened, yet still appears if we only use one or two phase parts of the masks. It's because that the amplitude modulations are the same, leading to symmetric phase-distribution of the masks, which equally contain the information from the original image. In this paper, we present an optical authentication system with silhouette removal based on two-beam interference. According to our method, the verification phase lock is a predefined POM. An image can be analytically encoded into another POM as the phase key and one amplitude-only mask (AOM) as the amplitude key. Only if the two keys and the phase lock are employed could the verification image be obtained. Any one of the keys would not expose the silhouette of the verification image. Furthermore, we can expand this method into a low-crosstalk hierarchical authentication system with single fixed random phase lock. The proposed system can not only confirm the legality of a user but also distinguish his/her identity level.

The rest of this paper is arranged as follows: Section 2 provides a brief description and a detailed security analysis for original method proposed by Zhang et al. Section 3 proposes an optical authentication method based on two beams interference. Section 4 extends our method to an optical hierarchical authentication system. Section 5 shows a series of computational simulations to certify the validity of this scheme, and Section 6 draws a conclusion.

2. Zhang's method and its vulnerability

In advance, we would like to give a brief description for the original cryptosystem based on interference proposed by Zhang et al. [12]. As shown in Fig. 1, two incident coherent lights, after respectively passing through two POMs and experiencing a Fresnel propagation, will interfere with each other at the output plane, at where a desired image can be obtained (usually recorded by a CCD). Assuming that the amplitude distribution of the image to be encrypted is $O(x, y)$, we should design the phase distributions of two POMs (M1, M2) and ensure the following equation is satisfied.

$$FrT_{\lambda,l}\{\exp[iM(x,y)]\} + FrT_{\lambda,l}\{\exp[iN(x,y)]\} = \sqrt{O(x,y)}\cdot\exp[i\cdot 2\pi\cdot rand(x,y)], \quad (1)$$

or

$$\exp[iM(x,y)] + \exp[iN(x,y)] = FrT_{\lambda,-l}\left\{\sqrt{O(x,y)}\cdot\exp[i\cdot 2\pi\cdot rand(x,y)]\right\}, = D(x,y) \quad (2)$$

where FrT denotes the Fresnel transform while λ and l represent the wavelength and the propagation distance, respectively. $rand(x, y)$ generates a random distribution between 0 and 1. $\exp[iM(x, y)]$ and $\exp[iN(x, y)]$ are expressions of M1 and M2, respectively. As $O(x, y)$ and $rand(x, y)$ are predefined, we can solve out the phase distributions of the two POMs.

$$M(x,y) = \arg\left[D(x,y)\right] - ar\cos\left\{\frac{\mathrm{abs}[D(x,y)]}{2}\right\}, \quad (3)$$

$$N(x,y) = \arg\{D(x,y) - \exp[i\cdot M(x,y)]\}, \quad (4)$$

where the operators arg( ), abs( ) and arcos( ) represent the phase, modulus, and arccosine of a function, respectively. And the amplitude distribution of $D(x, y)$ should range from 0 to 2.

So far, the image to be encrypted $O(x, y)$ has already encoded into two POMs, $\exp[iM(x, y)]$ and $\exp[iN(x, y)]$. Once the two POMs are correctly employed in the input of the system, a clear desired image will be acquired at the output plane, as shown in Fig. 2(a). However, there exists a potential safety problem that a

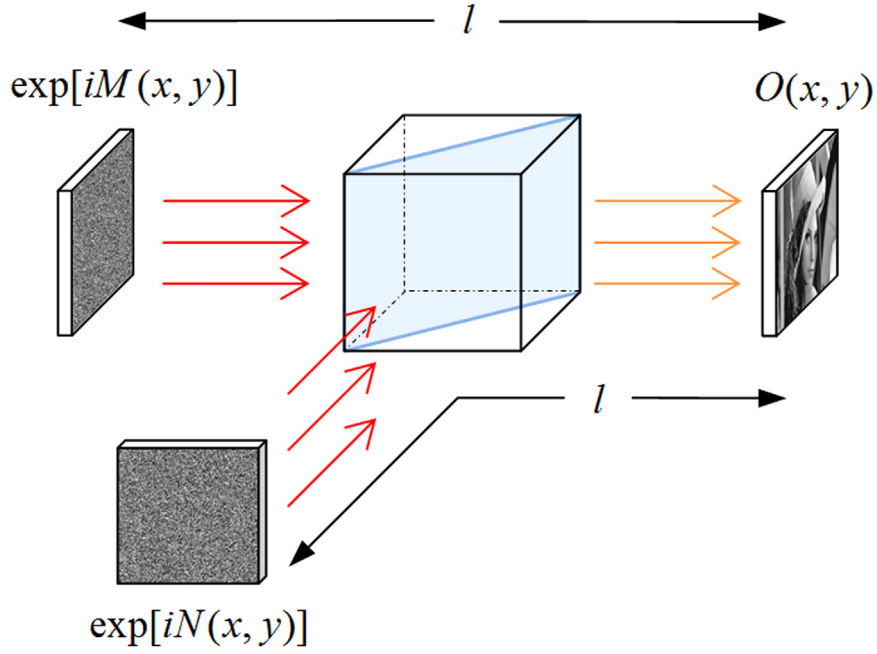

Fig. 1. The schematic diagram of Zhang's method.

Please cite this article as: Lu D, et al. Discussion and a new method of optical cryptosystem based on interference. Opt Laser Eng (2016), http://dx.doi.org/10.1016/j.optlaseng.2016.04.004