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

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

An interference-based optical authentication scheme using two phase-only masks with different diffraction distances

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
Optical authentication
Interference

ABSTRACT

A new method to eliminate the security risk of the well-known interference-based optical cryptosystem is proposed. In this method, which is suitable for security authentication application, two phase-only masks are separately placed at different distances from the output plane, where a certification image (public image) can be obtained. To further increase the security and flexibility of this authentication system, we employ one more validation image (secret image), which can be observed at another output plane, for confirming the identity of the user. Only if the two correct masks are properly settled at their positions one could obtain two significant images. Besides, even if the legal users exchange their masks (keys), the authentication process will fail and the authentication results will not reveal any information. Numerical simulations are performed to demonstrate the validity and security of the proposed method.

1. Introduction

Since Javidi proposed a double-random-phase encoding (DRPE) method for image encryption in 1995 [1], optical information security technology has been attracting more and more attention due to its high-speed parallel processing and multi-parameter capability. Apart from DPRE and DRPE-based techniques in different optical domains [2–5], various methods based on digital holography [6,7], diffractive imaging [8–10], interference [11], ghost imaging [12], integral imaging [13,14], ptychography [15,16] have also been proposed. The interference-based optical encryption/authentication scheme proposed by Zhang in 2008 [11], is one of the most studied method because of its simple structure and non-iterative characteristic. In Zhang's method, an image is analytically encoded into two phase-only masks (POMs); one of which, however, will reveal a silhouette of the original image. This internal security risk has aroused many researchers' concern and various improved method have been presented [17–30]. One solution is to utilize pixel scrambling techniques [17,18], which can visually erase the silhouette effect but still retain the equipollent nature and symmetry property of POMs. Some proposals suggest encoding the original image to into three POMs [19–21], of which one would not reveal the silhouette of the image, yet two would. Yuan proposed an information hiding method [22], 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 proposed a new optical cryptosystem based on equal modulus decomposition and interference principle [23]. Due to introducing two more amplitude modulations to the marks, the silhouette problem is weakened; yet it 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. All the improved approaches mentioned above are still based on analytical solutions, which cannot completely vanquish the linearity and the silhouette problem. Apart from the analytical solution, other researchers take advantage of phase retrieval algorithm (PRA) [26–30]. Although PRA will always be time consuming, it's an effective way to radically remove the equipollent nature of the POMs. In this paper, we present a dual optical authentication system with silhouette removal based on two-beam interference and PRA. According to our method, two POMs with different Fresnel propagation distances serve as two private keys of a legal user. And two certification images (public image and secret image) can be obtained at two output planes to confirm one's legality and identity, respectively. Comparing with the aforementioned methods, any one of the keys would not expose the silhouettes of the verification images. Furthermore, the introducing of a secret image can avoid an illegal attacker hacking into the proposed system by producing collision to the public image.

The rest of this paper is organized as follows: Section 2 provides a brief description and a security analysis for the original

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

http://dx.doi.org/10.1016/j.optlaseng.2016.04.002
0143-8166/

method proposed by Zhang. Section 3 proposes an interference-based optical authentication method using two phase-only masks with different diffraction distances. Section 4 extends our method to a dual authentication system. Section 5 performs a series of numerical simulations to certify the validity of this scheme, and Section 6 draws a conclusion.

2. Zhang's method and its silhouette effect

To begin with, we'd like to give a brief description for the interference-based original cryptosystem proposed by Zhang [11]. As shown in Fig. 1, two beams of coherent lights, being respectively modulated by two POMs, will go through a Fresnel propagation and then interfere with each other. A pre-designed image can be obtained at the output plane (usually recorded by a CCD). To make sure that we are able to get the desired amplitude-distributed image $O(x, y)$, we have to calculate out the phase distributions of two POMs (M1, M2), which should satisfy the following equation.

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

or

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

where FrT denotes the Fresnel transform while λ and l represent the wavelength and the propagation distance, respectively. $R(x, y)$ is an auto-generated random distribution ranging from 0 to 2π. $\exp[iM(x, y)]$ and $\exp[iN(x, y)]$ are expressions of M1 and M2, respectively. As $O(x, y)$ and $R(x, y)$ are known, we can easily solve out the phase distributions of the two POMs with the help of vector decomposition, as shown in Fig. 2.

$$\exp[iM(x,y)] = \frac{1}{2}D(x,y) + A(x,y), \quad (3)$$

$$\exp[iN(x,y)] = \frac{1}{2}D(x,y) + B(x,y) = \frac{1}{2}D(x,y) - A(x,y), \quad (4)$$

$$|D(x,y)| \le 2, \quad (5)$$

where $B^*(x, y) = A(x, y) = |A(x, y)| \cdot \exp\{i \cdot \arg[A(x, y)]\}$, and $|A(x, y)| = \sqrt{1 - [\frac{1}{2} \cdot |D(x, y)|]^2}$, $\arg[A(x, y)] = \arg[D(x, y)] - \frac{\pi}{2}$.

Eqs. (3) and (4) show that both of M1 and M2, and even the superfluous term $A(x, y)$, have a strong relationship with $D(x, y)$, which can directly expose the secret image after a Fresnel transform. That's why the silhouette appears when only one POM is applied for the decryption. Besides, it's obvious that there is only one possibility to decompose $D(x, y)$ into two phase-only distributions (M1, M2), which are symmetric with respect to $D(x, y)$. It can be inferred that the equipollent nature of the POMs is caused by the same propagation distance, and the uniform amplitude modulation of two POMs since both moduli of POMs are all-ones matrixes at the input plane.

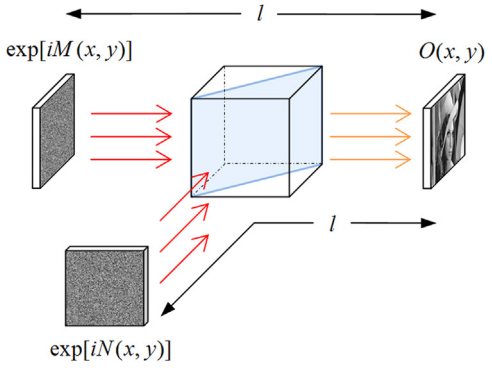

Fig. 1. Schematic diagram of Zhang's method.

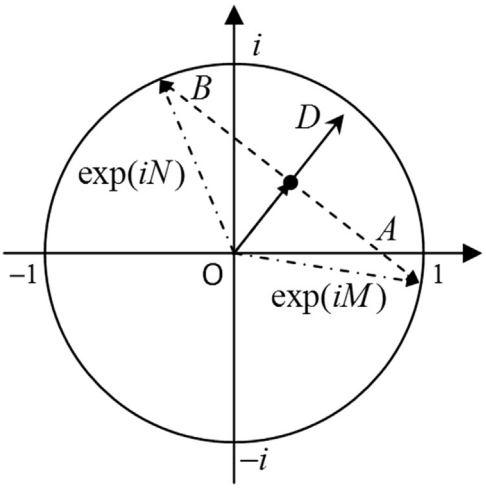

Fig. 2. Decomposition of $D(x, y)$ with Zhang's method.

3. An interference-based optical authentication system with silhouette removal

As we mentioned in Section 2, the silhouette problem of Zhang's method is due to the same Fresnel propagation distance and the uniform amplitude-modulations of the two POMs. To dissolve this security risk, we can either introduce other amplitude-modulations to the POMs or vary the propagation distances. In this paper, we'd like to take the latter operation since it can be realized by a relatively more simplified structure, as shown in Fig. 3. Thus, the propagation process can be described as

$$FrT_{\lambda,l_1}\{\exp[iM(x,y)]\} + FrT_{\lambda,l_2}\{\exp[iN(x,y)]\} = \sqrt{O(x,y)} \cdot \exp[i \cdot R(x,y)], \quad (6)$$

or

$$\exp[iM(x,y)] + FrT_{\lambda,l_2-l_1}\exp[iN(x,y)] = FrT_{\lambda,-l_1}\{\sqrt{O(x,y)} \cdot \exp[i \cdot R(x,y)]\} = D(x,y), \quad (7)$$

where l_1 and l_2 denote the Fresnel propagation distances of M1 and M2, respectively. Both $\exp[iM(x, y)]$ and $\exp[iN(x, y)]$ are treated as the private phase keys held by legal users. $O(x, y)$ is the interference intensity pattern as well as the target image at a specified output plane. By comparing the target image with all the standard certification images in the database, the system can thus verify whether a user is legal or not.

So far, all we have to do is to find out the phase-distribution of M1 and M2. Before doing this, we'd like to illustrate that how the silhouette problem can be avoided if we introduce different diffraction distances. As shown in Fig. 4, comparing with Zhang' method, infinite possibilities for the decomposition of the complex vector $D(x, y)$ can be found in our approach. In this situation, the POMs (M1 and M2) will no longer share the equipollent information from the image.

Back to our scheme, it's hard to analytically calculate out a

Please cite this article as: Lu D, et al. An interference-based optical authentication scheme using two phase-only masks with different diffraction distances. Opt Laser Eng (2016), http://dx.doi.org/10.1016/j.optlaseng.2016.04.002