Optics & Laser Technology 44 (2012) 888–892

Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

An improved optical identity authentication system with significant output images

Yuan Sheng*, Liu Ming-tang, Yao Shu-xia, Xin Yan-hui

Department of Information Engineering, North China University of Water Resources and Electric Power 36, Bei-huan Road, Zhengzhou 450011, PR China

ARTICLE INFO

Article history:
Received 25 September 2011
Received in revised form
12 November 2011
Accepted 12 November 2011
Available online 29 November 2011

Key words:
Optical identity authentication
Identity verification
Double random-phase encoding

ABSTRACT

An improved method for optical identity authentication system with significant output images is proposed. In this method, a predefined image is digitally encoded into two phase-masks relating to a fixed phase-mask, and this fixed phase-mask acts as a lock to the system. When the two phase-masks, serving as the key, are presented to the system, the predefined image is generated at the output. In addition to simple verification, our method is capable of identifying the type of input phase-mask, and the duties of identity verification and recognition are separated and, respectively, assigned to the amplitude and phase of the output image. Numerical simulation results show that our proposed method is feasible and the output image with better image quality can be obtained.

1. Introduction

Application of optical theories to information security has received increasing attention since Refregier and Javidi [1] proposed the method of double random-phase encoding (DRPE), which encodes a primary image into a stationary white noise. Subsequently, the DRPE technique was further extended from Fourier domain to fractional Fourier [2–5] and Fresnel domains [6,7]. Except for the optical image encryption in the application of phase encoding [1–12], optical identity authentication techniques have also been proposed and widely developed because the phase-masks are hard to duplicate [13–24].

An identity authentication system generally has two main duties: identity verification and recognition. Identity verification is to verify whether the user is authorized or not; and recognition is to make out the identities of the authorized users. Wang et al. proposed an optical encryption and verification method to encrypt an original image into a phase-only mask on the Fourier plane of a 4*f* correlator [18]. Li et al. modified this method to encode the image into a phase-only mask on the input plane of a 4*f* correlator [19]. In their methods, the phase-mask is obtained by phase retrieval algorithms such as the projection onto constraint sets (POCS) algorithm. The retrieved phase-mask and a fixed one, respectively, act as the key and the lock in the verification system. To reconstruct the predefined output image, the two phase-masks must be matched and located on the input plane and the Fourier plane, respectively. Abookasis et al. improved this method with a joint transform correlator for optical verification [20]. However, in all of the methods mentioned above, the iterative algorithm is employed to encode the original image into pure phase diffractive elements and the reconstructed output image is fuzzy. Moreover, the intensity of the output image assumes two duties of simple verification and identity recognition. Thus, different users must correspond to different output images and a large number of output images should be stored for multiuser application.

The basic ideas of these methods mentioned above are based on the diffraction of encoded elements. Recently, according to the optical interference principle, researchers proposed several verification systems [21–24]. For example, Zhang et al. proposed a method to encode a predefined output image into two phase-only masks [21]. When two light beams are modulated by the two matched phase-masks and interfere with each other at the output plane of the verification system, a known output image is generated. In this method, the generation of the two phase-masks is quite simple and does not need iterative algorithm. The secret image is protected by the phase function of the predefined output image and the parameters of the system. In absence of any of them, the two matched phase-masks can not be forged, so this method has a high security to avoiding attack.

Combining the verification methods based on the diffraction and the interference principles, we improve the optical identity authentication system with significant output images. Firstly, a predefined output image is digitally encoded into two phase-masks relating to a fixed phase-mask. The fixed phase-mask serves as the lock, while the generated two phase-masks serve as the key. A predefined output image could be generated at the output plane of the identity authentication system only if the key

* Corresponding author. Tel.: +86 371 69127302.
E-mail address: shn.yuan@sohu.com (S. Yuan).

0030-3992/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlastec.2011.11.014

phase-masks are right fit for the lock phase-mask. Our improved method yields better result and performance by utilizing the complementary advantages of a diffraction method [19] and an interference [21] method. The generation of two key phase-masks is quite simple and does not need the iterative algorithm, and a clear output image including its amplitude and phase can be yielded. In addition, even though intruders know the predefined output image, the two key phase-masks cannot be forged because they are also protected by the lock phase-mask. Moreover, the duties of identity verification and recognition are, respectively, assigned to the amplitude and phase of the output image. The duty assignment method may bring convenience in some applications.

2. Improved identity authentication scheme

2.1. Architecture of the identity authentication system

As shown in Fig. 1, our improved identity authentication system is composed by the interference architecture and the 4*f* system. The phase-masks M_1 and M_2 have the same distance of l to the input plane of the 4*f* system. The three planes P_1, P_2, and P_3 of the 4*f* system are defined as the input plane, the transform plane, and the output plane, respectively, and the corresponding coordinates of the three planes are denoted by (ξ,η), (u,v), and (x',y').

The identity authentication process can be described as follows: two coherent plane waves are, respectively, modulated by the phase-masks M_1 and M_2 (the keys), and then combined by a beam-splitter (BS). Thus, the two waves interfere with each other at the plane P_1 and generate the input image of the 4*f* system $I(\xi,\eta)$, which can be written as

$$I(\xi,\eta)=\exp(iM_1)\times h(x,y;l,\lambda)+\exp(iM_2)\times h(x,y;l,\lambda) \tag{1}$$

where

$$h(x,y;l,\lambda)=\frac{\exp(i2\pi l/\lambda)}{il\lambda}\exp\left[\frac{i\pi}{l\lambda}(x^2+y^2)\right] \tag{2}$$

is the point pulse response of the Fresnel transform, λ is the wavelength of the incident plane waves, and * denotes the convolution operation.

Subsequently, a predefined output image is generated at the output plane after the frequency spectrum of the input image $I(\xi,\eta)$ is modulated by the phase-mask M_3 (the lock) on the transform plane of the 4*f* system. The process can be mathematically expressed as

$$FT^{-1}\{FT\{I(\xi,\eta)\}\exp(iM_3)\}=f(x',y')\exp[iR(x',y')] \tag{3}$$

where FT and FT^{-1} represent the Fourier transform and the inverse Fourier transform, respectively; $f(x',y')$ and $R(x',y')$ are two significant images and denote the amplitude and the phase of the predefined output image, respectively. As long as the predefined output image (including its amplitude and phase) is generated, we believe the key phase-masks M_1 and M_2 are right for the lock M_3 and the user owned the key is authorized.

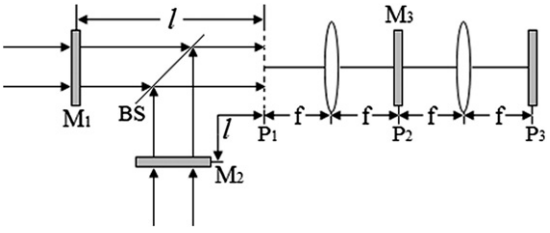

Fig. 1. Architecture of our proposed identity authentication system.

2.2. Generation of the key phase-masks

In the identity authentication system, the fixed phase-mask M_3 and the predefined output image (including the amplitude $f(x',y')$ and the phase $R(x',y')$) are known to the designer of the identity authentication system. Consequently, the main problem is how to find the two phase-masks M_1 and M_2 (the keys) according to the determined $f(x',y')$, $R(x',y')$, and M_3. Fortunately, it can be solved according to Zhang's method [21].

After a simple deduction for the Eqs. (1) and (3), we can have

$$[\exp(iM_1)+\exp(iM_2)]\times h(x,y;l,\lambda)=FT^{-1}\left\{\frac{FT\{f(x',y')\exp[iR(x',y')]\}}{\exp(iM_3)}\right\} \tag{4}$$

Here, the two phase-masks M_1 and M_2 can be obtained by a further deduction of Eq. (4), which can be written as

$$\exp(iM_1)+\exp(iM_2)=FT^{-1}\left\{\frac{FT\{f(x',y')\exp[iR(x',y')]\}}{FT\{h(x,y;l,\lambda)\}\exp(iM_3)}\right\} \tag{5}$$

If the right portion of the above equation is defined as

$$D=FT^{-1}\left\{\frac{FT\{f(x',y')\exp[iR(x',y')]\}}{FT\{h(x,y;l,\lambda)\}\exp(iM_3)}\right\} \tag{6}$$

Eq. (5) can be rewritten as

$$\exp(iM_2)=D-\exp(iM_1) \tag{7}$$

Since the modulus of the left portion of Eq. (7) is equal to Eq. (1), we have [21]

$$|D-\exp(iM_1)|^2=[D-\exp(iM_1)][D-\exp(iM_1)]^*=1 \tag{8}$$

where $[\cdot]_*$ denotes the conjugate of the argument. Then the two phase distributions can be obtained as [21]

$$M_1=\arg(D)-\arccos(abs(D)/2) \tag{9}$$

$$M_2=\arg(D-\exp(iM_1)) \tag{10}$$

where arg(.) represents the angle of the argument, and $abs(\cdot)$ denotes the modulus of the argument.

From the above deduction, we can see that the key phase-masks M_1 and M_2 are protected by the output image (including the amplitude $f(x',y')$ and the phase $R(x',y')$), the lock M_3, and the parameters (λ,l). They are confidential and known only to the designer of the verification system. In absence of any of them, the key phase-masks M_1 and M_2 cannot be forged. From another point of view, when any one of them (involving $f(x',y')$, $R(x',y')$, M_3, and the parameters (λ,l)) is changed, different key phase-masks M_1 and M_2 will be generated. To facilitate the multiuser application, we construct different key phase-masks M_1 and M_2 by changing the phases $R(x',y')$ of the output image and distribute them to different authorized users. The corresponding relationship between the key phase-masks M_1 and M_2 and the phases of the output images are illustrated in Fig. 2.

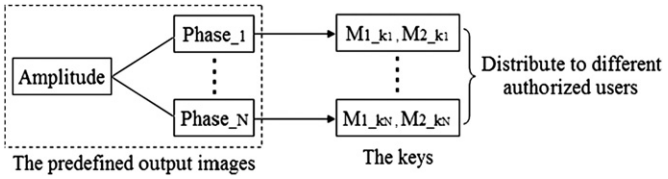

Fig. 2. Corresponding relationship between the key phase-masks and the phases of the output images.