Optics & Laser Technology 54 (2013) 120–127

Contents lists available at ScienceDirect

Optics & Laser Technology

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

An optical authentication system based on encryption technique and multimodal biometrics

Sheng Yuan [a,*], Tong Zhang [b], Xin Zhou [c], Xuemei Liu [a], Mingtang Liu [a]

[a] Department of Information Engineering, North China University of Water Resources and Electric Power, 36, Bei-huan Road, Zhengzhou, Henan 450011, PR China
[b] Henan Musuem, 8, Nongye Road, Zhengzhou 450008, PR China
[c] Department of Opto-electronics Science and Technology, Sichuan University, Chengdu 610065, PR China

ARTICLE INFO

Article history:
Received 24 April 2013
Accepted 17 May 2013
Available online 11 June 2013

Keywords:
Optical authentication technique
Optical encryption technique
Multimodal biometrics

ABSTRACT

A major concern nowadays for a biometric credential management system is its potential vulnerability to protect its information sources. To prevent a genuine user's templates from both internal and external threats, a novel and simple method combined optical encryption with multimodal biometric authentication technique is proposed. In this method, the standard biometric templates are generated real-timely by the verification keys owned by legal user so that they are unnecessary to be stored in a database. Compared with the traditional recognition algorithms, storage space and matching time are greatly saved. In addition, the verification keys are difficult to be forged due to the utilization of optical encryption technique. Although the verification keys are lost or stolen, they are useless for others in absence of the legal owner's biometric. A series of numerical simulations are performed to demonstrate the feasibility and performance of this method.

1. Introduction

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. Biometric identification consists of two stages: enrollment and verification. During the enrollment stage, a sample of the designated biometric is acquired. Some unique characteristics or features of this sample are then extracted to form a biometric template for subsequent comparison purposes. During the verification stage, an updated biometric sample is acquired. As in enrollment, features of this biometric sample are extracted. These features are then compared with the previously generated biometric template. Finally, the comparing results are used to determine whether the user is authorized or not.

In recent years, many optical information processing techniques have been widely applied in the field of information security [1–7], as they have the distinct advantage of processing two dimensional complex data in parallel. Optical identity authentication technique [8–13] has also aroused great interest for researchers and many approaches have been exploited such as the optical 4*f* correlator [8] and joint transform correlator based on the projection onto constraint sets (POCS) algorithm [9], and optical interference [10], etc. However, the keys have no relationship with the identity of the owner so that anyone can use the keys to pass the authenticator. Once the keys are lost or stolen, the security of the authentication system will be threatened.

In order to avoid the threat of the keys being lost or stolen, there has been an increasing interest in utilizing specific biometric feature of the user. Kim et al. have implemented a first practical digital holographic security system that combines digital holographic memory with the electrical biometrics [14]. Recently, Saini et al. proposed a new biohashing system based on joint transform correlator [15]. The main advantage of this technique is the possibility of the optical implementation of the feature extraction for a biometric image. Subsequently, they also proposed a new authentication system based on multiple biometrics and digital holography [16]. This method has advantage over other digital holographic security system due to its capability of authentication by using the biometric image of the enrolled person. However, in these authentication methods based on optical theory, the vulnerability of a database for a biometric credential management system is rarely concerned.

To ensure the security of database, we combine the optical encryption with multimodal biometric authentication technique and propose a novel optical authentication method in this paper. During the enrollment stage, two biometric templates, the face and palmprint of a legal user, are encoded into two phase-masks with the aid of another biometric (palmprint). The encoded

* Corresponding author. Tel.: +86 18203976519.
E-mail address: shn.yuan@sohu.com (S. Yuan).

0030-3992/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.05.021

process is implemented digitally according to the optical interference principle. In the identity verification process, the standard biometric images or templates are generated real-timely by the keys owned by legal users so that they are unnecessary to be stored in a database. This method changes one-to-many matching into one-to-one matching, so the matching time is reduced significantly. With the aid of the encryption system and biometric, the verification keys are difficult to be forged and the lost or stolen keys are useless for other person. Numerical simulations are performed to verify these performances.

2. Optical authentication system based on multimodal biometrics

2.1. Schematic of the authentication system

The authentication system is schematically shown in Fig. 1. Mr_1 and Mr_2 are two random phase-masks which are generated corresponding to the biometric templates of legal users. In order to prevent the phase-masks Mr_1 and Mr_2 from being forged, three independent random phase-masks (M_{k1}, M_{k2} and M_{k3}) are taken and fixed on the three input planes as the encryption key of the system, shown in Fig. 1. Thus, they are confidential and only known by the designer of the system. Moreover, M_P is another phase-only mask generated by another biometric image of a legal user such as palmprint. For simplify expression, we define three phase functions as $M_1 = 2\pi(Mr_1 + M_{k1})$, $M_2 = 2\pi(Mr_2 + M_{k2})$ and $M_3 = 2\pi(M_P + M_{k3})$.

2.2. Authentication principle

In the verification process, three coherent parallel light beams are modulated by the phase-masks located in their own light-path respectively, and then combined by two beam splitters (BS1 and BS2). Thus the three beams interfere with each other and generate a predefined image $g(\xi,\eta)$ at the plane P1 shown in Fig. 1. Fig. 2 is the flowchart of the authentication process, which can also be mathematically expressed as

$$g(\xi,\eta) = \exp(iM_1) * h(\xi,\eta;l_1) + \exp(iM_2) * h(\xi,\eta;l_2) + \exp(iM_3) * h(\xi,\eta;l_3)$$
$$= a(\xi,\eta)\exp[i2\pi\phi(\xi,\eta)] \quad (1)$$

where

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

is the point pulse response of the Fresnel transform, l_1, l_2 and l_3 denote the distances from the three phase-masks to the plane P1. Here, we set $l_1 = l_2 = l$. λ is the wavelength of the incident lights, and $*$ denotes the convolution operation. (ξ,η) denotes the coordinate on the plane P1. Two biometric templates $a(\xi,\eta)$ and $\phi(\xi,\eta)$ are taken as the amplitude and phase distributions of the predefined image $g(\xi,\eta)$, which is composed by the log-polar face and palmprint of a legal user (taken as the amplitude and phase part, respectively) in this paper, shown in the dashed box of Fig. 2.

The predefined complex image (i.e. templates) will be generated as long as the verification keys and the palmprint are matched. Now, how to compare the updated biometrics with the generated templates? Here, we adopt the phase-only filters (POFs), which is located in the frequency domain of the 4f correlator and constructed by the log-polar face and fingerprint of the user. Although POF is a mature technique, it is needed to be noted that the POF has some difference with the POF introduced in reference [17], which constructs from the phase part of frequency spectrum of a complex image. But here, the POFs are only generated by the frequency spectrum of the amplitude or phase part of the complex image, and they are respectively called as POF_A and POF_P. The construction process of the POFs can be illustrated as follows:

(i) POF_A constructed from the amplitude part of a complex image $g(\xi,\eta)$.

$$\text{Let} \quad f(\xi,\eta) = a(\xi,\eta), \quad (3)$$

where, $a'(\xi,\eta)$ is the updated log-polar face of a user in this paper. Then perform the Fourier transform to it,

$$F(u,v) = FT\{f(\xi,\eta)\} = A_f(u,v)\exp[i\Phi_f(u,v)], \quad (4)$$

where $FT\{\cdot\}$ denotes the Fourier transform, $A_f(u,v)$ and $\Phi_f(u,v)$ are the amplitude and the phase distributions of $F(u,v)$, respectively.

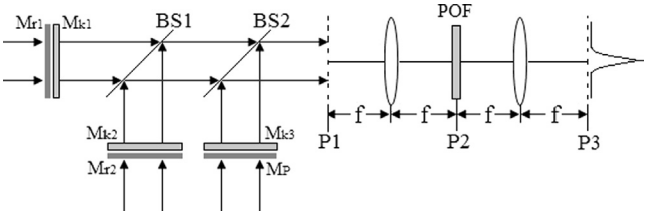

Fig. 1. Schematic of the information authentication system.

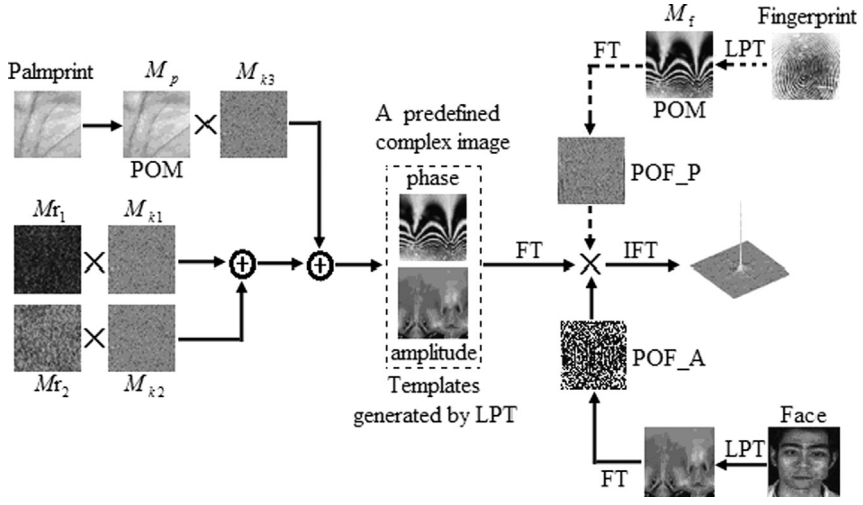

Fig. 2. Schematic illustrated the verification process. '×' denotes dot multiplication operator; '⊕' interference of two light beams; 'LPT' log polar transform; 'POM' phase-only mask; 'POF' phase-only filter; 'FT' Fourier transform; 'IFT' inverse Fourier transform.