Measurement 63 (2015) 41–48

Contents lists available at ScienceDirect

Measurement

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

Extraction and application of dynamic pupillometry features for biometric authentication

Vitor Yano [a,*], Alessandro Zimmer [b], Lee Luan Ling [a]

[a] Department of Communications, School of Electrical and Computer Engineering, University of Campinas, Campinas, SP 13083-852, Brazil
[b] Department of Electrical Engineering, Federal University of Paraná, Curitiba, PR 81531-970, Brazil

ARTICLE INFO

Article history:
Received 5 June 2014
Received in revised form 26 October 2014
Accepted 3 December 2014
Available online 11 December 2014

Keywords:
Dynamic pupillometry
Biometrics
Iris recognition

ABSTRACT

Iris recognition is considered one of the most secure biometric recognition methods. However, even this biometric trait can be frauded in some cases. In other cases, the quality of the captured image can affect the system recognition performance. This paper proposes a multimodal biometric authentication system that combines the use of dynamic features from the Pupillary Light Reflex (PLR) and the static features from the iris pattern for a better performance. A dynamic pupillometer device has been developed and a prototype system for features extraction and classification has been implemented. A pupillometric database has been created using data from 90 volunteers, and tests of the biometric system have lead to experimental of 0% EER.

1. Introduction

Biometric identification is already a fully consolidated research area. Some of interested groups on this field include government agencies, military, academic institutions, financial corporations and technology companies. The estimated revenue of commercial devices, systems and solutions for person recognition and verification based on physiological or behavioral features of individuals for the year of 2014 exceeds $10.2 billion [1].

The claimed advantages of biometrics over objects or knowledge-based identification are also well-known: as a body part or a behavior cannot be shared like a card or a password, the recognition of a person "by what they are" can prevent losses, copies or thefts [2]. This argument, however, is being increasingly proved not always true. Together with the development of biometric technologies, their spoofing vulnerabilities and also the anti-spoofing countermeasures have turned on a increasingly growing field of study [3–6].

Some of the strategies currently used in order to prevent direct attacks against biometric systems include hybrid authentication (which combines biometric features with a password or a card), multimodal biometrics [7] and liveness detection [6]. While the first one could hamper a fraud by involving a second security level, it still must deal with some issues of traditional authentication methods, such as losses or sharing.

Multimodal biometric authentication combines multiple biometric features to verify an identity. Depending on the features and the way they are fused, it can significantly difficult an imposter attack, due to the need of spoofing of multiple subsystems. This, however, still cannot guarantee that no fraud is possible.

The third method against spoofing attacks uses an evidence that the biometric characteristic presented to the sensor corresponds to a living human being, in order to prevent the use of artificial prostheses, removed body parts and corpses. The form of detection depends upon each technology, and can be based on three kinds of factors [6]: intrinsic properties of a living body (e.g. temperature, electrical resistance, reflectance), involuntary signals (such as the heart beat, pulse, pupillary hippus [8]) and

* Corresponding author. Tel.: +55 4195697915.
E-mail addresses: vitoryan@decom.fee.unicamp.br (V. Yano), zimmer@eletrica.ufpr.br (A. Zimmer), lee@decom.fee.unicamp.br (L.L. Ling).

http://dx.doi.org/10.1016/j.measurement.2014.12.001
0263-2241/

challenge-responses, which requires the user cooperation (blinks, smiles or other movements). This last method can be circumvented by the simulation of involuntary signals, or by the use of materials with attributes similar to the human body [6].

1.1. Pupillary Light Reflex

One example of signal that can be used for liveness detection is the Pupillary Light Reflex (PLR). As the reaction of pupil to changes in the light intensity only occurs in living persons, and the traditional iris recognition systems are vulnerable to the use of high resolution fake images [5,6], there are some proposals for using this signal, or its consequences in the iris texture, to avoid spoofing of this kind of biometric systems [9,10].

The PLR is an involuntary reaction of the body to an external stimulus that is based on the balance between the sympathetic and parasympathetic nervous systems, which are both parts of the autonomous nervous system [11]. For this reason, more than just a liveness indicator, the PLR can provide information about the condition of peripheral structures of the nervous system [12], being already demonstrated useful for the assessment of some diseases [13–15].

Moreover, the PLR has different characteristics in each individual [16–18], so its features can also be used for biometric identification.

1.2. Dynamic pupillometry

Pupillometry is the measurement of physical characteristics of the pupil, such as its diameter and format, and it is usually performed for psychological or clinical medical purposes [15,19].

In the case of static pupillometry, the assessment is done at one or more instants, by applying parasympathetico-mimetic agents solutions (for pupil constriction) such as methacholine and pilocarpine, or mydriatic agents (for dilation) such as tropicamide, cocaine or hydroxyamphetamine. Besides than being an invasive method, the action of the solutions depends on the permeability of the ocular epithelium of each individual.

Thus, a better way to analyze the pupil behavior is through the recording of its movement during the PLR, using a method known as dynamic pupillometry [15].

2. State of art

Iris pattern has been proved virtually unique to each person, even between twins [20]. Its features also do not seem to change over the time [21], and the procedure used for a sample acquisition does not requires any kind of contact. These characteristics makes this biometrics to be considered one of the most secure [22]. However, it is also not a spoof-proof biometric recognition method [23].

To avoid frauds in iris recognition systems, there are methods to detect when a fake iris is presented to the system sensor. The use of the Fourier Transform, for example, is proposed to detect periodic features on printed iris patterns [8], but is not effective if the fake image resolution is high enough or the sample acquisition is defocused enough that it is not possible to distinguish a real iris pattern and a printed one [24]. The detection of specular reflection on the cornea, or the pupillary hippus [8], is also vulnerable to contact lenses or printed iris images with a hole through which a real pupil is visible [24]. Another proposal is to use the Purkinje images to detect fake irises [24], but this method also cannot deal with real eyes of dead people.

The use of human reflexes for identification is a recent proposal for the development of "spoof-proof" biometric systems [25], based on the idea that, even if some biometric information is leaked from the database, the dynamic nature of the features difficults their reproduction. Furthermore, for being automatic and involuntary responses, they cannot be trained, imitated, prevented or controlled, as occurs with other dynamic biometrics (handwritten signature, gait, keystroke dynamics) [17].

Based on this, Nishigaki and Arai [17] propose the use of information from the eyes saccade response and the blind spot position for user authentication. Tests with 10 subjects lead to results of 0% FAR and 0% FRR in the best case. The authors, however, warn that is still necessary to confirm the singularity and permanence of the blind spot position and the saccade response time. A practical use of this system would be void due to the complexity of the data acquisition setup.

Other relevant works that investigate the use of eye movements for biometric authentication have been presented by Kasprowski et al. [26], Bednarik et al. [27], Kinnunen et al. [28] and Komogortsev et al. [29]. However, only one of them [27] makes use of the pupil size as a feature. The method consists in keeping track of the person's eyes while he/she reads a text or looks at an image. Tests with 12 subjects lead to recognition accuracy of up to 90%.

Another approach that uses dynamic features of the iris and pupil for authentication is proposed by Costa & Gonzaga [30]. In that work, an acquisition system based on the consensual reflex of the pupil is used: while a video camera records the left eye in the absence of visible light, the right eye is illuminated in predefined periods. Using five features extracted from the videos (pupil dilation time, gray average level, correlation of gray levels and contrast in specific regions of the iris and time periods), 0.049% EER has been achieved for a database consisting of 555 videos regarding 111 individuals. However, no dark-adaptation step is mentioned, which means that these results could be high dependant on non-controlled conditions of the experiments. For each sample, the recording time is fixed in 14 s, being half of this without light stimulus and the other half with white illumination on the right eye.

3. Proposal

Considering the issues stated above, in this paper we propose the use of some Pupillary Light Reflex (PLR) dynamic features, together with the static features of the iris pattern, for a more reliable and secure biometric authentication system. A simple diagram of the system is shown in Fig. 1.