



ELSEVIER

Contents lists available at ScienceDirect

## Pattern Recognition Letters

journal homepage: [www.elsevier.com/locate/patrec](http://www.elsevier.com/locate/patrec)

## A low-cost and calibration-free gaze estimator for soft biometrics: An explorative study<sup>☆</sup>

Dario Cazzato<sup>a,\*</sup>, Andrea Evangelista<sup>a</sup>, Marco Leo<sup>b</sup>, Pierluigi Carcagnì<sup>b</sup>, Cosimo Distante<sup>b</sup>

<sup>a</sup> Faculty of Engineering, University of Salento, Lecce 73100, Italy

<sup>b</sup> National Research Council of Italy – Institute of Optics, Arnesano (LE) 73010, Italy

## ARTICLE INFO

Article history:  
Available online xxx

Keywords:  
Free gaze estimation  
Head pose estimation  
Pupil detection  
Soft-biometrics

## ABSTRACT

Soft biometric systems have spread among recent years, both for powering classical biometrics, as well as stand alone solutions with several application scopes ranging from digital signage to human-robot interaction. Among all, in the recent years emerged the possibility to consider as a soft biometrics also the temporal evolution of the human gaze and some recent works in the literature explored this exciting research line by using expensive and (perhaps) unsafe devices which require user cooperation to be calibrated. This work is instead the first attempt to perform biometric identification of individuals on the basis of data acquired by a low-cost, non-invasive, safe and calibration-free gaze estimation framework consisting of two main components conveniently combined and performing user's head pose estimation and eyes' pupil localization on data acquired by a RGB-D device. The experimental evidence of the feasibility of using the proposed framework as soft-biometrics is given on a set of users watching three benchmark heterogeneous videos in an unconstrained environment.

© 2015 Elsevier B.V. All rights reserved.

### 1. Introduction

Biometrics is the science of establishing the identity of an individual basing on physical, chemical or behavioral attributes of the person. In the literature, several features have been employed in order to achieve the recognition task, like palmprint [29], iris [42] or fingerprint [47], as well as DNA, face, retina and so on. Biometrics main purpose is to enhance the security and reliability of a system, ensuring that a provided service is accessed only by a legitimate user. Biometric-based security applications vary from ATM, like the work of [16], to server authentication [46] and to system accesses, like in the works of [28] and [39]. Another significant application field is the forensics, where biometrics have applications for terrorist identification and/or criminal investigation [31]. The diffusion of large-scale biometric systems in both commercial and government applications has increased the researchers' awareness of this technology. As a consequence of this rapid growth, also the challenges associated with designing and deploying biometric systems have been highlighted. Indeed, the problem of biometric recognition is a grand challenge in its own right [23]. Hard biometric systems raise many security and privacy issues, since they are based on personal, physiological and behavioral data that could be stolen and misused [8]. Moreover, they

need to process information that could not be always accessible, or available only by means of intrusive devices in order to obtain the required reliability and precision for the particular application context. In large-scale identification applications, due to the larger number of comparisons to be performed, these systems may not yet be extremely accurate [25]. Also noise in the data, intra-class variation and non-universality of the biometrics are source of errors. To improve reliability, different biometrics can be merged in the same solution: at this aim, the work of [21] formulates the problem of multiple biometrics, showing the potential improvement of multibiometrics. However, requirements of such solution increase in terms of computational needs, as well as the overall intrusiveness. At this purpose, the concept of soft biometrics has spread in the literature. [22] define soft biometrics as characteristics that provide some information about the individual, but such that they lack of the distinctiveness and permanence to sufficiently differentiate any two individuals. Examples of soft biometric estimations by computer vision algorithms are age estimation [18] or gender recognition [4], but also the race, the height, the color of the hair or the shape of the face are classified as soft biometrics. These features can be merged in an easier way to provide multiple label classification [20], or in such a way that a set of biometrics can enhance another estimation problem, like in the work of [40]. Due to the less intrusiveness and aptitude to be combined, soft biometric systems have spread among recent years in a wide range of application fields. [34] propose a review of soft biometrics usage in the context of video surveillance. Other application fields

<sup>☆</sup> This paper has been recommended for acceptance by Maria De Marsico.

\* Corresponding author. Tel.: +39 0832 321816; fax: +39 0832 420553.

E-mail address: [dario.cazzato@unisalento.it](mailto:dario.cazzato@unisalento.it), [dario.cazzato@ino.it](mailto:dario.cazzato@ino.it) (D. Cazzato).

are digital signage [12], human-robot interaction enhancement [10] and signature verification ([19]). Even age estimation for access control constitutes a soft biometric based system. In recent years, even law enforcement and online service providers are actively pursuing age-estimation technology in order to identify child pornography [6].

Even though soft biometrics cannot be used alone to distinguish individuals, in the literature soft and hard biometrics have been combined to strengthen the discriminative power of the system and/or to provide an alternative source of information that could be easily integrated in the identification process. This way, soft biometrics can be employed to preliminary narrow down the search on a database, decreasing the global required computational time [15]. At this purpose, [41] proposes soft biometrics to filter a large biometrics database, improving the speed and the search efficiency. The work of [51] exploits two fusion strategy to merge soft and hard biometrics information in order to improve identity verification. To mitigate the problem of not always feasible biometric traits, in [32], a new framework for continuous user authentication that fuses soft biometrical traits with two conventional authentication schemes, namely password and face biometric, is proposed. The work of [24] integrates faces, fingerprints and soft biometrics traits for user recognition, while [33] improve face image matching and retrieval performance by means of demographic information and facial marks. [2] combine soft biometrics traits as body weight and fat measurements with fingerprint. Finally, the work of [52] uses soft biometrics like age, gender and shape of the face to enhance performance of face verification.

Among well consolidated soft biometrics, the idea of gaze analysis as a personal distinctive feature has been also taken into account. The milestone of this research area is a series of works which make use of an head mounted eye tracker, based on the detection of infrared light reflection, to temporally analyze the eye movements during predefined stimuli. The final aims of the data analysis range from the evaluation of student behavioral skills [7] to the identification of users among a set of predefined ones [27], [17]. Instead of analyzing eye movement, more recently, [9] have proposed to consider the temporal evolution of the gaze direction as a soft-biometrics. The study was based on data acquired by a Tobii 1750<sup>1</sup> remote eye tracker that is expensive, it requires the user cooperation to achieve an initial calibration and it employs infrared light concentrated on the eye pupils whose safety is still under discussion (as demonstrate the recent updates of required standards for commercial devices). The work demonstrated that the gaze direction is able to distinguish among users but its real applicability is limited by its operating modes and hardware requirements. This paper tries to overcome these drawbacks by introducing a gaze estimation framework that works on visual data acquired from a remote low-cost depth sensor device that does not require any initial person dependent calibration. It allows the user to freely rotate the head in the field of view of the sensor and it is insensitive to the presence of eyeglasses, beard or hairstyle. Making use of the proposed framework the paper performs also a preliminary study about the possibility to use the temporal evolution of the gaze estimation outcomes as a soft biometric engine and this is achieved by qualitative and quantitative evaluation of data acquired for different users while watching three benchmark heterogeneous videos. Summing up, the paper introduces a twofold level of innovation: on the one side it introduces an innovative approach to estimate the human gaze and on the other side it represents, at the best of our knowledge, the first study about the possibility to use gaze tracks extracted without using specialized hardware for soft-biometrics purposes.

The rest of the paper is organized as follows: Section 2 introduces the proposed gaze estimation framework, Section 3 details how the experimental phases have been set up and finally the study about the

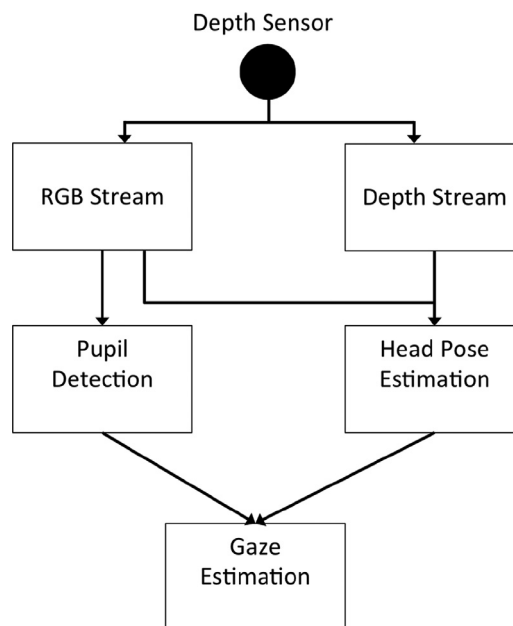


Fig. 1. A block diagram of the proposed solution.

evaluation of gaze tracks as soft-biometrics is presented in Section 4. Section 5 concludes the paper.

## 2. Proposed gaze estimation solution

The proposed gaze estimation method works on depth and RGB images extracted from commercial depth sensors e.g., Microsoft Kinect<sup>2</sup> and ASUS Xtion Pro Live<sup>3</sup>. The acquired data are processed by a multistep approach performing, at first, head pose estimation using both depth and RGB streams. The head pose estimation algorithm computes the exact position of the head with regards to the sensor, in terms of yaw, pitch and roll angles. Head pose information, integrated with the 3D positions of the user, can supply a rough estimation of the human gaze. In particular, it can be carried out by computing the intersection between the sensor plane and a straight line whose direction in the 3D space is defined by head pose angles [11]. Unfortunately, any gaze estimation that does not take into account the localization of the eye centers is highly inaccurate [37], especially for some kinds of application. For this reason the proposed approach, as a second step, computes pupil localization over the RGB data. This additional information is then used to improve the initial gaze estimation by means of the computation of a correction factor for the angles of the 3D model.

Fig. 1 shows an overview of the proposed solution whereas the following subsections describe in details each computational step.

### 2.1. Head pose estimation

In this step the detection of the human face and the estimation of its pose are performed: input data are RGB and depth streams, which are the inputs to the following algorithmic steps. First of all, face detection is performed on the RGB images by matching appearance with predetermined models. After the first detection, it is then possible to track the detected face over time, reducing this way the computational load needed to process the input streams. Detection of the characteristic points of the face and their temporal tracking

<sup>1</sup> <http://www.tobii.com/>.

<sup>2</sup> [www.microsoft.com/en-us/kinectforwindows/](http://www.microsoft.com/en-us/kinectforwindows/).

<sup>3</sup> [www.asus.com/Multimedia/](http://www.asus.com/Multimedia/).

Download English Version:

<https://daneshyari.com/en/article/4970318>

Download Persian Version:

<https://daneshyari.com/article/4970318>

[Daneshyari.com](https://daneshyari.com)