



THE 16TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

**Real-Time Iris Recognition of
Individuals – an Entrepreneurial Approach**

Cătălin Lupu¹, Corneliu-Octavian Turcu²

Abstract: Recognition of people by biometric characteristics has a long tradition, especially in the field of forensics. Among the main biometric features used so far can be listed: fingerprint, facial physiognomy, voice, etc. A new biometric feature used lately is the iris. It has many advantages over others, especially in terms of stability over time, being constant throughout life. However, given that it is necessary to take the features from a very small, moving object and from a considerable distance, most current systems have relied only on recognition after the iris only in a “static” and “fixed” way. An actual approach is real-time identification, especially given the increased performance of cameras. Real-time recognition of individuals can be used by entrepreneurs so that, after implementing the proposed methods, they can offer them for use to government institutions or other private partners.

Keywords: iris; biometric system; individuals’ recognition; real-time; entrepreneur

1. Introduction

Biometrics is a term derived from the Greek words *bios* (life) and *metrikos* (measure) and represents several automated methods used to identify a person using certain biometric features (palm geometry, fingerprint, iris, retina, face geometry, body weight, pressure blood, etc.) or behavioral (vocal timbre, DNA configuration, handwriting dynamics, signature scanning, keystroke dynamics, etc.), knowing that some of these biometric features, such as fingerprints or iris, or behavioral for example, the voice timbre, can uniquely identify a person. Given this uniqueness, biometric information can be used to design and implement technologies, equipment and systems designed to determine identity with performance far superior to existing ones (Bojamma & Nithya, 2013, pp. 153-160).

One of the best-known biometric features is the fingerprint, the British scientist Sir Francis Galton being the first to propose the use of fingerprints in order to identify since the nineteenth century. He developed a detailed study of fingerprints in which he also presented a classification system based on the fingerprints of all ten fingers, a system that is still the basis of identification schemes in use today. Fingerprinting has been introduced as a method of identifying of the persons in the British police since 1890 by Sir Richard Edward Henry.

In terms of information technology, biometrics is associated with technologies and techniques designed for security and identity confirmation based on individual and measurable biological characteristics of

¹ PhD, “Ștefan cel Mare” University of Suceava, Romania, Address: 13 Universitatii street, 720229, Suceava, Romania, Tel.: +40.230.216.147, Fax +40.230.520.080, Corresponding author: catalinl@eed.usv.ro.

² PhD, “Ștefan cel Mare” University of Suceava, Romania, Address: 13 Universitatii street, 720229, Suceava, Romania, Tel.: +40.230.216.147, Fax +40.230.520.080, E-mail: cturcu@eed.usv.ro.

the person. For example, fingerprints, hand geometry, face geometry, iris or retina fingerprint (code), voice timbre can be used in systems and schemes for access to a computer, in a certain room and, why not, to a banking account.

Automatic person identification is the process by which a biometric system associates a person with a specific identity, this can be done in terms of verification or identification. As part of the verification process, the system only authenticates a claimed identity; in other words, the system checks if a person is who they claim to be. In the identification, the complexity of the process increases, the system determining the person's identity by consulting a database or by testing a neural network with information about people, in other words, the system determines who the person is without specifying a name or other identifying information.

Designing a verification system is much simpler than an identity recognition system. A verification system authenticates the identity claimed by the person by comparing the particular biological traits provided by him at a given time with the measures of these traits previously stored in the system and associated with the identity claimed by the person; for example, the fingerprint of a person claiming to be Popescu is compared to the fingerprint of Popescu previously stored in a database or neural network of the system. Unlike the verification system, the identification or recognition system has a higher procedural complexity, the biometric features provided by a person being compared with the measures of all similar biometric features stored in a database or in a neural network. For example, the fingerprint of a person who wants access to a special purpose room is compared to the fingerprints of all the people allowed to enter that room. Another conclusive example is access to a personal car. There are anti-fraud systems used to protect against the theft of the car or the goods inside it. The system includes complex sensory systems (web-cam type) located inside / outside the car, and when someone wants to enter the vehicle, it is checked whether he has access to enter or not; people who have access to that vehicle have the iris code or fingerprint stored in a database; if the person has the code in the database, he is allowed to open the doors or start the engine, otherwise frames are sent to the Police, security companies or to the owner of the vehicle and can action in a timely manner.

Following the events in New York on 11 September 2001, the meaning of access control in the system has changed radically, both in terms of the means of exercise and the areas of application. In terms of means, the dominant discussion in the late 1990s was whether or not to introduce biometric identification systems, making the association with fingerprinting only to elucidate criminal cases. The strongest opposition came from the banking system, but not only. Other instruments seemed awkward or dangerous and, as such, were rejected in series. After that date, things changed radically in terms of biometric identification.

The fields of application have expanded, all coming from the strong conviction of system owners and administrators, thus highlighting other ways of verifying people who want access to most presidential, governmental and other public or private institutions, and airports have expanded their areas subject to special attention.

Information systems have not remained the same. Just the simple reference to what several important companies have achieved in terms of security is quite eloquent, because almost every movement of staff is under control, using its total dependence on special cards. It can be said that, in distributed data processing systems, but also in centralized ones, high-performance access control systems are required. It is said that “good security drives away bad danger”, which could highlight a good understanding of the threats to which a system is exposed, its vulnerabilities, but also the risks associated with it,

especially in terms of systems infrastructure, here resulting in a good identification of preventive measures to counteract them.

2. Applications of Biometrics

Establishing the identity of a person with great certainty has become decisive in a very large number of applications in our society today, characterized by unprecedented interconnection. Questions such as “Is that person exactly who they claim to be?”, “Is this person authorized to use this device or this facility?”, Are increasingly asked in different scenarios, such as when issuing a permit. driving in the United States or at the state border crossing. The need for very robust user authentication techniques is growing, given the important developments in the field of computer networks, communications and mobility. Thus, biometric technologies are increasingly incorporated into many applications. These applications can be divided into three main groups:

1. Commercial applications, such as network authentication, electronic data security, electronic commerce, Internet access, use of an ATM or bank card, access control, use of mobile phones, PDAs, medical records management, learning remote, etc.;
2. Government applications, such as the issuance of an identity card, the management of persons in a prison, the issuance of a driving license, control at the state border crossing, etc.;
3. Applications in forensics, such as identifying corpses, criminal investigations, determining parents based on DNA, etc.

3. Steps in Recognizing People Based on Iris Recognition

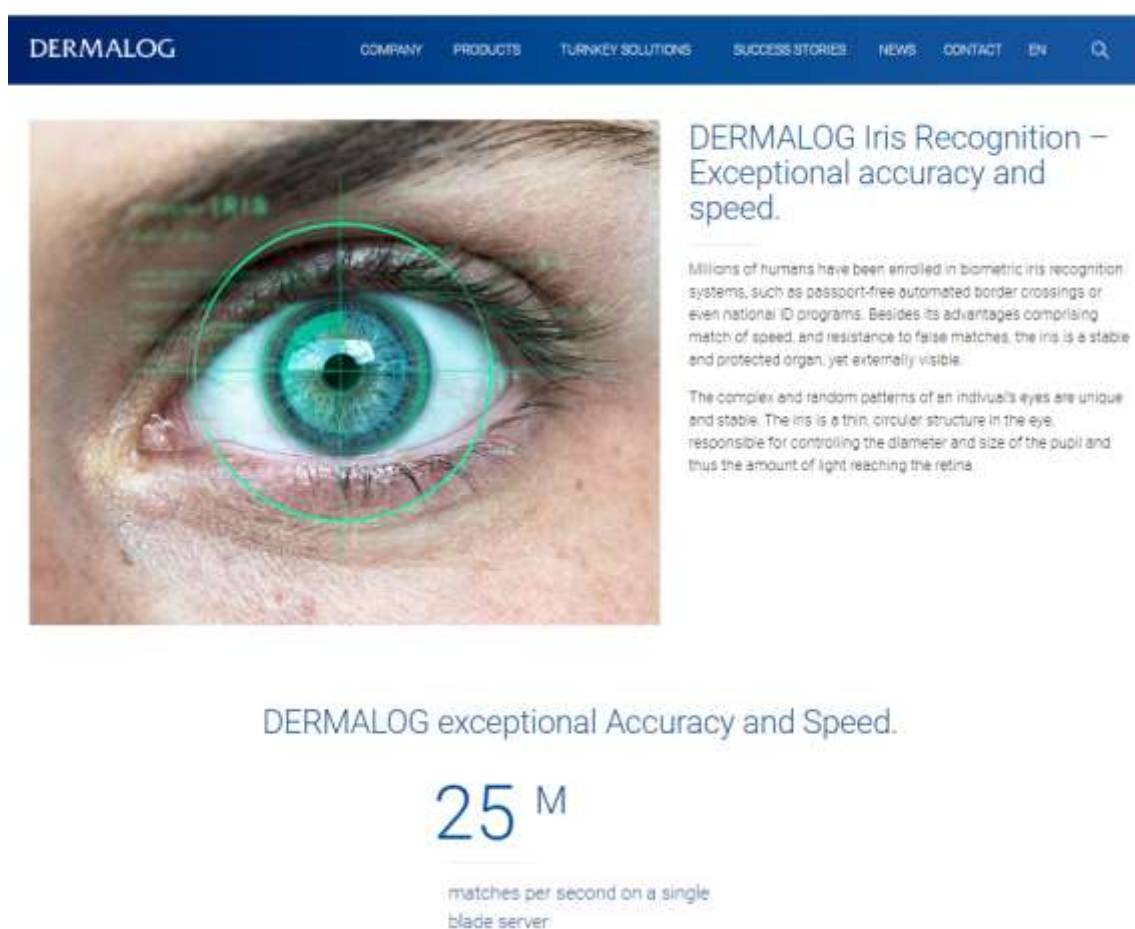
In the case of an iris recognition system, follow the steps below, in the order in which they are presented:

- taking the image from the camera for iris recognition, for example Panasonic BM-ET100US or UBKEY MirrorKem, or uploading it from a file (for example from iridescent databases such as CASIA (Chinese Academy of Sciences - Institute of Automation), MMU, UBIRIS, etc.);
- graphic processing, which aims to improve the image taken from the camera or file; it is done by applying various filters, by histogram equalization or by other methods of image processing;
- image segmentation - after obtaining a processed image with a maximum of useful information, it will be segmented, in order to obtain the center and radius of the pupil and iris;
- image normalization - after segmentation, the normalization of the iris region involves the framing of the circular region in a rectangle of constant size in order to be able to be compared with other existing templates in the database or in a neural network;
- coding - extracting the iris code for registration in a database or for recognition;
- inserting data in a database;
- match - in case of identification or verification it will be tried to determine if the presented image corresponds to any of the database, based on 1:1 comparison (in case of verification, when additional information about the user is provided - the question can be asked: Image X shown corresponds to user Y?) Or 1: N (in case of identification, when the whole database is queried to obtain data about the user related to the presented image - the question is Who is the

user who presented the image of the X iris?). In case of registration this matching module may be missing; however, a type 1: N check can be performed in the database to identify if the user is already registered, thus eliminating the possibility for a single user to use different credentials for authentication.

4. Liveness Approaches of Iris Recognition

There are several approaches to iris recognition without user cooperation. One of the most professional implementations is the German company DERMALOG's solution. The approach can be seen in Figure 1 (Iris Recognition - Software - Products - Dermatolog - The Biometrics Innovation Leader, 2021).



The image is a screenshot of the DERMALOG website. At the top, there is a dark blue navigation bar with the DERMALOG logo on the left and menu items: COMPANY, PRODUCTS, TURNKEY SOLUTIONS, SUCCESS STORIES, NEWS, CONTACT, EN, and a search icon. Below the navigation bar is a large image of a human eye with a green circular overlay and a vertical line through the pupil, representing iris recognition. To the right of the eye image, the text reads: "DERMALOG Iris Recognition – Exceptional accuracy and speed." Below this, there are two paragraphs of text. The first paragraph states: "Millions of humans have been enrolled in biometric iris recognition systems, such as passport-free automated border crossings or even national ID programs. Besides its advantages comprising match of speed, and resistance to false matches, the iris is a stable and protected organ, yet externally visible." The second paragraph states: "The complex and random patterns of an individual's eyes are unique and stable. The iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina." Below the eye image and text, there is a large number "25^M" with the text "matches per second on a single blade server" underneath it.

Figure 1. Dermalog's web-page

Real-time and liveness iris recognition has many applications in real life, especially in the field of identifying persons that wants to participate to a private event. Many other approaches will be studied during the postdoc stage.

5. Acknowledgement

This work is supported by the project ANTREPENORDOC, in the framework of Human Resources Development Operational Programme 2014-2020, financed from the European Social Fund under the contract number 36355/23.05.2019 HRD OP /380/6/13 – SMIS Code: 123847.

References

Bojamma, A. M.; Nithya B. & Prasad. C. N. (2013). An Overview of Biometric System. *International Journal of Computer Science Engineering and Information Technology Research (IJCEITR)*, pp. 153-160.

*** (2021). *Iris Recognition - Software - Products - Dermatolog - the Biometrics Innovation Leader*. <https://www.dermalog.com/products/software/iris-recognition>.