Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 7 (56) No. 1 - 2014

RECOGNITION OF A PERSON BASED ON THE CHARACTERISTICS OF THE IRIS AND RETINA

I. ARON[1] A. CTIN. MANEA[1]

Abstract: *Biometric solutions address the fundamental problems of recognizing a person based on features of the iris and the retina, because a person's biometric data are unique and cannot be transferred. Biometrics are automated methods of identifying a person or verifying the identity of a person based on morphological or behavioural characteristics. Examples of morphological characteristics include images of the hand, finger, facial features and recognition of the iris. Behavioural characteristics are traits that have been learned or acquired. Dynamic signature verification, speaker verification and the dynamics of pressure are examples of behavioural characteristics.*

Key words: *biometrics, biometric system, recognition of the individual, iris recognition, image of the retina.*

1. Introduction

Electronic security today is in a critical need to find the correct and safe alternatives which ought to be efficient from the financial perspective, to passwords and personal identification numbers (PIN) since yearly financial losses increase dramatically because of computer fraud as well as fraudulent accessing of computers and identity theft.

Biometric solutions address the fundamental problems of recognizing a person based on features of the iris and the retina, because a person's biometric data are unique and cannot be transferred. Biometrics are automated methods of identifying a person or verifying the identity of a person based on morphological or behavioural characteristics. Examples of morphological characteristics include images of the hand, finger, face and iris recognition features. Behavioural characteristics are traits that are learned or acquired.

Dynamic signature verification, speaker verification, and pressure dynamics are examples of behavioural characteristics.

The biometric system uses components of an electronic computer to capture the biometric information and examples of programs and operations belonging to a computer in order to maintain and manipulate the system.

In general, the system translates the measurements in a mathematical computer-readable format. When for the first time a customer creates a biometric

[1] Law Department, *Transilvania* University of Braşov.

profile, known as a template, that template is stored in a database.

The biometric system then compares this template with the new image created every time a customer accesses the system.

Biometrics provides data regarding values in two different ways.

First, a biometric component automates the access in a secure location, releasing or at least reducing the need for permanent monitoring by professional staff.

Secondly, when entering into a scheme of authentication, the biometer (measuring instrument of morphological or behavioural characteristics - voice, speech, signature) adds a high degree of verification for users and passwords. The biometer adds a unique identifier to the authentication network, one that is extremely difficult to duplicate.

Smart cards and data packs also provide a unique identifier, but the biometer has an advantage over such equipment as a user cannot lose or forget his/her fingerprint, retina or voice.

Practical applications of biometric systems target various domains: healthcare, financial services, transportation, public security and justice.

Such applications are online identifications for e-commerce, access control in a particular building or restricted area, offline staff identification, automatic machines for financial reading (ATM), the purchase of tickets through the Internet and access control in militarized areas, etc..

Using iris recognition, a person simply goes to the automatic device of iris recognition and looks into the sensor camera in order to access his/her accounts.

The camera instantaneously photographs the person's iris. If the information about the people's irises corresponds to the one stored in the database, then access is granted.

A positive log can be read through eyeglasses, contact lenses and most sunglasses.

It is important to distinguish whether a biometric system is used to verify or identify someone. These are separate purposes and certain biometric systems are more suitable for one than for the other, though no biometric system is limited to one or the other.

The requirements of the background will dictate what system is chosen. The most widely used by biometrics is verification.

As the name suggests, the biometric system verifies the user based on the information provided by the user. For example, when X enters his/her username and password, the biometric system introduces biometric data for X. If there is a match, the system checks whether the user is actually X.

Identification seeks to establish who the person is without gathering information from him/her.

For example, face recognition systems are commonly used for identification. A device captures an image of the person, of his/her face and looks for a match of this in its database.

Identification is complicated and intensive in terms of resources involved because the system must enable a far too complicated comparison of the images, rather than a 1:1 comparison achieved through a system check.

Iris scan biometrics considers the unique characteristics and features of the human iris in order to verify the identity of an individual.

The iris scanning process begins with a photograph taken with a special camera that uses infrared light to illuminate the eye and capture a very high resolution image.

This process takes only one or two seconds and provides details of the iris,

which are recorded and stored for future matching and verification.

Sunglasses and contact lenses do not affect image quality and iris scanning systems.

The inner margin of the iris is located by means of a scanning algorithm that highlights the different patterns and characteristics of the iris. An algorithm is a set of directives instructing the biometric system how to interpret a specific problem. Algorithms have a number of steps and are used by the biometric system to determine if a pattern (the first record), and a subsequent registration are the same.

The iris appears before birth and, except for accidents involving the eyeballs it remains unchanged throughout the life of the individual. It is extremely complex and has over 200 unique signs.

The fact that an individual's left eye is different from the right one and in terms of patterns irises are easy to capture, establishes iris scanning technology as one belonging to biometrics, this being highly resistant to false matches and fraud.

The acceptance rate of false matches in iris recognition systems is one in 1.2 million, statistically better than the average of the fingerprint recognition system. The real benefit lies in the high rate of false patterns rejection. Fingerprint scans have a false patterns rejection rate of 3 percent, while iris scanning systems boast rates at 0 percent.

Iris scanning technology has been tested in financial circles in England, USA, Japan and Germany since the beginning of 1997. In these pilot centres, the information regarding the client's iris becomes the verification tool for access to a bank account, eliminating the need to enter an identification number (PIN) by the client. When the client had his iris scanned and the identity verification was positive, access was granted to the bank account. These applications were successful because they eliminated the difficulties of forgetting the password or losing it.

Airports have begun to use iris scanning for registration, identification or verification of employees crossing secured areas and allowing access to airline passengers. This system allows a quick and easy verification of the identity of the people in order to be allowed access through the checkpoint.

Other applications include monitoring of transfers and releases of prisoners as well as other projects designed to authenticate purchases through the Internet, Internet banking, Internet voting and the purchase of shares on the internet, etc.

A high accuracy technology as iris scanning is a great success because it provides enhanced security.

2. Iris features

The iris has many features that can be used to distinguish an iris from the other.

One of the main features visible is represented by the network of the connective tissue strip that creates the appearance of radial division of the iris and is formed over 8 months of pregnancy.

During the development of the iris, the first seven months of pregnancy are crucial, because of the process of chaotic morphogenesis, it remains unique, which means that twins have different irises. The iris has 266 degrees of liberates (the number of patterns in the iris), which allows an iris to be different from another.

The fact that an iris is protected behind the eyelid considerably reduces the probability of an accident and / or scratches that cause changes.

Also, the iris never grows old which means that it remains in a stable form from the age of about one until death. The use of glasses or contact lenses (coloured or colourless) has a minimal effect on iris

representation and therefore does not affect identification technology.

From the above, we can conclude that the iris is characterized by a number of characteristics which allow the identification of the person, such as:

- uniqueness;
- immutability;
- cannot be counterfeited;
- diversity of varieties (patterns) of the iris;
- can not be influenced by the use of accessories - glasses, contact lenses.

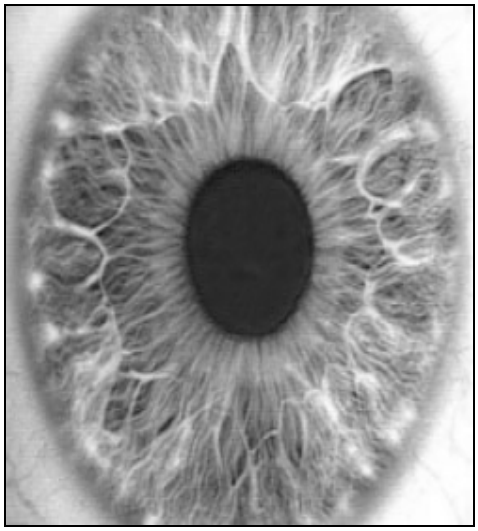

Fig.1. *The Iris*

Iris recognition is based on the following main visible features:

- the connective tissue that gives the appearance of dividing the iris in radial strips;
- circles;
- signs;
- freckles;
- crown.

It can be said that the iris has a code.

Expressed simply, iris recognition technology converts these visible characteristics in a sequence of codes with a length of 512 bytes for a model recorded with a view to attempt identification.

According to Dr. Daugman, the 11 mm diameter of the iris provides 3.4 bytes of information per square millimetre.

This density of information shows that each iris can have 266 "degrees of freedom" as it is quoted in most of the works in the literature on iris recognition.

A key point of the differentiation technology in iris scanning is the fact that the 512 bytes models for each iris facilitate a matching speed of over 500,000 models per second.

3. Biometric recognition system based on iris scanning

The iris identification process is performed using several systems. In general, the process of the iris identification system includes the following four steps:

1. Capturing the image;
2. Defining the location of the iris;
3. Optimizing the picture;
4. Storage and comparison of the image.

Iris image can be captured by a standard camera using both natural and infrared light and can be a manual or an automatic procedure.

The camera can be positioned at a distance of between 9 cm and one meter to capture the image.

In the manual procedure, the user must adjust the camera to frame the iris and should be at a distance of 15 cm to 30 cm from the camera.

This process is much more difficult when done manually and requires special training of the user in order to be successful.

The automatic procedure uses a set of cameras that automatically locates the face and iris.

Once the camera has located the eye, the iris recognition system then identifies the image that best illustrates the focus and clarity of the iris.

The image is then analyzed to identify the outer margins of the iris, where it meets the sclera, the pupil limit and the center of the eye pupil.

The recognition system then identifies the image areas of the iris that fit the extraction of the trait and analysis.

These involve the transfer areas that are covered by eyelids, any deep shadows.

Once the image was captured, such an algorithm should be used to filter and to designate segments of the iris into hundreds of vectors.

The algorithm should also take into account changes that may occur in an iris, pupil expansion or contraction due to the influence of light.

This information is used to produce a vector registration called Iris Code, which represents a record of 512 bytes which is then stored in a database for further comparison.

4. Retinal image

Retinal image consists in determining the appearance and size of blood vessels existing in the retina.

It is an extremely safe method of identification but it is the least used because of its invasiveness. The person must take off his/her glasses or contact lenses and to focus their gaze on a point so that the optical system of the eye lens does not change the focus of the optical reading system.

While the eye is held still, a low intensity infrared beam scans circularly the central area of the retina. The amount of reflected light, modulated by the reflectivity differences between blood vessels and the surrounding tissue is stored and represents the information that will be processed for identification.

The mathematical algorithm used for comparison transforms the size of the blood vessels into a numerical value, memorized as a barcode, their angular position being also recorded.

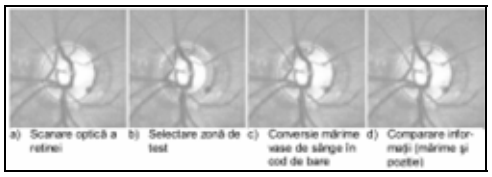

Fig.2. *The blood vessels on eye*

One of the greatest challenges of automated iris recognition system is to capture a high quality image of the iris while remaining non-invasive to the person whose iris image is captured. As iris is relatively small (an inch in diameter), dark, and the person is very sensitive when it comes to his/her eyes, careful handling is required.

In order to capture the iris image, the following should be considered:

- iris images must be acquired so that they have a high enough resolution and accuracy to be used in the recognition process;
- a good contrast of the iris without implying a level of light that disturbs the person;
- images should be well framed (centered);
- the distortions of the acquired image should be eliminated as much as possible.

Using eye image, the boundary between pupil and iris is detected after the eye position in the image given is located. Once the center and the radius are extracted, the right and the left radius of the iris are searched based on this data.

Using the center and the radius which are calculated in advance, the polar coordinate

system, out of which the characteristic of the iris is extracted, is established.

The extracted pattern of the iris is partitioned into prints in the form of a band. Each local area of these prints is transformed by means of a special cleaning 2D filter into a complex number. In fact, the sign of the real or imaginary part of the number converted is coded in 1 for a positive sign and 0 for a negative sign. The bytes thus obtained are compared with the bytes of all personal codes in the database or registered memory.

Finally, the system starts processing so as to recognize / identify the iris given by matching the score.

5. Multibiometric systems

There are systems that combine numerous unimodal biometric systems in an optimal manner. This concept increases the accuracy of the identification system and the resistance to counterfeiting, as all the characteristics should be counterfeit simultaneously. Of course, the combination of different systems should lead to improving the performance by introducing the combination of more items of information. The multibiometric system should not be understood as being obtained by putting together several systems, but through the creation of a complex system, able to use features of various systems, to select them and create linking elements between the uniqueness traits of the same individual.

In addition, for the development of a design of this comprehensive system, certain factors must be set such as:

- choosing and determining the number of biometric features - they are determined by the nature of the application and the correlations between traits. Some equipments make it easier to use an application that includes the combination of several features of the user, and others require the use of other combinations, such as face, voice and lip movement of an individual, the fingerprint and the face.
- the level at which information provided by multiple features will be integrated into the biometric system - at the level of extraction of the features, the sets of features specific to more identification ways are integrated, and from these, a new set of features is generated, which is used in performing the identification and in the modules for making the final decisions of the biometric system regarding a specific identity.
- the methodology of integrating information - the complexity of developing such a system determines that all multibiometric systems be based on a combination of no more than three unimodal systems. Some systems use, the face, the fingerprint and the hand geometry in combination, others use the face and the iris.

Proposals for improving the identification / verification of a person did not restrict to the multibiometric system. In July 2004, researchers from the Michigan State University proposed, in the International Conference on Biometric Authentication in Hong Kong, the completion of the multibiometric system with data - gender, age, height, weight, eye color, ethnicity, etc. These data are collected from each person once s/he uses biometric technology, a fact which was not yet determined in any of the biometric technology presentations. These data are called by the author "Soft Biometrics Trait" (SBT).

SBT are features that provide some information with a high degree of circumstantiation about a particular individual, but lacking distinctiveness and permanence to provide a sufficient differentiation of two individuals. SBT improves the performance of traditional biometric systems by introducing these

features for the selection of a wide database. Entries into the database will be limited to those subjects who fit the profile resulting from the filtration.

Experts underline the fact that multibiometric systems require a rather long time to verify a person's identity.

Therefore, the old anthropometric system of A. Bertillon is useful as a complementary element to a complex multibiometric system able to extract the information needed for identification, at the same time taking into account the limited accuracy of the first identification system.

Issues regarding the invasion of privacy and human civil rights continue to be made when resorting to a biometric identification system. The main doubt of the civil society concerns the opportunity of the biometric system, which could lead to an easier manner of identity theft.

Also, civil society raises the question of the excessive control of state authorities on the private life of individuals as well as the possibility of using personal data in activities against the democratic system in order to promote political, economic or ideological group interests. The opposition to the widespread use of the collection of data on individuals traveling to the U.S. was generated by some discriminatory accents in the use of biometric identification systems, users being selected, in some cases, simply based on belonging to non Caucasian races.

Beyond these doubts, partly substantiated, referring to biometric identification systems, we should note that the development of this type of identification has a major significance for the development of the forensic science, providing new investigative tools. Proper use of biometric identification systems can have a great impact on legal practice by improving forensic investigation of antisocial deeds and for finding out the truth, serving the purpose and the fulfilment of Forensic science.

6. The role and benefits of biometrics in access control

How can biometrics be integrated in access control applications?

What are the key elements that need to be taken into account when using a biometric device?

Biometrics identifies a person by means of a unique human characteristic: the shape and size of the hand, a fingerprint, the face or more features of the eye. If the purpose of an access control system is to control where certain people can go or not, then only a biometric device will be truly effective.

Consequently, biometrics is used at the main door of thousands of companies worldwide, the doors to the runways of major airports and the entrance into other areas where the combination between security and convenience is desirable.

More than 900 palm print readers control the customers' and employees' access in special areas of Italian banks and more than 100 units perform similar functions in Russia. In the UK, prisons are based on biometric systems to track prisoners and visitors.

Universities use palm readers for the meal program in campuses and in order to protect access to bedrooms and their own computer centers.

Hospitals use biometric devices to control the access and payroll accuracy.

Presently, there are biometric systems that meet the needs of almost all commercial applications for access control. And as costs continue to decrease, justification for the use of a biometric system has become a reality and a necessity for increasingly more organizations.

For many it is surprising that a frequent use of biometric access control is to be found in applications that require minimal security.

For example, health clubs are major users as biometric readers grant customers' access in the club in a simple way.

They need not have a club card and no longer have the problem of administering a system of cards.

This does not mean that high security issues are ignored - there are many well-known implementations. Since 1991, millions of check-ups have been made at the International Airport in San Francisco through biometric systems, some days reaching a peak of more than 50,000. Palmprint readers are scattered throughout the airport, providing more than 180 entries and verifying the identity of more than 18,000 employees. The use of biometrics at the San Francisco Airport is fully integrated into the primary access control.

References

1. Hong, L., Jain, A.K., Panke, S.: *Can Multibiometrics Improve Performance?* In: Proceedings AutolD'99, Summit, New Jersey, USA, 1999.
2. Lim, S., Lee, K., Byeon, O., et al.: *Efficient iris recognition through improvement of the feature vector and the classifier*. In: ETRI Journal, vol. 23, no.2, Daejeon, Korea, 2001.
3. Ma, Li, Wang, Y., Tan, T.: *Iris recognition based on multi-channel Gabor filters*. In: ACCV2002: 5th Asian Conference on Computer Vision, 23-25 January Melborne, Australia, 2002.
4. Onsy, A., Maha, S.: *A new algorithm to locate human iris margins*. In: The first IEEE International Symposium on signalling processes and information technology, 28 to 30 December, Cairo, Hilton Ramses Publishing House,2001.
5. Philips PJ, Martin A., et al.: *An Introduction to Evaluating Biometric Systems*. In: The National Academies Press, Washington, 2010.
6. Wildes, R.: *Iris recognition - a biometric engineering technology.* In: Procedures of the IEEE, vol 84 no.9, New York, 1997.
7. Williams, G.O.: *Iris recognition technology*. In: IEE magazine electronic and aerospace systems, Vol. 12, no.4, New York, 1996.