BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LIX No. 4/2007	17 - 26	Seria Tehnică

Biometrics – issues regarding automated system for identification of a person

Adrian Lorentz[*], Nicolae Paraschiv[*], Toader Melinte[**]

[*] Universitatea Petrol-Gaze din Ploieşti, Bd. Bucureşti 39, Ploieşti,
e-mail: alorentz@upg-ploieşti.ro
[**] S.C. SEEKTRON S.A PLOIESTI

Abstract

For centuries humanity has recognized that some physiological and/or behavioral traits (such as face or voice) are distinct from person to person, reason why these traits have been used in identification processes. There are archaeological evidences to demonstrate that individuality of fingerprint impressions were recognized by the ancient civilizations. Nowadays there are countries where a large segment of the population is illiterate (such as India) and thumbprint impression is considered a legal signature instead handwritten signature. This paper presents some aspects and results regarding the design of biometric systems, how does it work in conjunction with applications and legal/privacy issues.

Key words: *system, biometrics, security, automatic, recognition*

Introduction

It is widely accepted the fact that many physiological and/or behavioral traits are different from person to person, reason why this kind of characteristics can be used to distinguish between identities in identification and/or recognition processes.

The term "biometrics" comes from the Greek *bios* (life) and *metrikos* (measure) and denotes automatic methods/techniques for identifying a person using specific physiological (for example, fingerprint) and/or behavioral (for example, voice) characteristics of that person. Since there are many biological characteristics that can be collected and measured, biometrics captured the attention of scientific, governmental and commercial communities, interested by development and implementation of more reliable identification and recognition processes.

In an organized and systematic manner, biometrics started to be used in France at the beginning of the 19th century when Alphonse Bertillon, a police official of the police department in Paris, developed a method of identification based on a number of anthropometric measurements such as height, weight, color of eyes, feet length etc.; all these measurements were registered and then classified after head dimension.

One of the most studied biometric characteristic is the fingerprint. Even there are ancient evidences of fingerprinting, usage of fingerprint in a systematic manner for person identification was proposed at the end of the 19th century by the British scientist Sir Francis Galton; in the

same period of time, fingerprinting was introduced as method of person identification in British police by Sir Richard Edward Henry. Since the beginning of 1960s are commercially available automatic identification systems based on fingerprint, systems that have been used especially by the police and law enforcements in specific security applications.

For years, in computer and information technology were used many security techniques, schemes and mechanisms that satisfied specific identity verification/confirmation requirements in order to enable access of a person to a computer or to a room. Traditionally, they are based on something that person posses (a key, a badge with a photograph), or on something that person knows (a password, a personal identification number (PIN)). Disadvantages are obvious since keys or badges could be stolen, lost or destroyed, passwords and PINs could be forgotten, lost or, somehow, guessed.

Biometrics proposal to improve security in computer and information technology consist of using something that a person is. Characteristics like fingerprints, face, iris, retina, handprints, handwritten signature or voice that could be collected and processed, can be used in design and implementation of more reliable security systems.

Basics of biometric systems design

Understanding how a biometric system works needs knowledge regarding which anthropometric and/or behavioral human characteristics are adequate for person identification purposes.

An ideal characteristic should be [1]:

- universal – every person possesses it,
- unique – no two persons share exactly the same manifestation of the characteristic,
- permanent – the characteristic does not change and cannot be altered,
- collectable – a sensor can easily acquire the characteristic.

It is very hard (maybe even impossible) to identify a characteristic that satisfies all the above requirements. Even if it exists it might prove not usable for a biometric system in practice. Other aspects that need attention from a biometric system designer are accuracy, speed, performance and costs involved. Issues of great interest are raised by social factor, such as the level to which people accept a biometric identifier (acceptability), and the design process itself, such as how easy it is to fraud the system (circumvention).

For decades many biometrics are in use and many are in study: facial characteristics recognition (from still imagery, video sequences, 2 and 3D), fingerprints and handprints, hand geometry, iris and retinal recognition, handwritten signature, voice patterns, few of most commonly used being briefly presented in the following paragraphs.

A possible candidate to an ideal biometric characteristic is represented by deoxyribonucleic acid (DNA). Yet it is unusable for many applications because of invasive processes of acquisition of samples (body tissue, skin, blood, hair) that are not easy and widely accepted by people. Also, samples must be taken in extremely secured conditions because they are very sensitive and could be contaminated. Furthermore, there are needed expensive computational resources for processing.

Irrespective of the chosen biometric method first it is aquired a sample from the user. After acquisition, the sample is processed using different techniques and the result, known as *template*, is stored in a database for future use in identification/recognition processes.

Some of most commonly biometric characteristics currently in use are:

Facial Recognition

The most common biometric method is the face recognition which is done all the time in our daily lives to identify persons around us, reason why face recognition represents a very active domain of study.

Facial recognition represents a nonintrusive biometric method based on either: 1) the location, the shape and spatial relationships that can be constructed between specific facial features such as eyes, eyebrows, nose, lips and chin [2], or 2) the global analysis of image that represents a face and its decomposition into a number of component images.

Even if commercially available systems offer reasonable performance, there are still enough improvements to be done. A facial recognition system should be able to detect automatically the image of a face in a generic image, to detect the type and location of the face features, extract them and construct the spatial relations and then recognize it. Currently, available systems seem to have problems related with orientation, illumination, the large range of facial expressions and deformations from various reasons (aging, accidents).

Fingerprint Identification

Usage of fingerprints for personal identification is done for centuries but fingerprinting techniques are systematically used for criminal investigations for more than 100 years. Because of its history, large range of applications (laptop, mobile phones, cars etc.) and affordability, it is expected that fingerprinting to be the leading biometric method.

A fingerprint is represented by the pattern of ridges and furrows located on the surface of each finger (see Fig. 1). This pattern is different from finger to finger at the same person and even the fingerprints of identical twins are different.

Fig. 1 Fingerprint images acquired with different optical scanners

There are commercially available a large range of fingerprint readers that can provide the image of a fingerprint. Because fingerprints have traditionally been associated with criminal investigations one problem with fingerprint technology is acceptability. Another problem is that the fingerprints of a small fraction of the population may be inadequate for automatic identification because the prints may be deformed because of aging, genetic condition, environment, or the work (for example, a tailor it is expected to have a poor quality fingerprints).

Hand Geometry

Measurements of the human hand like shape, fingers length and width, overall size can be used as biometric features.

The technique of hand geometry is very simple, relatively easy to use, and inexpensive. A major disadvantage is that it can not be used with acceptable performance for identification of a person from a large population. Other problems are raised by limitations in dexterity caused by arthritis, variations caused by growth during childhood, presence of jewelry.

Retina

The vascular configuration of the retina is presumed a biometric characteristic unique. Because it is protected and it is not easy to replicate or change this vascular configuration, retinal recognition is one of the most reliable biometric.

The process of image acquisition is invasive and implies cooperation and acceptance of the user. Also, retinal recognition is expensive.

Iris

The iris is represented by the colored part of the eye that surrounds the pupil. Each iris is unique, and even irises of identical twins are different.

The complexity of iris structure recommends iris identification as a feasible and reliable biometric.

Design of a biometric system

Every previous biometric method has advantages and disadvantages and the choice that must be taken depends on the application.

There are two modes of operation for a biometric system: verification and recognition.

Verification (see Fig. 2) consists in comparison of the claimed identity and biometric data acquired from user with previously stored identity and biometric data associated.

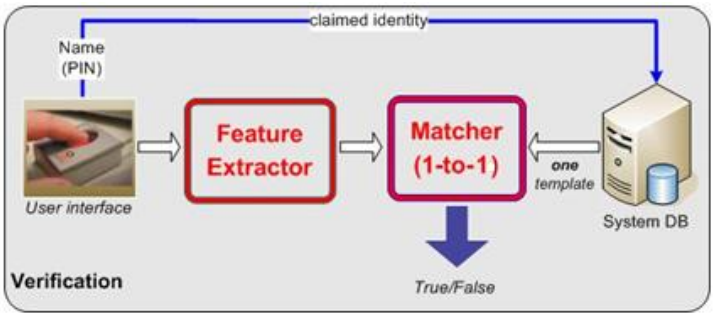

Fig. 2 Generic verification system

In recognition (see Fig. 3) the user doesn't provide any identity only a sample of biometric data. It is the job of the biometric system to say which identity is associated with that data. The biometric data being used is compared against the corresponding biometric data associated with all identities previously stored in the system. For this reason it is obvious that it is easier to design a biometric system for verification than for recognition.

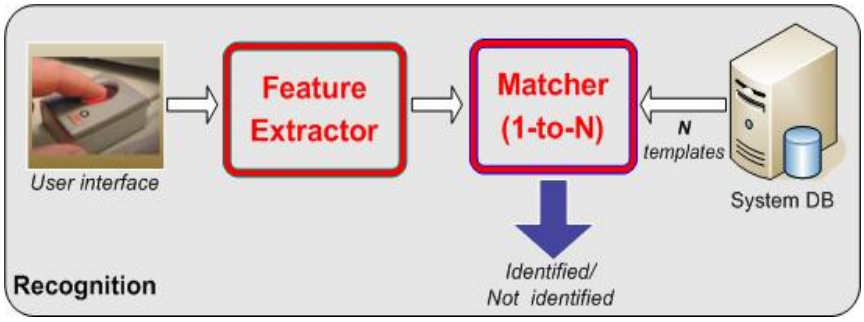

Fig. 3 Generic recognition system

Operational, a biometric system can be divided into the following distinct modules: an enrollment module, an identification module and a recognition module.

During enrollment (see Fig. 4), a biometric sensor scans the biometric feature presented by the user to acquire a digital representation of that feature, which is usually a digital image. This acquired image is processed by a computer program that generates a more compact representation called *template*. The template for each user is stored in the system's database or on a portable media such as a smartcard.

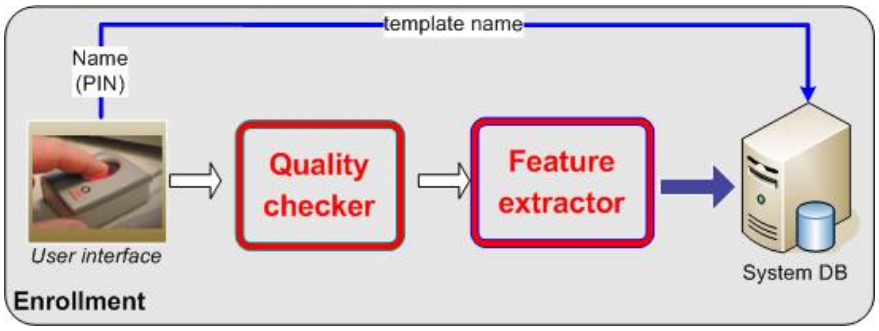

Fig. 4 Generic enrollment module

The job of identification module is to recognize the person. During identification, the biometric sensor scans the biometric characteristic presented by the user to be identified and process it in the same manner as during enrollment so the result has the same digital format as the template.

The template generated in the live scan process is then compared with a template stored in the system database using another computer program called *feature matcher*.

In case of verification the system will make only one comparison between the template generated when the biometric feature was presented by user and the template stored in the system database during enrollment and associated with the identity claimed by the user. If they are not the same, the user will be rejected, otherwise will be accepted.

In case of recognition the system will have to compare the template generated when the user presents the biometric characteristic against all the templates stored in the database. If the generated template does not match with any stored template, the person will be rejected as impostor, otherwise will be associated with the corresponding identity associated with the stored template.

The accuracy of a biometric system is questionable because of variations that are inherently present in any biometric characteristic. For example, a fingerprint might be changed from a presentation to another because of different pressure and surface scanned, so on. From this kind of reasons the system can establish an identity only with a certain level of accuracy.

As an example, assume that a person is a user of a verification system, the person claim that is *Ionescu* and is already enrolled in the system. The decision taken by the system will be either to

accept that the person is *Ionescu* or to reject the user as an impostor. In both cases the decision could be correct or incorrect, true or false respectively.

This way there are four possible outcomes: *true accept*, where a genuine user is accepted; *true reject*, where an impostor is rejected; *false accept*, where an impostor is accepted; and *false reject*, where a genuine user is rejected. True accept and true reject are correct, whereas false accept and false reject are incorrect.

The performance of a biometric system may be characterized by calculating how frequently are committed the errors of false acceptance and false rejection by the system. For this purpose are used by system designers and assessors two numbers: false acceptance rate (FAR) and false rejection rate (FRR). The FAR represents the probability with which the system accepts an impostor as a genuine user. The FRR represents the probability with which the system rejects a genuine user as an impostor.

A biometric system should have ideally extremely low values for both FAR and FRR. In practice, however, it has been proved that a smaller FRR usually means a larger FAR, while a smaller FAR usually means a larger FRR. These values have extremely importance in taking the decision regarding the operating mode of the system.

Choice of method – application and privacy issues

Every biometric technique presented has advantages and disadvantages and the choice of a particular method is strictly related to the domain of its application. For example, access to a very sensitive objective such as a nuclear facility might require a biometric system with an extremely low FAR of 0.001% (one impostor accepted from 100.000 attempts) and a low FRR of 0.1% (one valid user rejected in 1.000 attempts). In such case perhaps retinal or iris recognition would be preferable to voice, face or fingerprint recognition.

Biometrics represents a rapidly evolving and emerging technology that is widely used in law enforcement applications, most commonly being the identification of criminals and the access control in facilities and objectives. Also, there are many areas where biometrics can improve security outside of law enforcements, such as prevention of frauds in case of bank transactions.

Furthermore, there are countries that consider biometrics as alternative of identification of citizens or countries that already implement this kind of identification. Anyway, there are privacy concerns for citizens regarding how, and by whom, their biological and behavioral characteristics are used.

Other domains of applicability of biometrics could be (but not limited to) security for information and computer systems, computer networks, medicine.

Even until now biometric methods demonstrated some disadvantages it is obvious that they will have a great impact on our social life in the near future.

Conclusions

Biometric techniques seem to be the next step in order to improve the security of a wide range of applications related to identity verification and recognition, from commercial to law enforcement and criminal investigations.

A single biometric method cannot be considered as sufficient to implement a reliable identification so it is expected that the future to belong to multimodal biometric systems.

There are still to be conducted experiments and research to find out new representations and matching algorithms, fusion of biometrics, template protection, reliable and relevant testing

procedures and protocols; also, must be developed new and more rapid techniques for database indexing in conjunction with improvements to error rate estimation, so on.

References

[1] Maltoni, D., Dario, M., Jain, A., Prabhakar, S. – *Handbook of Fingerprint Recognition*, Springer, 2003
[2] S. Prabhakar, S. Pankanti, A.K. Jain – *Biometric Recognition: Security and Privacy Concerns*", IEEE Security & Privacy, March/April 2003, pp. 33-42

Metodele biometrice – aspecte privind sistemele automate de identificare a persoanei

Rezumat

Lucrarea prezintă unele aspecte privind metodele biometrice de identificare automată a persoanei. După o evidențiere a celor mai utilizate dintre aceste metode (recunoaşterea facială, amprenta digitală, recunoaşterea bazată pe retină şi iris) se prezintă modele generice ale modulelor esențiale dintr-un sistem automat de identificare: înregistrare, verificare şi recunoaştere. Totodată, sunt prezentate o serie de aspecte vizând proiectarea sistemelor automate de identiticare, modul de selecție a unei metode biometrice şi domeniile principale de aplicabilitate. Într-o manieră succintă sunt abordate şi o serie de probleme de natură juridică, privind protecția datelor cu caracter privat relativ la persoană şi intimitatea acesteia.