Biometric Security Technology

Marcos Faundez-Zanuy
Escola Universitària Politècnica de Mataró, Spain

INTRODUCTION

The word biometrics comes from the Greek words "bios" (life) and "metrikos" (measure). Strictly speaking, it refers to a science involving the statistical analysis of biological characteristics. Thus, we should refer to biometric recognition of people, as those security applications that analyze human characteristics for identity verification or identification. However, we will use the short term "biometrics" to refer to "biometric recognition of people".

Biometric recognition offers a promising approach for security applications, with some advantages over the classical methods, which depend on something you have (key, card, etc.), or something you know (password, **PIN**, etc.). A nice property of biometric traits is that they are based on something you are or something you do, so you do not need to remember anything neither to hold any token.

Authentication methods by means of biometrics are a particular portion of security systems, with a good number of advantages over classical methods. However, there are also drawbacks (see Table 1).

Depending on the application, one of the previous methods, or a combination of them, will be the most appropriate. This article describes the main issues to be known for decision making, when trying to adopt a biometric security technology solution.

MAIN FOCUS OF THE ARTICLE

This article presents an overview of the main topics related to biometric security technology, with the central purpose to provide a primer on this subject.

Biometrics can offer greater security and convenience than traditional methods for people recognition. Even if we do not want to replace a classic method

Table 1. Advantages and drawbacks of the three main authentication method approaches

Authentication method	Advantages	Drawbacks
Handheld tokens (card, ID, passport, etc.)	▪ A new one can be issued. ▪ It is quite standard, although moving to a different country, facility, etc.	▪ It can be stolen. ▪ A fake one can be issued. ▪ It can be shared. ▪ One person can be registered with different identities.
Knowledge based (password, PIN, etc.)	▪ It is a simple and economical method. ▪ If there are problems, it can be replaced by a new one quite easily.	▪ It can be guessed or cracked. ▪ Good passwords are difficult to remember. ▪ It can be shared. ▪ One person can be registered with different identities.
Biometrics	▪ It cannot be lost, forgotten, guessed, stolen, shared, etc. ▪ It is quite easy to check if one person has several identities. ▪ It can provide a greater degree of security than the other ones.	▪ In some cases a fake one can be issued. ▪ It is neither replaceable nor secret. ▪ If a person's biometric data is stolen, it is not possible to replace it.

(**password** or handheld token) by a biometric one, for sure, we are potential users of these systems, which will even be mandatory for new passport models. For this reason, it is useful to be familiarized with the possibilities of biometric security technology.

BIOMETRIC TRAITS

The first question is: Which characteristic can be used for biometric recognition? As common sense says, a good biometric trait must accomplish a set of properties. Mainly they are (Clarke, 1994), (Mansfield & Wayman, 2002):

- Universality: Every person should have the characteristic.
- Distinctiveness: Any two persons should be different enough to distinguish each other based on this characteristic.
- Permanence: the characteristic should be stable enough (with respect to the matching criterion) along time, different environment conditions, etc.
- Collectability: the characteristic should be acquirable and quantitatively measurable.
- Acceptability: people should be willing to accept the biometric system, and do not feel that it is annoying, invasive, etc.
- Performance: the identification accuracy and required time for a successful recognition must be reasonably good.
- Circumvention: the ability of fraudulent people and techniques to fool the biometric system should be negligible.

Biometric traits can be split into two main categories:

- Physiological biometrics: it is based on direct measurements of a part of the human body. Fingerprint (Maltoni et al., 2003), face, iris and hand-scan (Faundez-Zanuy, Navarro-Mérida, 2005) recognition belong to this group.
- Behavioral biometrics: it is based on measurements and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body. Signature (Faundez-Zanuy, 2005c) , gait, gesture and key stroking recognition belong to this group.

However, this classification is quite artificial. For instance, the speech signal (Faundez-Zanuy and Monte, 2005) depends on behavioral traits such as semantics, diction, pronunciation, idiosyncrasy, etc. (related to socio-economic status, education, place of birth, etc.) (Furui, 1989). However, it also depends on the speaker's physiology, such as the shape of the vocal tract. On the other hand, physiological traits are also influenced by user behavior, such as the manner in which a user presents a finger, looks at a camera, etc.

Verification and Identification

Biometric systems can be operated in two modes, named identification and verification. We will refer to recognition for the general case, when we do not want to differentiate between them. However, some authors consider recognition and identification synonymous.

- Identification: In this approach no identity is claimed from the user. The automatic system must determine who the user is. If he/ she belongs to a predefined set of known users, it is referred to as closed-set identification. However, for sure the set of users known (learnt) by the system is much smaller than the potential number of people that can attempt to enter. The more general situation where the system has to manage with users that perhaps are not modeled inside the database is referred to as open-set identification. Adding a "none-of-the-above" option to closed-set identification gives open-set identification. The system performance can be evaluated using an identification rate.
- Verification: In this approach the goal of the system is to determine whether the person is the one that claims to be. This implies that the user must provide an identity and the system just accepts or rejects the users according to a successful or unsuccessful verification. Sometimes this operation mode is named authentication or detection. The system performance can be evaluated using the False Acceptance Rate (FAR, those situations where an impostor is accepted) and the False Rejection Rate (FRR, those situations where a user is incorrectly rejected), also known in detection