Category: Bioinformatics

Biometric Authentication

Julien Mahier
ENSICAEN, France

Marc Pasquet
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Christophe Rosenberger
GREYC Laboratory (ENSICAEN – Université Caen Basse Normandie - CNRS), France

Félix Cuozzo
ENSICAEN, France

INTRODUCTION

For ages, humans recognized themselves according to different characteristics (appearance, behavior…). Biometrics is a well known technique to identify an individual or verify its identity; as, for example, fingerprints have been used for more than 100 years to identify one criminal. With computers, this analysis can be realized very quickly and with a higher reliability.

Biometrics has many applications: site monitoring (Bird, Masoud, Papanikolopoulos, & Isaacs, 2005), e-commerce (Jain & Pankanti, 2006)… The main benefits of biometrics are to provide better security and to facilitate the authentication process for a user. For example, it can be easy to obtain the password of a user, but it is more difficult to look like the user if a face recognition system is used for the user verification. Biometrics can also provide many advantages for particular applications. Indeed, biometric authentication can be realized in a contactless way that could be important for cultural aspects or reasons of hygiene. For all these motivations, biometrics is an emergent technology that could be more present in our daily life.

The goal of this chapter is to make an overview of biometrics. We focus on the authentication process, whose goal is to verify the identity of an individual. Ideal biometric information must have multiple properties:

- **Universality:** all individuals must be characterized by this information;
- **Uniqueness:** this information must as dissimilar as possible for two different persons;
- **Permanency:** it should be present during the whole life of an individual;
- **Collectability:** it can be measured (in a easy way);
- **Acceptability:** it concerns the possibility of a real use by users.

The plan of this chapter is given below. The background part presents the different biometric modalities studied in the research labs and used in real conditions. The main thrust of this chapter is an analysis of the benefits and limitations of biometric authentication. We present also the general architecture of a biometric system. Future trends stress the different research topics that should be treated to improve the biometric authentication. It concerns the combination of different biometric systems and their performance evaluation. We conclude by resuming the main aspects of this domain.

BACKGROUND

We detail, in this section, the different biometric modalities from the state of the art that can be used for the authentication process. Figure 1 illustrates the different types of biometric information. Biological analysis exploits some information that is present for any alive mammal (DNA, blood…). The behavioral analysis is specific to a human being and characterizes the way an individual makes some daily tasks (gait, talking…). Last, morphological analysis uses some information on how we look (for another individual or for a particular sensor).

Biological Analysis

As mentioned previously, biological biometric information can be extracted from any human being (see Figure 2). Generally, this information is not very easy to obtain. Some particular sensors are needed and the extraction of the biometric information can be quite long. For example, the DNA analysis with the most recent research techniques is possible in a few hours. We can cite the blood analysis that can only differentiate two individuals with different

Figure 1. Different biometric information in the state of the art

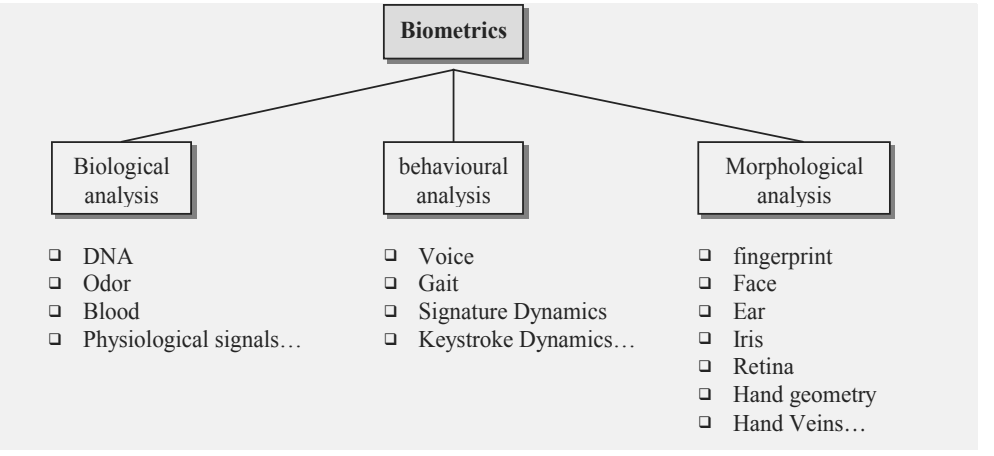
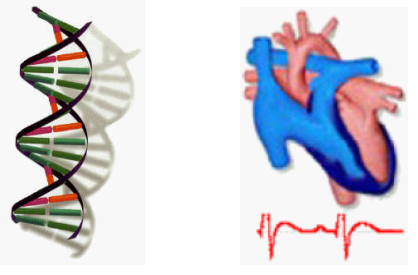


Figure 2. Some illustrations of the biological analysis (K. Phua et al., 2007)



Rhesus groups. We focus, in this chapter, on recent biological biometrics.

The electroencephalogram (brain signal) as a biometric information was studied in 1999 (Poulos, Rangoussi, Chrissikopoulos, & Evangelou, 1999). The EER value obtained by this approach is at the range of 16% to 28%. The odor as biometric information has also been tested (Korotkaya, 2003). This feasibility study showed the limitations of the actual sensors to use this information in a real context.

An industrial company proposed, in 2004, a biometric authentication solution based on dynamic electrophysiological characteristics of the living body, primarily of the beating heart (Idesia Ltd., 2004). Heart sound signals are also recently used for the authentication process (Phua et al., 2007). The biometric system comprises an electronic stethoscope, a computer equipped with a sound card, and the software application. This system provides a promising performance (EER equals to 4%).

Behavioral Analysis

We are able to recognize someone considering the way he/she walks or the way he/she types with a keyboard (see Figure 3).

An original biometric information has been recently proposed (Orozco, Asfaw, Shirmohammadi, Adler, El Saddik, 2006) using haptics devices. Results provide an EER near 10%, and open a new area of research. Individual recognition by considering its gait has also been studied (Man & Bhanu, 2006). The performance evaluation of this kind of approach puts into obviousness an average value of EER between 19% to 37%.

An individual can be recognized thanks to its voice. Voice verification has been treated by researchers for 50 years (Petrovska-Delacretaz, El Hannani, & Chollet, 2007). Many problems have to be solved, such as acquisition artifacts (ambient noise for example) or the variability of an individual's voice due to its stress or mood. The best results obtained by combining different methods give an EER near 5%, but the robustness of the authentication/identification is difficult to reach.

Many research works focus on keystroke analysis as authentication solution for controlling the access to a computer or a mobile phone. The major reason is that the knowledge of a password is often shared with many individuals. A recent work studied the feasibility of using keystroke authentication for mobile phones (Clarke & Furnell, 2007). The method, based on neural network classifiers, achieves promising results with an EER of 15.2%. A similar approach by using a computer keyboard provides better results (EER near 5%). The main advantage of this biometric modality is that no additional sensor is required.

Online signature verification is an interesting method because it is very common for a user. The signature shape is not really used in this context, but only the way it has been