Chapter 1
Privacy Enhancing Technologies in Biometrics

Patrizio Campisi
Università degli Studi Roma TRE, Italy

Emanuele Maiorana
Università degli Studi Roma TRE, Italy

Alessandro Neri
Università degli Studi Roma TRE, Italy

ABSTRACT

The wide diffusion of biometric based authentication systems, which has been witnessed in the last few years, has raised the need to protect both the security and the privacy of the employed biometric templates. In fact, unlike passwords or tokens, biometric traits cannot be revoked or reissued and, if compromised, they can disclose unique information about the user's identity. Moreover, since biometrics represent personal information, they can be used to acquire data which can be used to discriminate people because of religion, health, sex, gender, personal attitudes, and so forth. In this chapter, the privacy requirements, the major threats to privacy, and the best practices to employ in order to deploy privacy sympathetic systems, are discussed within the biometric framework. An overview of state of the art on privacy enhancing technologies, applied to biometric based authentication systems, is presented.

INTRODUCTION

In the recent past we have witnessed the rapid spreading of biometric technologies for automatic people authentication, due to the several inherent advantages they offer over classic methods. Biometrics can be defined as the analysis of physiological or behavioral people characteristics for automatic recognition purposes. Biometric authentication relies on who a person is or what a person does, in contrast with traditional authentication approaches, based on what a person knows (password) or what a person has (e.g. ID card, token) (Jain, 2004), (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Being based on

DOI: 10.4018/978-1-60566-836-9.ch001

strictly personal traits, biometric data cannot be forgotten or lost, and they are much more difficult to be stolen, copied or forged than traditional identifiers.

Loosely speaking, biometric systems are essentially pattern-recognition applications, performing verification or identification using features derived from biometric data like fingerprint, face, iris, retina, hand geometry, thermogram, DNA, ear shape, body odor, vein pattern, electrocardiogram, brain waves, etc. as physiological characteristics or signature, voice, handwriting, key stroke, gait, lip motion, etc. as behavioral characteristics.

Biometric authentication systems consist of two stages: the *enrollment* subsystem and the *authentication* subsystem. In the *enrollment* stage biometric measurements are collected from a subject, and checked for their quality. Relevant information is then extracted from the available data, and eventually stored in a database or in a personal card. The *authentication* process can be implemented in two different modes, depending on the desired application: in the *verification* mode, a subject claims his identity by showing some identifiers (ID, ATM card) and by supplying his biometric characteristics. Then the system compares the template extracted from the fresh biometrics with the stored ones. On the contrary, when the *identification* mode is selected, the whole database is searched through for matching between the stored templates and the samples acquired from the subject.

In the design process of a biometric based authentication system, different issues, strictly related to the specific application under analysis, must be taken into account. As well established in literature, from an ideal point of view, biometrics should be universal (each person should possess the characteristic), unique (for a given biometrics, different persons should have different characteristics), permanent (biometrics should be stable with respect to time variation), collectable (biometrics should be measurable with enough precision by means of sensors usable in real life), acceptable (no cultural, moral, ethical, etc. concerns should arise in the user the biometric characteristic is acquired). Moreover, besides the choice of the biometrics to employ, many other issues must be considered in the design stage (Jain, 2004). Specifically, the system accuracy can be estimated using the error rates representing the probability of authenticating an impostor, namely the False Accept Rate (FAR), and the probability of rejecting a genuine user, namely the False Rejection Rate (FRR).

The computational speed, which is related to the time necessary to the system to take a decision, is also an important design parameter, especially for those systems intended for large populations. Moreover, the system should be able to manage the exceptions which can occur when a user does not have the biometrics, namely the Failure to Acquire, when a user cannot be enrolled because of technology limitations or procedural problems, namely the Failure to Enroll, or when, beside technology limitations or procedural problems, the user does not enroll or cannot use the biometric system, namely the Failure to Use. System cost has also to be taken into account. It comprises several factors like the cost of all the components of the authentication system, of system maintenance, of operators training, and of exception handling.

Besides all the aforementioned requirements, the use of biometric data rises many security concerns (CESG UK Biometric Working Group, 2003), (Roberts, 2007), (Adler, 2008), not affecting other methods employed for automatic people recognition. In a scenario where biometrics can be used to grant physical or logical access, security issues regarding the whole biometric system become of paramount importance. In (CESG UK Biometric Working Group, 2003), (Roberts, 2007), (Adler, 2008) the main security concerns related to the use of a biometric based authentication system are highlighted: is it possible to understand when a system becomes insecure? Which action should be taken when a system is violated? Can biometrics be repudiated? Can biometrics be stolen? The main threats to a biometric system can