Chapter 2
Overview of Biometrics and Biometrics Systems

ABSTRACT

Recent security threats increase the necessity to establish the identity of every person. Biometric authentication is a solution to person authentication by analyzing physiological or behavioral characteristics. In this chapter, various biometric notions and terms are reviewed, along with typical biometric system components and different functionalities and performance parameters. The design and development of a biometric system, depending on a particular application scenario, is covered. This chapter also focuses on the inherent issues associated with biometric data and system performance through introducing radically new methods based on intelligent information fusion and intelligent pattern recognition, thus creating a notion of intelligent security systems. At the end of the chapter, the potential drawbacks of biometric unimodal systems, which serves as the motivation to introduce the concept of multimodal biometric system in the context of intelligent security systems, is discussed.

1. INTRODUCTION

Controlling access to prohibited areas and protecting important government and civilian objects are among the main activities of national and international security organizations. Similarly, with the advancement of large-scale networks (e.g., social networks, e-commerce, e-learning) and the growing concern for identity theft problems, the design of appropriate personal authentication systems is becoming more and more important. Usually, person authentication for access control to a prohibited area or for identification in different networks or social services scenarios (e.g.,

DOI: 10.4018/978-1-4666-3646-0.ch002

banking, welfare disbursement, immigration policies, etc.) is done using biometric authentication. According to Ratha et al. (Ratha, Senior, & Bolle, 2001), "Biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics." Over the last decades, people are using biometric authentication system in lieu of password or token based authentication systems for properties such as uniqueness, permanence over time, universality, user acceptance, and ease of use (Jain, Boelle, & Pankanti, 1999).

2. BIOMETRIC IDENTIFIERS

Biometric authentication offers a natural and reliable solution to the problem of establishing identity of a person utilizing his/her physiological or behavioural biometric characteristics or identifiers (Jain, Flynn, & Ross, 2007). The term "biometry" literally means "life science," and focused on studying biometric identifiers. These biometric identifiers, also called biometric traits, are integral part of a person's identity (Bolle, Connell, Pankanti, Ratha, & Senior, 2004). Some of the *physiological* characteristics that are now used for biometric recognition include face, fingerprint, hand-geometry, ear, iris, retina, DNA, palmprint, hand vein, etc. Voice, gait, signature, keystroke dynamics are examples of *behavioral* characteristics used for biometric recognition. *Soft biometrics* emerged as a new group of biometric gaining more and more attention. It includes measurements related to person's height, race, age, and gender. Finally, we identify one more group: *social* biometrics, making its way into the state-of-the-art security systems. This group includes data obtained from observing social behavior of the subject, interests, social network connections, work and leisure patterns, hobbies, and communication over social media.

2.1. Physiological Identifiers

Physiological biometrics are based on the body measurements, where a basic method to obtain the data is direct measurement of a part of the human body (Biometrics, 2009). Generally, it is assumed that physiological biometric identifiers are more stables than behavioral identifiers because most physiological identifiers remain unchanged over the course of individual's lifetime and do not depend significantly on external factors (Kung, Mak, & Lin, 2005). Face, fingerprint, and iris are the most commonly used physiological identifiers in today's automatic authentication systems. The other physiological biometric identifiers include retina, DNA, hand-geometry, ear shape, palmprint, hand, vein, teeth. Figure 1 shows some of the physiological biometric identifiers used for person authentication.

Face: Face is the most widely used biometric identifier to conduct human authentication. It is used every day by nearly everyone as the primary means for recognizing other humans. Among all the biometric traits, face is the most common and heavily used biometric for person identification. Face recognition is friendly and non-invasive (Feng, Dong, Hu, & Zhang, 2004).

The advantages of facial recognition include high public acceptance of the modality, commonly available sensors, not physically intrusive nature, and the ease with which humans can verify the results of security system based on facial biometric (Wilson, 2010).

Challenges in the face recognition process include different illumination conditions and backgrounds, changes in the facial expressions, aging, camouflage, and occlusions of some facial features (Singh, 2008). These challenges may reduce the overall recognition accuracy if not properly addressed.

Fingerprint: Fingerprint is one of the first biometric identifiers being used for recognition of one's belongings. Merchants in ancient times