Biometric Technologies

Yingzi (Eliza) Du
Indiana University, Purdue University, USA

INTRODUCTION

Biometrics is an emerging technology for automatic human identification and verification using unique biological traits (Woodward, Orlans, & Higgins, 2002). These traits include face, fingerprints, iris, voice, hand geometry, handwriting, retina, and veins. For example, fingerprint recognition analyzes ridge ends, bifurcation, or dots of finger tips; voice recognition analyzes speech signal characteristics; iris recognition analyzes the pits, striations, filaments, rings, dark spots, and freckles of eyes; and face recognition analyzes facial parameters (Du *et al.*, 2004). It is based on "something you are" rather than "something you have" (Du, 2005). Compared to the traditional identification and verification ways, such as user name/password, and paper IDs, biometrics is more convenient to use, reduces fraud, and is more secure (Reid, 2004).

BACKGROUND

Biometrics has been widely used in criminal justice; U.S. immigration and naturalization services; and e-commerce and e-government. For example, fingerprints have long been used to identify criminals. The Department of Homeland Security (2004) has deployed the US-VISIT Program for border security, which uses biometric technologies to help secure the nation's borders and expedite the entry/exit process while enhancing the integrity of the immigration system and respecting the privacy of the visitors. Biometrics has been used to replace the user name and password in e-commerce and e-government for information access.

BIOMETRICS SYSTEM

Biometric system usually includes two subsystems: (1) the biometric enrollment system (Figure 1a) and (2) biometric matching system (Figure 1b).

The biometric enrollment system includes the Sensor Module, the Data Acquisition Module, the Data Preprocessing Module, the Pattern Analysis Module, the Pattern Extraction Module, and the Biometric Database Module. And the Data Acquisition Module interprets the biometric data into digital signals (images). The Data Preprocessing Module processes these signals to reduce the noise. The Pattern Analysis Module finds the most distinctive patterns of the biometric traits. The Pattern Extraction Module picks these distinctive patterns and generates identifiable templates. These templates will be then saved in the biometric database.

Compared to the biometric enrollment system, the biometric matching system adds the Pattern Matching Module and the Decision Module. In the biometric matching system, the newly sensed biometric data will be first processed similarly as the enrollment data, and the system will generate the pattern templates from the data. The Pattern Matching Module compares the newly generated templates with those in the biometric database and calculates match scores or quality scores for final decision. If the matching score is higher than the predetermined threshold, the system identifies/verifies it.

The false acceptance rate (FAR) and the false rejection rate (FRR) are used to measure if the biometric system is reliable (Ratha, Connell, & Bolle, 2001). A biometric system that generates high scores of either FAR or FRR is not reliable and cannot be used.

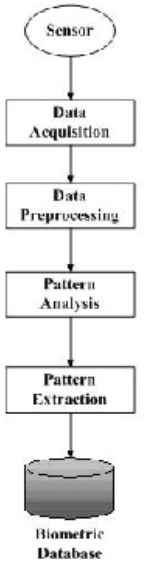
The FAR measures the percentage of incorrect identification:

$$FAR(\%) = \frac{\text{Number of false acceptance}}{\text{Total number of acceptance by the system}} \times 100\% \cdot \quad (1)$$

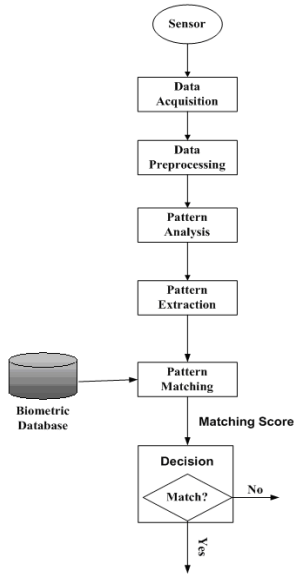
The FRR measures the percentage of incorrect rejection:

$$FRR(\%) = \frac{\text{Number of false rejections}}{\text{Total number of rejections by the system}} \times 100\% \cdot \quad (2)$$

Figure 1. Biometrics system



(a) Biometric Enrollment System



(b) Biometric Matching System

BIOMETRICS TECHNOLOGIES

Currently, the common used biometric systems include fingerprint, iris, face, and voice. The following paragraphs briefly describe each biometrics technology.

Fingerprint Recognition

Fingerprints have been extensively used in modern law enforcement. Fingerprint recognition is a well established and accepted method for person identification. Every person has minute raised ridges, which display a number of characteristics known as minutiae (Figure 2). The minutiae do not change naturally during a person's life (Pankanti, Prabhakar, & Jain, 2002). Fingerprint recognition systems usually extract information about the location, type, and direction of significant minutiae and generate templates for matching.

There are three types of fingerprint recognition systems to acquire digital fingerprint images:

- **Optical sensors.** The optical fingerprint devices can generate very high resolution images and are often used by law enforcement and gate/door access. However, this kind of sensor is sensitive to the dirt and grease that may be on the finger.
- **Solid-state sensors.** Using integrated circuit (IC) to generate the image of the fingerprint. This kind of sensor is more cost efficient and easy to be integrated with other devices. But the image quality is not very high.
- **Ultrasound sensors.** An ultrasound camera is used to acquire images from the finger. This approach allows distinguishing between real fingers and any imitations. Furthermore, it is not sensitive to any dirt, grease, and so forth. However, this kind of fingerprint system is very expensive and not ready for mass-market application yet.

Figure 2. Fingerprint in detail

Iris Recognition

The iris is the round, pigmented tissue that lies behind the cornea (Figure 3). Compared to other kinds of biometric systems, such as face recognition and fingerprint recognition systems, iris recognition is more reliable and can achieve a higher accuracy rate.