Biometrics

Richa Singh
West Virginia University, USA

Mayank Vatsa
West Virginia University, USA

Phalguni Gupta
Indian Institute of Technology, India

INTRODUCTION

The modern information age gives rise to various challenges, such as organization of society and its security. In the context of organization of society, *security* has become an important challenge. Because of the increased importance of security and organization, identification and authentication methods have developed into a key technology in various areas, such as entrance control in buildings, access control for automatic teller machines, or in the prominent field of criminal investigation.

Identity verification techniques such as keys, cards, passwords, and PIN are widely used security applications. However, passwords or keys may often be forgotten, disclosed, changed, or stolen. Biometrics is an identity verification technique which is being used nowadays and is more reliable, compared to traditional techniques. Biometrics means "life measurement," but here, the term is associated with the unique characteristics of an individual. Biometrics is thus defined as the "automated methods of identifying or authenticating the identity of a living person, based on physiological or behavioral characteristics." Physiological characteristics include features such as face, fingerprint, and iris. Behavioral characteristics include signature, gait, and voice. This method of identity verification is preferred over traditional passwords and PIN-based methods for various reasons, such as (Jain, Bolle, & Pankanti, 1999; Jain, Ross, & Prabhakar, 2004):

- The person to be identified is required to be physically present for the identity verification.
- Identification based on biometric techniques obviates the need to remember a password or carry a token.
- It cannot be misplaced or forgotten.

Biometrics is essentially a multi-disciplinary area of research, which includes fields like pattern recognition image processing, computer vision, soft computing, and artificial intelligence. For example, face image is captured by a digital camera, which is preprocessed using image enhancement algorithms, and then facial information is extracted and matched. During this process, image processing techniques are used to enhance the face image and pattern recognition, and soft computing techniques are used to extract and match facial features. A biometric system can be either an identification system or a verification (authentication) system, depending on the application. Identification and verification are defined as (Jain et al., 1999, 2004; Ross, Nandakumar, & Jain, 2006):

- **Identification–One to Many:** Identification involves determining a person's identity by searching through the database for a match. For example, identification is performed in a watch list to find if the query image matches with any of the images in the watch list.
- **Verification–One to One:** Verification involves determining if the identity which the person is claiming is correct or not. Examples of verification include access to an ATM, it can be obtained by matching the features of the individual with the features of the claimed identity in the database. It is not required to perform match with complete database.

In this article, we present an overview of the biometric systems and different types of biometric modalities. The next section describes various components of biometric systems, and the third section briefly describes the characteristics of biometric systems. The fourth section provides an overview of different unimodal and

multimodal biometric systems. In the fifth section, we have discussed different measures used to evaluate the performance of biometric systems. Finally, we discuss research issues and future directions of biometrics in the last section.

COMPONENTS OF BIOMETRIC SYSTEM

Biometric authentication is performed by matching the biometric features of an enrolled individual with the features of the query subject. Different stages of a biometric system are: capture, enhancement, feature extraction, and matching. During capture, raw biometric data is captured by a suitable device, such as a fingerprint scanner or a camera. Enhancement includes processing the raw data to enhance the quality of the data for correct feature extraction. Enhancement is specially required when the quality of the raw data is poor—for example, if the face image is blurry or contains noise. The raw data contains lots of redundant information which is not useful for recognition. Feature extraction involves extracting invariant features from the raw data and generating biometric template which is unique for every individual and can be used for recognition. Finally, the matching stage involves matching two features or templates. The template stored in the database is matched with the query template.

CHARACTERISTICS OF BIOMETRIC SYSTEMS

Every biometric modality should have the following properties (Jain, Hong, Pankanti, & Bolle, 1997; Jain et al., 1999, 2004; Maltoni, Maio, Jain, & Prabhakar, 2004; Wayman, Jain, Maltoni, & Maio, 2005):

- **Universality.** Everyone must have the attribute. The attribute must be one that is universal and seldom lost to accident or disease.
- **Invariance of properties.** It should be unchanged over a long period of time. The attribute should not be subject to significant differences based on age, or either episodic or chronic disease.
- **Measurability.** The properties should be suitable for capture without waiting time, and it must be easy to gather the attribute data passively.
- **Singularity.** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique, assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
- **Acceptance.** The biometric data should be captured in a way acceptable to a large percentage of the population. The modalities which involve invasive technologies for data capture, such as technologies which require a part of the human body to be taken, or which (apparently) impair the human body are excluded.
- **Reducibility.** The captured data should be capable of being reduced to a file which is easy to handle.
- **Reliability and tamper-resistant.** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- **Privacy.** The process should not violate the privacy of the person.
- **Comparable.** The attribute should be reducible to a state in which it can be digitally compared to others. The less probabilistic the matching involved, the more authoritative the identification.
- **Inimitable.** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

TYPES OF BIOMETRIC SYSTEMS

There are two types of biometric systems: unimodal and multimodal. Unimodal biometric systems use only one characteristic or feature for recognition, such as face recognition, fingerprint recognition, and iris recognition. Multimodal biometric systems typically use multiple information obtained from one biometric modality—for example, minutiae and pores obtained from a single fingerprint image, or information obtained from more than one biometric modality, such as fusing information from face and fingerprint.