

## **Biometrics:**

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- (i) the person to be identified is required to be physically present at the point-of-identification;
- (ii) identification based on biometric techniques obviates the need to remember a password or carry a token.

With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric based systems of identification are receiving considerable interest. Various types of biometric systems are being used for real-time identification, the most popular are based on face, iris and fingerprint matching. However, there are other biometric systems that utilize retinal scan, speech, signatures and hand geometry.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

## **Verification vs Identification:**

There are two different ways to resolve a person's identity: verification and identification. Verification (*Am I whom I claim I am?*) involves confirming or denying a person's *claimed identity*. In identification, one has to establish a person's identity (*Who am I?*). Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system.

## **Applications:**

Biometrics is a rapidly evolving technology which has been widely used in forensics such as criminal identification and prison security. Recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication in a large number of civilian applications. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with key-less entry and key-less ignition. Due to increased security threats, many countries have started using biometrics for border control and national ID cards.

## **Fingerprint Matching:**

Among all the biometric techniques, fingerprint-based identification is the oldest method, which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

## **Fingerprint Classification:**

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database (FBI database contains approximately 70 million fingerprints!). To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database.

## Biometric Systems

A *biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode:

- In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "*Does this biometric data belong to Bob?*"). Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity.
- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "*Whose biometric data is this?*"). Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities . Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.