Biometrics - Overview

The term Biometrics is composed of two words − *Bio* (Greek word for Life) and *Metrics* (Measurements). Biometrics is a branch of information technology that aims towards establishing one's identity based on personal traits.

Biometrics is presently a buzzword in the domain of information security as it provides high degree of accuracy in identifying an individual.

What is Biometrics?

> Biometrics is a technology used to identify, analyze, and measure an individual's physical and behavioral characteristics.

Each human being is unique in terms of characteristics, which make him or her different from all others. The physical attributes such as finger prints, color of iris, color of hair, hand geometry, and behavioral characteristics such as tone and accent of speech, signature, or the way of typing keys of computer keyboard etc., make a person stand separate from the rest.

This uniqueness of a person is then used by the biometric systems to −

- Identify and verify a person.
- Authenticate a person to give appropriate rights of system operations.
- Keep the system safe from unethical handling.

What is a Biometric System?

> A biometric system is a technology which takes an individual's physiological, behavioral, or both traits as input, analyzes it, and identifies the individual as a genuine or malicious user.

Evolution of Biometrics

The idea of biometrics was present since few years from now. In 14^{th} century, China practiced taking finger prints of merchants and their children to separate them from all others. Fingerprinting is still used today.

- In the 19^{th} century, an Anthropologist named **Alphonse Bertillion** developed a method (named *Bertillionage*) of taking body measurements of persons to identify them. He had

realized that even if some features of human body are changed, such as length of hair, weight, etc., some physical traits of body remain unchanged, such as length of fingers. This method diminished quickly as it was found that the persons with same body measurements alone can be falsely taken as one. Subsequently, Richard Edward Henry from Scotland Yard developed a method for fingerprinting.

- The idea of retinal identification was conceived by Dr. Carleton Simon and Dr. Isadore Goldstein in 1935. In 1976, a research and development effort was put in at EyeDentify Inc. The first commercial retina scanning system was made available in 1981.
- Iris recognition was invented by John Daugman in 1993 at Cambridge University.
- In 2001, Biometrics Automated Toolset (BAT) was introduced in Kosovo, which provided a concrete identification means.

Today, biometric has come up as an independent field of study with precise technologies of establishing personal identities.

Why Biometrics is Required?

With increasing use of Information Technology in the field of banking, science, medication, etc., there is an immense need to protect the systems and data from unauthorized users.

Biometrics is used for **authenticating** and **authorizing** a person. Though these terms are often coupled; they mean different.

Authentication (Identification)

This process tries to find out answer of question, “Are you the same who you are claiming to be?”, or, “Do I know you?” This is one-to-many matching and comparison of a person’s biometrics with the whole database.

Verification

This is the one-to-one process of matching where live sample entered by the candidate is compared with a previously stored template in the database. If both are matching with more than 70% agreeable similarity, then the verification is successful.

Authorization

It is the process of assigning access rights to the authenticated or verified users. It tries to find out the answer for the question, “Are you eligible to have certain rights to access this resource?”

Shortcomings of Conventional Security Aids

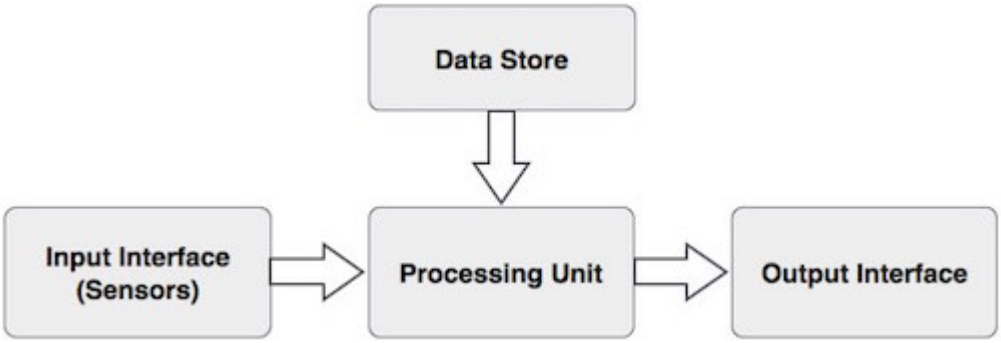
The conventional methods of information system security used ID cards, passwords, Personal Identification Numbers (PINs), etc. They come with the following disadvantages −

- They all mean recognizing some code associated with the person rather than recognizing the person who actually produced it.
- They can be forgotten, lost, or stolen.
- They can be bypassed or easily compromised.
- They are not precise.

In such cases, the security of the system is threatened. When the systems need high level of reliable protection, biometrics comes to help by binding the identity more oriented to individual.

Basic Components of a Biometric System

In general, a biometric system can be divided into four basic components. Let us see them briefly −



Input Interface (Sensors)

It is the sensing component of a biometrics system that converts human biological data into digital form.

For example,

- A Metal Oxide Semiconductor (CMOS) imager or a Charge Coupled Device (CCD) in the case of face recognition, handprint recognition, or iris/retinal recognition systems.
- An optical sensor in case of fingerprint systems.
- A microphone in case of voice recognition systems.

Processing Unit

The processing component is a microprocessor, Digital Signal Processor (DSP), or computer that processes the data captured from the sensors.

The processing of the biometric sample involves −

- Sample image enhancement
- Sample image normalization
- Feature extraction
- Comparison of the biometric sample with all stored samples in database.

Database Store

The database stores the enrolled sample, which is recalled to perform a match at the time of authentication. For identification, there can be any memory from Random Access Memory (RAM), flash EPROM, or a data server. For verification, a removable storage element like a contact or contactless smart card is used.

Output Interface

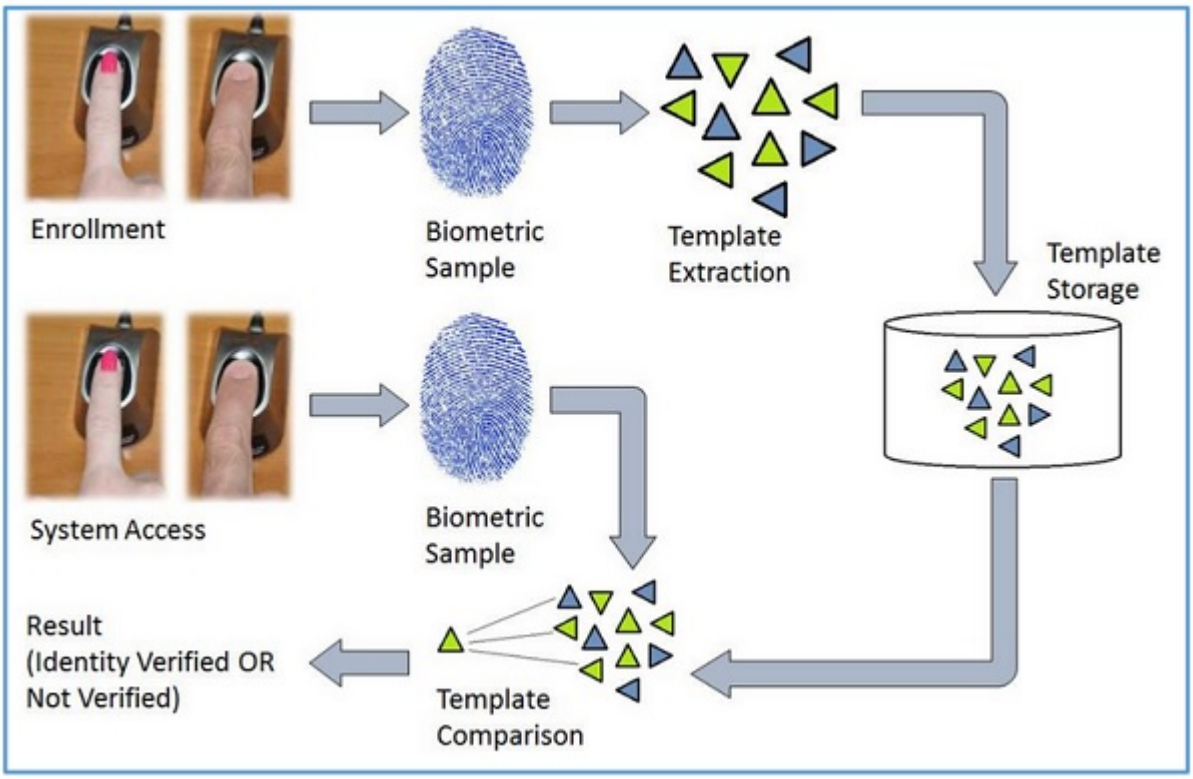
The output interface communicates the decision of the biometric system to enable the access to the user. This can be a simple serial communication protocol RS232, or the higher bandwidth USB protocol. It could also be TCP/IP protocol, Radio Frequency Identification (RFID), Bluetooth, or one of the many cellular protocols.

General Working of a Biometric System

There are four general steps a biometric system takes to perform identification and verification −

- Acquire live sample from candidate. (using sensors)
- Extract prominent features from sample. (using processing unit)
- Compare live sample with samples stored in database. (using algorithms)
- Present the decision. (Accept or reject the candidate.)

The biometric sample is acquired from candidate user. The prominent features are extracted from the sample and it is then compared with all the samples stored in the database. When the input sample matches with one of the samples in the database, the biometric system allows the person to access the resources; otherwise prohibits.



Biometrics Terminology

Biometric Template − It is a digital reference of the distinct characteristics that are extracted from a biometric sample.

Candidate/Subject − A person who enters his biometric sample.

Closed-Set Identification − The person is known to be existing in the database.

Enrollment − It is when a candidate uses a biometric system for the first time, it records the basic information such as name, address, etc. and then records the candidate's biometric trait.

False Acceptance Rate (FAR) − It is the measure of possibility that a biometric system will incorrectly identify an unauthorized user as a valid user.

$$FAR = \frac{\text{Number of False Acceptances}}{\text{Number of Identification Attempts}}$$

A biometric system providing **low FAR ensures high security**.

False Reject Rate (FRR) − It is the measure of possibility that the biometric system will incorrectly reject an authorized user as an invalid user.

$$FRR = \frac{\text{Number of False Rejections}}{\text{Number of Identification Attempts}}$$

Open-Set Identification − The person is not guaranteed to be existing in the database.

Task − It is when the biometric system searches the database for matching sample.

Application Areas of Biometrics

There are a number of applications where biometric systems are useful. Few of them are given below −

- Controlling workplace access.
- Identity establishment of people for authentic citizenship and immigration systems.
- Applying access control to sensitive information and systems.
- Identifying criminals by forensics.
- Executing online e-commerce transactions.
- Fraud and theft reduction.
- Law enforcement.