First Chapter Lesson-7: Biometrics

At the end of this lesson-

- 1. You will be able to explain Biometrics.
- 2. You will be able to describe the elements for implementing biometrics system.
- 3. You will be able to explain biometrics mechanism.
- 4. You will be able to explain the structural and behavioral characteristics of humans which are used in the biometrics system.
- 5. You will be able to describe application areas of biometrics technology.

Biometrics:

Bio means ‘Life’ and Metric means ‘measure’. Biometrics technology measures and analyses biological data. Biometrics is such a technology that is used to identify individuals uniquely based on physiological and behavioral characteristics.

In other words, 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.

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

Each human being is unique in terms of characteristics, which make him or her different from all others. These characteristics make a person stand separate from the rest.

Biological data or attributes used in biometrics are two types:

Physiological :

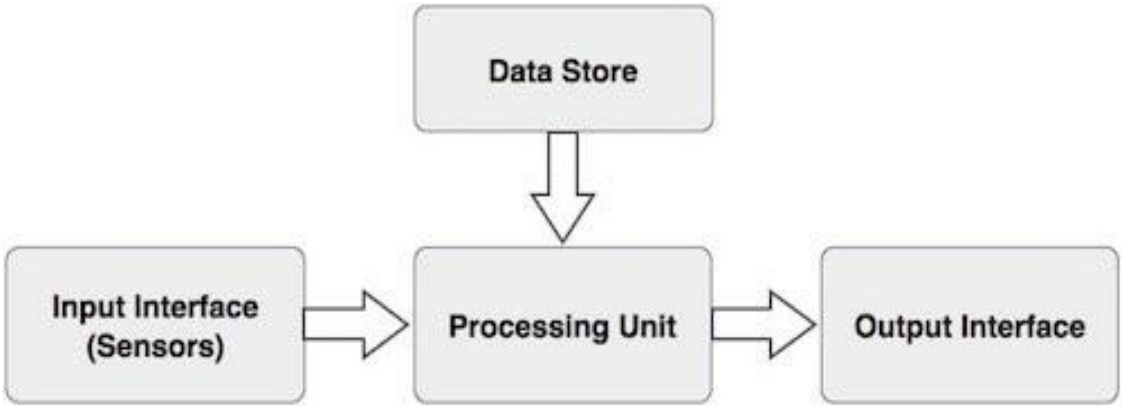
- Face
- Finger Print
- Hand Geometry
- Iris & Retina
- DNA

Behavioral:

- Voice/ tone and accent of speech
- Signature
- Typing Keystroke

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.

Database Store

The database stores the enrolled sample, which is recalled to perform a match at the time of authentication.

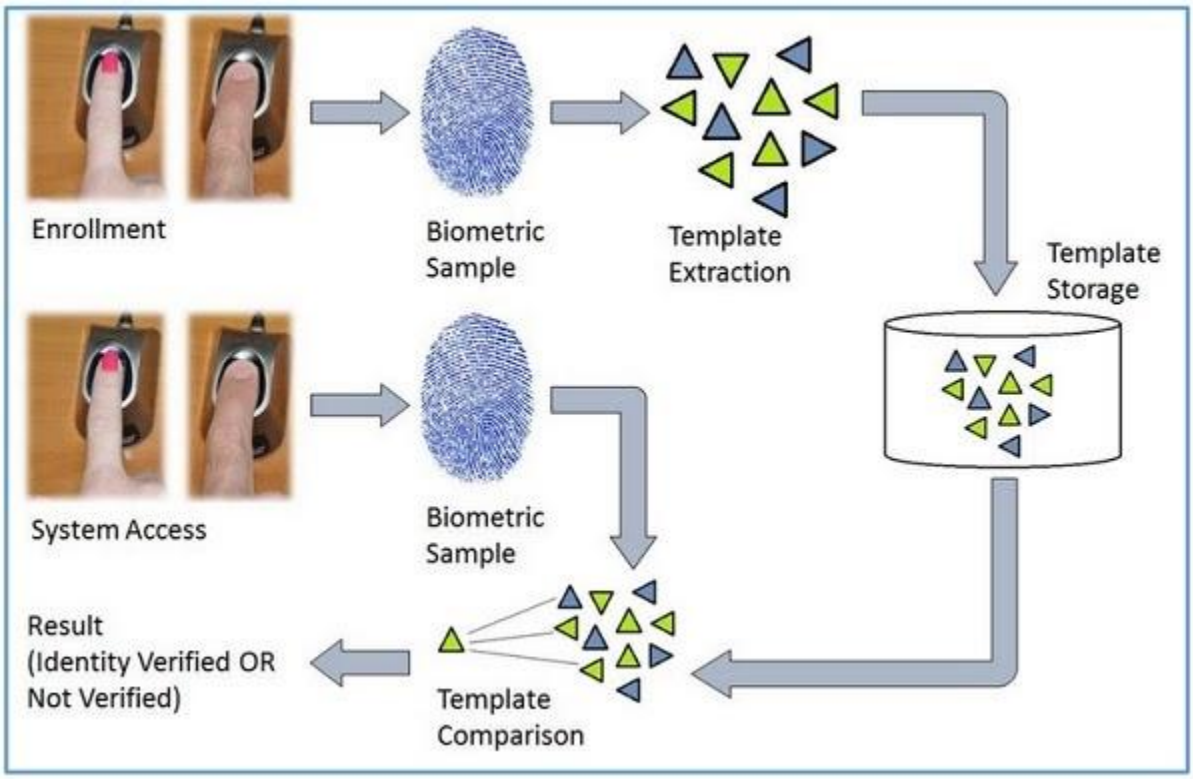
Output Interface

The output interface communicates the decision of the biometric system to enable the access to the user. It could also be TCP/IP protocol, Radio Frequency Identification (RFID), Bluetooth, or one of the many cellular protocols.

General Working Process 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.

Types of Biometric System depending on human trait:

Physiological System:

- Fingerprint Recognition system
- Hand Geometry Recognition system
- Facial Recognition System
- Iris Recognition System
- Retinal Scanning System
- DNA Recognition System

Behavioral System:

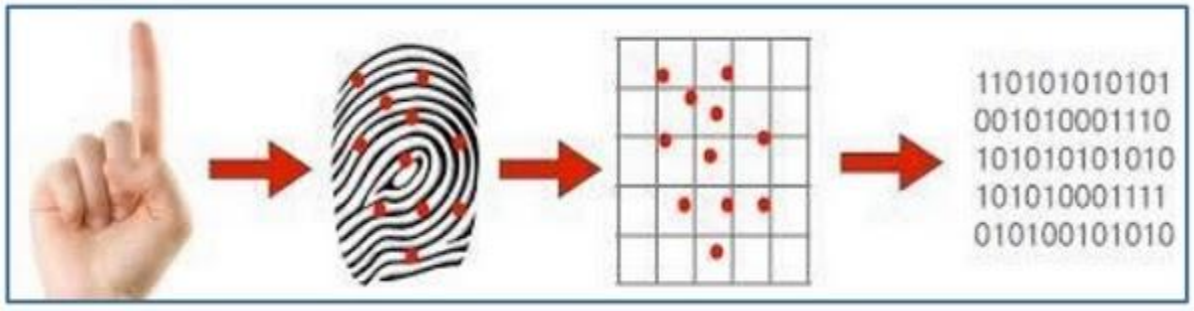
- Voice/ tone and accent of speech Recognition System
- Signature Verification System
- Typing Keystroke Recognition System

Finger Print Recognition System:

It is the most known and used biometrics solution to authenticate people on biometric systems. The reasons for it being so popular are there are ten available sources of biometric and ease of acquisition. Fingerprint is one of oldest and most popular recognition technique

Every person has a unique fingerprint which is composed of ridges, grooves, and direction of the lines. There are three basic patterns of ridges namely, **arch, loop**, and **whorl**. The uniqueness of fingerprint is determined by these features as well as **minutiae features** such as bifurcation and spots (ridge endings).

Finger print reader uses a light-sensitive microchip to produce a digital image. The computer analyzes the image automatically, selecting just the fingerprint, and then uses sophisticated pattern-matching software to match.



Finger print reader is a biometric device that take an image as input and compare with the image stored in database before.

Advantages:

- It is the most contemporary method.
- It is most economical method.
- It is highly reliable and secure.
- It works on a small template size, which speeds up the verifying process.
- It consumes less memory space.

Disadvantages:

- Scars, cuts or absence of finger can hinder the recognition process.
- The systems can be fooled by using artificial finger made of wax.
- It involves physical contact with the system.
- They leave the pattern of finger behind at the time of entering sample.

Uses:

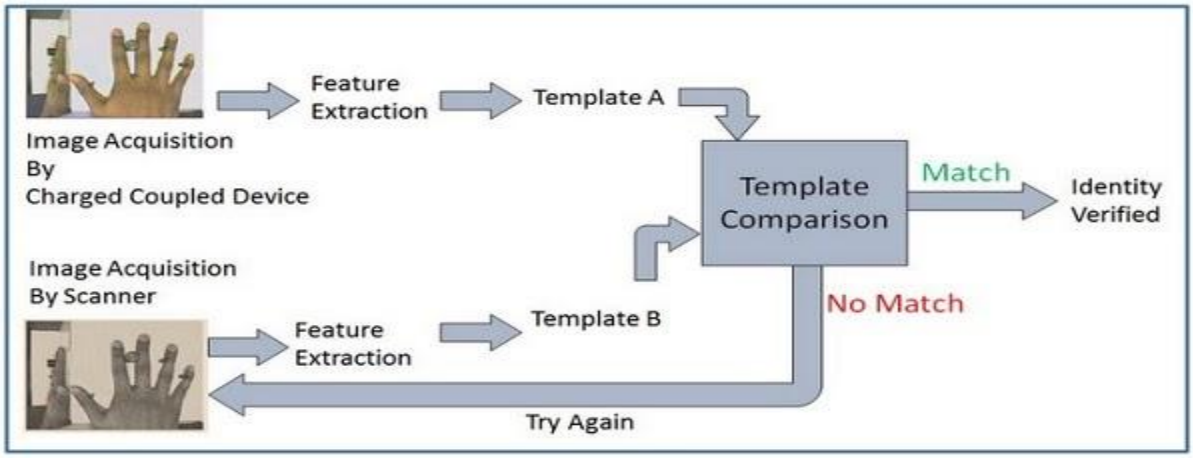
- Used as user name and password for a computer system and website.

- Access control
- In Banking Payment system.
- To identify DNA

Hand Geometry Recognition System:

It includes measuring length and width of palm, surface area, length and position of fingers, and overall bone structure of the hand. A person's hand is unique and can be used to identify a person from others.

Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.



Advantages:

- It is sturdy and user friendly.
- The changes in skin moisture or texture do not affect the result.
- Need less memory.

Disadvantages:

- Since the hand geometry is not unique, it is not very reliable.
- It is effective in case of adults and not for the growing children.
- If candidate's hand is with jewelry, plaster, or arthritis, it is likely to introduce a problem.

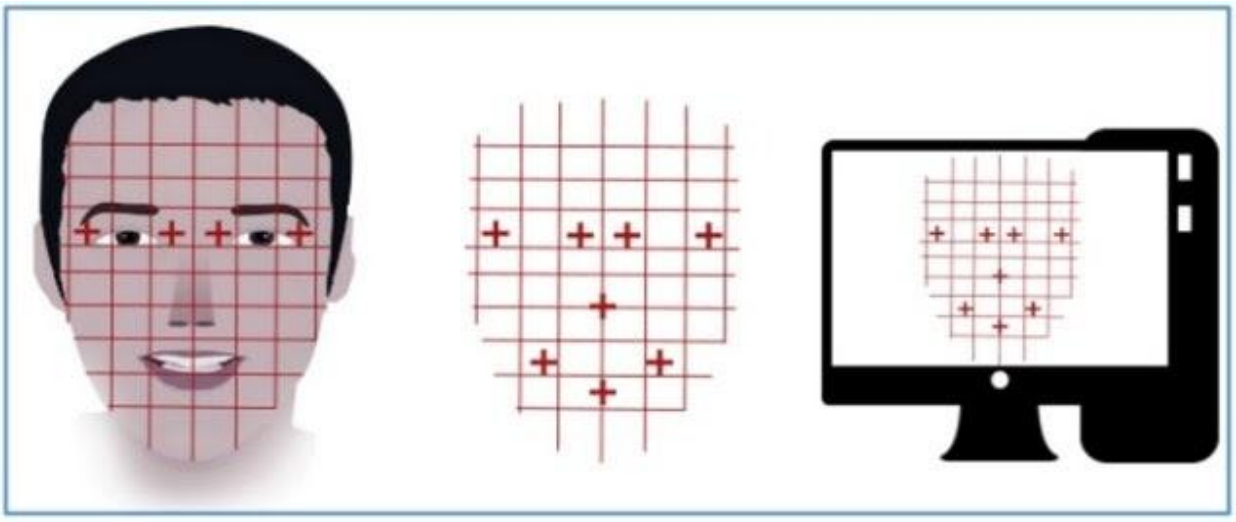
Uses:

- Airport in/out control.
- To record attendance of the employees of a company.
- Nuclear power plants and military use Hand Geometry Recognition for access control.

Face Recognition System:

Facial recognition is based on determining shape and size of jaw, chin, shape and location of the eyes, eyebrows, nose, lips, and cheekbones.

2D facial scanners start reading face geometry and recording it on the grid. The facial geometry is transferred to the database in terms of points. The comparison algorithms perform face matching and come up with the results.



Advantages:

- Easy to use.
- Accuracy is good.
- It offers easy storage of templates in database.
- It reduces the statistic complexities to recognize face image.
- It involves no physical contact with the system.

Disadvantages:

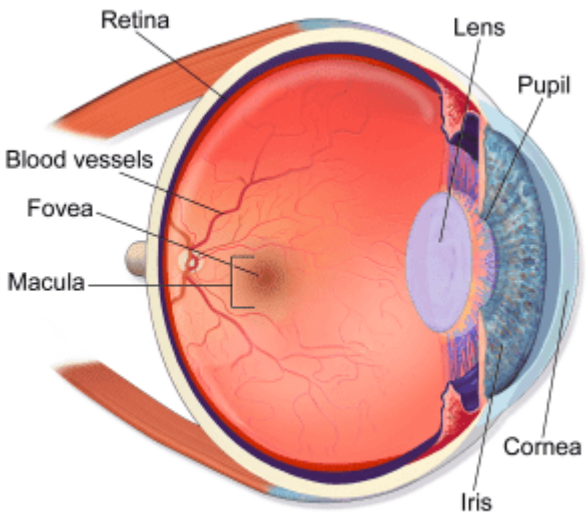
- Facial traits change over time.
- Uniqueness is not guaranteed, for example, in case of identical twins.
- If a candidate face shows different expressions such as light smile, then it can affect the result.
- It requires adequate lighting to get correct input.

Uses:

- General Identity Verification.
- Verification for access control.
- Human-Computer Interaction.
- Criminal Identification.
- Surveillance.

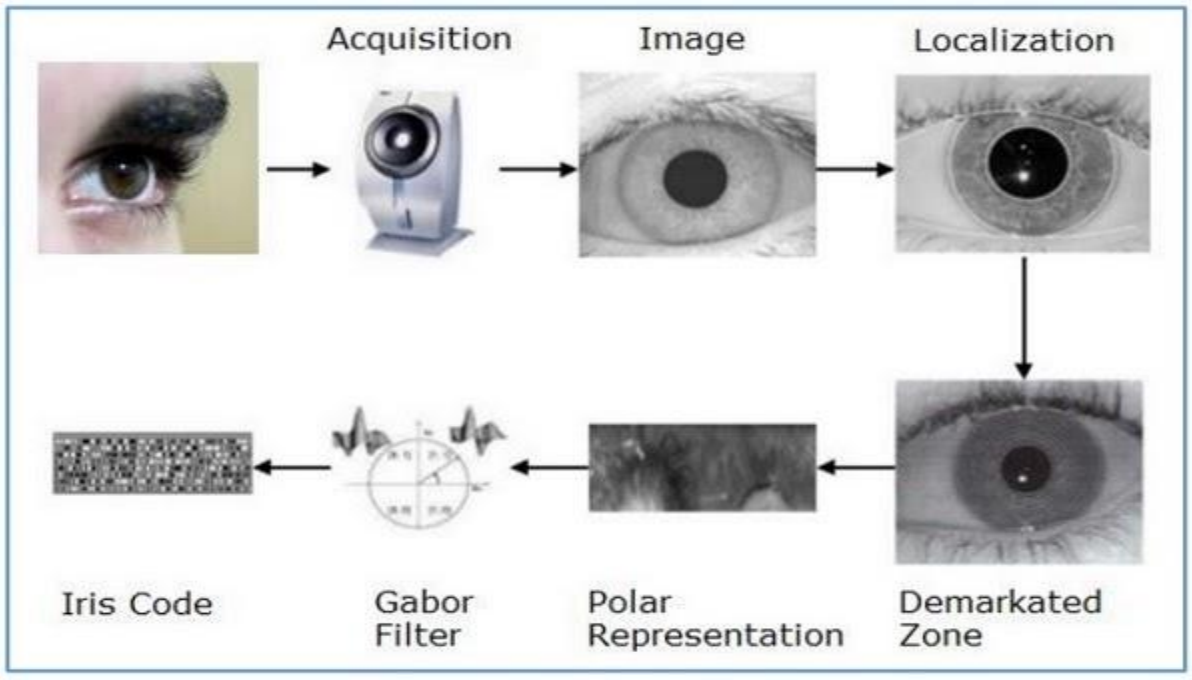
Iris Recognition System:

Iris recognition works on the basis of iris pattern in human eye. The iris is the pigmented elastic tissue that has adjustable circular opening in center. It controls the diameter of pupil. In adult humans, the texture of iris is stable throughout their lives. The iris patterns of left and right eyes are different. The iris patterns and colors change from person to person.



Eye Anatomy

It involves taking the picture of iris with a capable camera, storing it, and comparing the same with the candidate eyes using mathematical algorithms.



Advantages:

- It is highly accurate as the chance of matching two irises is 1 in 10 billion people.
- It is highly scalable as the iris pattern remains same throughout a person's lifetime.
- The candidate need not remove glasses or contact lenses; they do not hamper the accuracy of the system.
- It involves no physical contact with the system.
- It provides instant verification (2 to 5 seconds) because of its small template size.

Disadvantages:

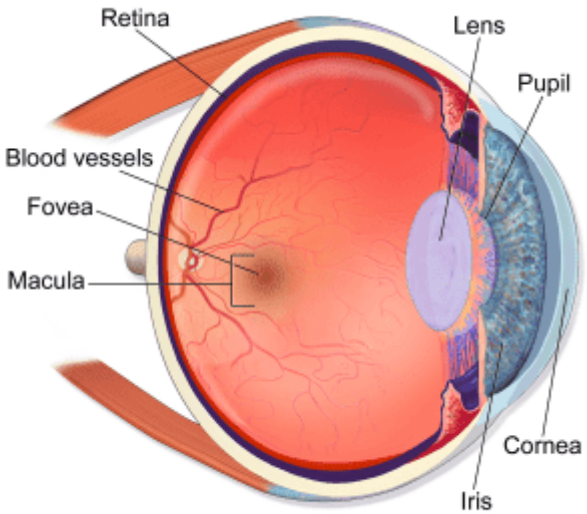
- Iris scanners are expensive.
- High quality images can fool the scanner.
- A person is required to keep his/her head very still for accurate scanning.
- Needs lot of memory.

Uses:

- This system offers to go foreign country without passport.
- Used in Government Company, military and different financial company for identifying purpose.
- Google uses iris recognition for accessing their data centers.

Retinal Scanning System:

Retina is the lining layer at the back of the eyeball that covers 65% of the eyeball's inner surface. It contains **photosensitive** cells. Each person's retina is unique due to the complex network of blood vessels that supply blood.



Eye Anatomy

In retinal scanning process, a person is asked to remove lenses or eyeglasses. A low-intensity infrared light beam is casted into a person's eye for 10 to 15 seconds. This infrared light is absorbed by the blood vessels forming a pattern of blood vessels during the scan. This pattern is then digitized and stored in the database.

It is a reliable biometric as the retina pattern remains unchanged throughout the person's life, barring the patterns of persons having diabetes, glaucoma, or some degenerative disorders.

Advantages:

- It cannot be forged.
- It is highly reliable as the error rate is 1 out of a crore samples (which is almost 0%).

Disadvantages:

- It is not very user friendly as the user needs to maintain steadiness that can cause discomfort.
- It tends to reveal some poor health conditions such as hypertension or diabetes, which causes privacy issues.
- Accuracy of the results is prone to diseases such as cataracts, glaucoma, diabetes, etc.

Uses:

- It is practiced by some government bodies such as CID, FBI, etc.

- Apart from security applications, it is also used for ophthalmological diagnostics.

DNA Recognition System:

Deoxyribo **N**euclic **A**cid (DNA) is the genetic material found in humans. Every human, barring identical twins, is uniquely identifiable by the traits found in their DNA, which is located in the nucleus of the cell.

DNA can be collected from any number of sources: blood, hair, finger nails, mouth swabs, blood stains, saliva, straws, and any number of other sources that has been attached to the body at some time.

Within cells, DNA is organized in long double helix structure called **chromosomes**. There are 23 pairs of chromosomes in humans. Out of the 46 total chromosomes, the offspring inherits 23 chromosomes from each biological parent. 99.7% of an offspring's DNA is shared with their parents. The remaining 0.3% DNA contains repetitive coding unique to an individual.

The fundamental steps of DNA profiling are −

- Separating the DNA from sample acquired from either of blood, saliva, hair, semen, or tissue.
- Separating the DNA sample into shorter segments.
- Organizing the DNA segments according to size.
- Comparing the DNA segments from various samples.

The more detailed the sample is, the more precise the comparison and in turn the identification of the individual is.

DNA Biometrics differs from all others in the following ways −

- It needs a tangible physical sample instead of image.
- DNA matching is done on physical samples. There is no feature extraction or template saving.

Advantages:

- It provides the highest accuracy.

Disadvantages:

- Length of procedure from sample acquisition to result is large.
- Being more informative, it brings privacy issues.
- It needs more storage space.
- Sampling contamination or degradation of sample may affect the result.

Uses:

- DNA matching has become a popular use in criminal trials, especially in proving rape cases.
- It is mainly used to prove guilt or innocence.
- It is used in physical and network security.

Voice Recognition System:

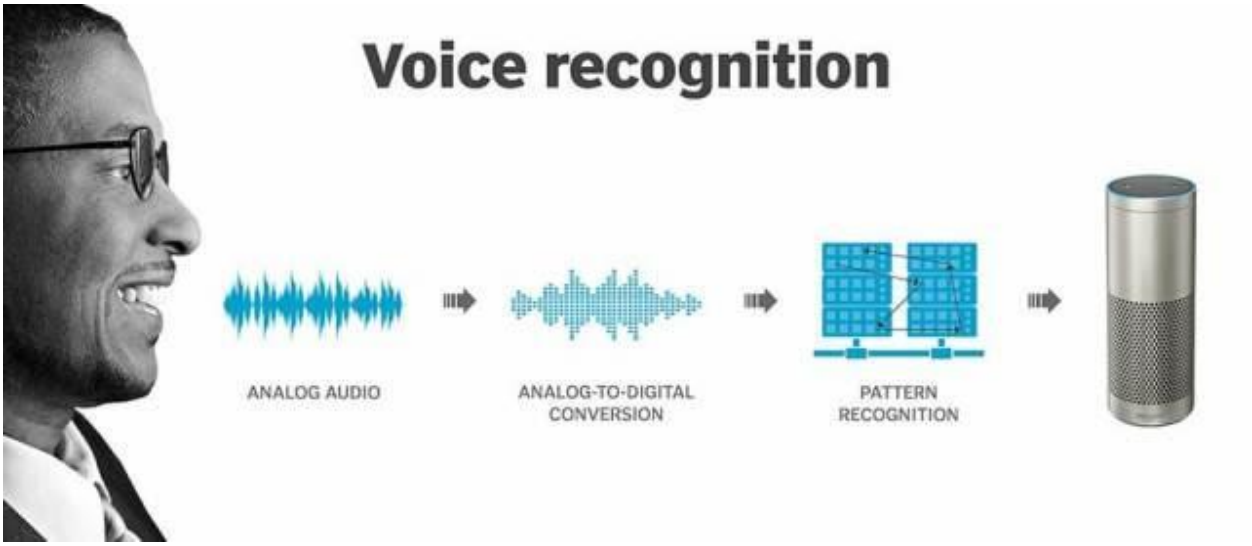
Voice and speech recognition are two separate biometric modalities that, because they are dependent on the human voice, see a considerable amount of synergy.

Both are contactless, software based technologies, and as such are counted among the most convenient biometrics in regular use.

Voice recognition, also commonly referred to a voiceprint, is the identification and authentication arm of the vocal modalities.

By measuring the sounds a user makes while speaking, voice recognition software can measure the unique biological factors that, combined, produce her voice.

Voiceprints can be measured passively as a user speaks naturally in conversation, or actively, if she is made to speak a passphrase.

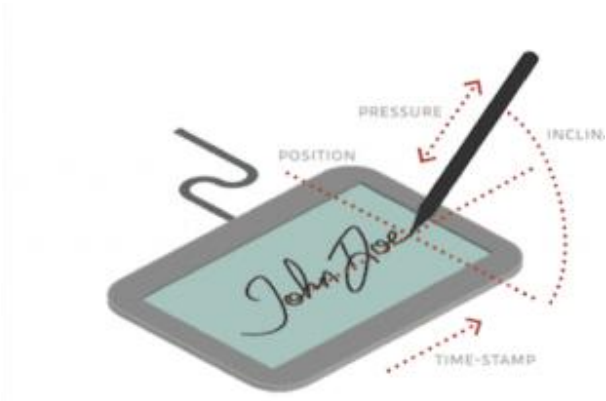


Voice recognition is strengthening other biometric login solutions. The USAA banking app, for example, uses facial recognition and voice recognition to provide easy and secure multi-factor biometric security, the voice component adding an extra level of liveness detection to the process.

Signature Verification System:

The behavioral patterns include the changes in the timing of writing, pauses, pressure, direction of strokes, and speed during the course of signing. It could be easy to duplicate the graphical appearance of the signature but it is not easy to imitate the signature with the same behavior the person shows while signing.

This technology consists of a pen and a specialized writing tablet, both connected to a computer for template comparison and verification. A high quality tablet can capture the behavioral traits such as speed, pressure, and timing while signing.



During enrollment phase, the candidate must sign on the writing tablet multiple times for data acquisition. The signature recognition algorithms then extracts the unique features such as timing, pressure, speed, direction of strokes, important points on the path of signature, and the size of signature. The algorithm assigns different values of weights to those points.

At the time of identification, the candidate enters the live sample of the signature, which is compared with the signatures in the database.

Advantages:

- It is a non-invasive tool.
- We all use our signature in some sort of commerce, and thus there are virtually no privacy rights issues involved.
- Even if the system is hacked and the template is stolen, it is easy to restore the template.

Disadvantages:

- User need to get accustomed of using signing tablet. Error rate is high till it happens.

Uses:

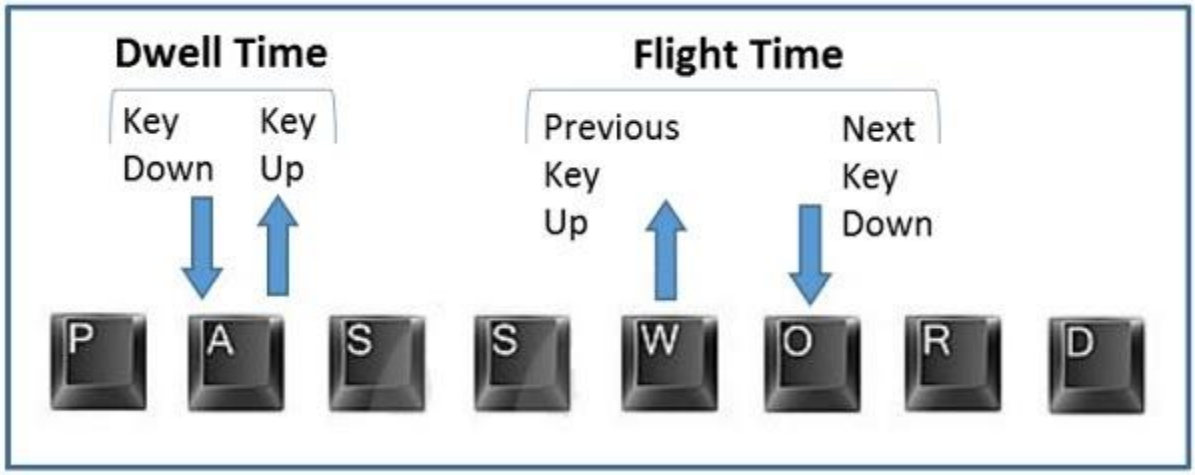
- Signature verification is a technique used by banks, intelligence agencies and high-profile institutions to validate the identity of an individual.
- Signature verification is often used to compare signatures in bank offices and other branch capture.

Keystroke Recognition System:

This biometric analyzes candidate's typing pattern, the rhythm, and the speed of typing on a keyboard. The **dwell time** and **flight time** measurements are used in keystroke recognition.

Dwell time − It is the duration of time for which a key is pressed.

Flight time − It is the time elapsed between releasing a key and pressing the following key.



The candidates differ in the way they type on the keyboard as the time they take to find the right key, the flight time, and the dwelling time. Their speed and rhythm of typing also varies according to their level of comfort with the keyboard. Keystroke recognition system monitors the keyboard inputs thousands of times per second in a single attempt to identify users based on their habits of typing.

Advantages:

- It needs no special hardware to track this biometric.
- It is a quick and secure way of identification.
- A person typing does not have to worry about being watched.
- Users need no training for enrollment or entering their live samples.

Disadvantages:

- The candidate's typing rhythm can change between a number of days or within a day itself because of tiredness, sickness, influence of medicines or alcohol, change of keyboard, etc.
- There are no known features dedicated solely to carry out discriminating information.

Uses:

- Keystroke Recognition is used for identification/verification. It is used with user ID/password as a form of **multifactor authentication**.
- It is used for surveillance. Some software solutions track keystroke behavior for each user account without end-user's knowledge. This tracking is used to analyze if the account was being shared or used by anyone else than the

genuine account owner. It is used to verify if some software license is being shared.

Application Areas of Biometrics:

- Controlling the access to a room, sensitive information, digital system, software etc.
- To record attendance of the teachers, students for an educational institute or employees of a commercial company.
- Identity establishment of people for authentic citizenship and immigration systems.
- Driving License
- Secured payment system or executing online e-commerce transactions.
- Identifying criminals by forensics.
- Fraud and theft reduction.
- Law enforcement.

Advantages of Biometrics System:

- No more forgotten or stolen passwords.
- Positive and accurate Identification
- Highest level of security
- Offers mobility
- Impossible to forge
- Serves as a Key that cannot be transferred.
- Safe & user friendly

Lesson Evaluation-

Knowledge Based Questions:

- a. What is biometrics?
-

Comprehension Based Questions:

- b. Explain the technology used for identifying an individual.
- b. "Biometrics is a behavior's properties dependent technology"- Explain.
- b. What are the advantages and disadvantages of using biometrics technology?
- b. "Using biometrics system is convenient for office security"- Explain.

Creative Questions:

According to the stem answer the following Questions:

The identity of many garment workers who were killed in the destruction of Rana Plaza in Savar was not initially identified. Later, with the intention of the government, high technology made it possible to identify most bodies.

c) Identify and explain the procedure adopted for the identification of the bodies of the workers described in the stem.

According to the stem answer the following Questions:

Rafiq has brought his business company under the control of computer technology. The main gate of his organization is opened when an employee place finger on a machine. On the other hand, employees have to wait a bit in front of a machine when they enter their rooms.

c) Discuss the process of entering into the main gate of the company.

d) Which one is more convenient between two techniques used in main gate and employees own room? Analyze.

Multiple Choice Questions:

1. In Biometrics system Fingerprint is-

a) Unique Identity b) Finger Identity c) Input Data d) Biological Data

2. What is called the technology that identify an individual based on structural characteristics?

a) Biometrics b) Bioinformatics c) Biotechnology d) Genetic Engineering

3. Which one is used in Biometrics?

a) Sensor b) Digital Meter c) Weight Meter d) Thermometer

4. The behavioral characteristics of Biometrics are-

i. Voice Recognition ii. DNA iii. Signature Verification

Which one is correct?

a) i & ii b) i & iii c) ii & iii d) i, ii & iii

5. The structural characteristics of Biometrics are-

i. Face Recognition ii. DNA iii. Finger Print

Which one is correct?

a) i & ii b) i & iii c) ii & iii d) i, ii & iii