Biometrics

Realistic Authentication

tutorialspoint

SIMPLYEASYLEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

This tutorial provides introductory knowledge on Biometrics. By accessing this tutorial, you would get sufficient information about the basics of biometrics and different biometric modalities such as physiological, behavioral, and combination of both modalities.

This tutorial also provides a glimpse of various security issues related to biometric systems, and the comparison of various biometric systems.

Audience

This tutorial is prepared for the students at beginner level who aspire to understand biometrics and various biometric systems. It would also be useful for enthusiasts in the fields of Electronics, IT security, and Biology.

Prerequisites

Biometrics is an advanced concept and we cannot claim that a reader can sail through this tutorial without having any grip over some basic knowledge of Computer Science, and Mathematics. Knowledge of Science is a plus.

Disclaimer & Copyright

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher. We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com.

Table of Contents

About the Tutorial i

Audience i

Prerequisites i

Disclaimer & Copyright i

Table of Contents ii

1. OVERVIEW OF BIOMETRICS 1

What is Biometrics? 1

What is a Biometric System? 1

Evolution of Biometrics 1

Why Biometrics is Required? 2

Basic Components of a Biometric System 3

General Working of a Biometric System 4

Biometrics Terminology 5

Application Areas of Biometrics 6

2. BIOMETRIC MODALITIES 7

Types of Biometric Modalities 7

3. PHYSIOLOGICAL MODALITIES 9

Fingerprint Recognition System 9

Facial Recognition System 10

Iris Recognition System 11

Hand Geometry Recognition System 13

Retinal Scanning System 14

DNA Recognition System 15

4. BEHAVIORAL MODALITIES 17

Gait Recognition 17

Signature Recognition System 18

Keystroke Recognition System 20

5. VOICE RECOGNITION 22

Voice Recognition System 22

Difference between Voice and Speech Recognition 23

6. MULTIMODAL BIOMETRIC SYSTEMS 25

Why Multimodal Biometrics is Required? 25

Working of Multimodal Biometric System 25

Design Issues with Multimodal Biometric Systems 27

7. BIOMETRIC MODALITY SELECTION 28

Criteria for Effective Biometric System 28

Comparison of Various Biometric Modalities 29

8. BIOMETRIC SYSTEM PERFORMANCE 30

Performance Measurements 30

9. PATTERN RECOGNITION AND BIOMETRICS 31

Pattern Recognition in Biometrics 31

Components of Pattern Recognition 31

Popular Algorithms in Pattern Recognition 32

10. SIGNAL PROCESSING AND BIOMETRICS 33

What is a Signal? 33

Signal Processing in Biometrics 33

Digital Signal Processing Systems (DSPs) 34

DSP in Biometrics 34

11. BIOMETRICS AND IMAGE PROCESSING 35

Requirement of Image Processing in Biometrics 35

12. BIOMETRIC SYSTEM SECURITY 37

Biometric System Vulnerability..37

Risks with Biometric System Security..37

Biometric System Security 38

Criteria for Generating Biometric Templates 39

1. OVERVIEW OF BIOMETRICS

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 14th century, China practiced taking finger prints of merchants and their children to separate them from all others. Fingerprinting is still used today.

- In the 19th 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.

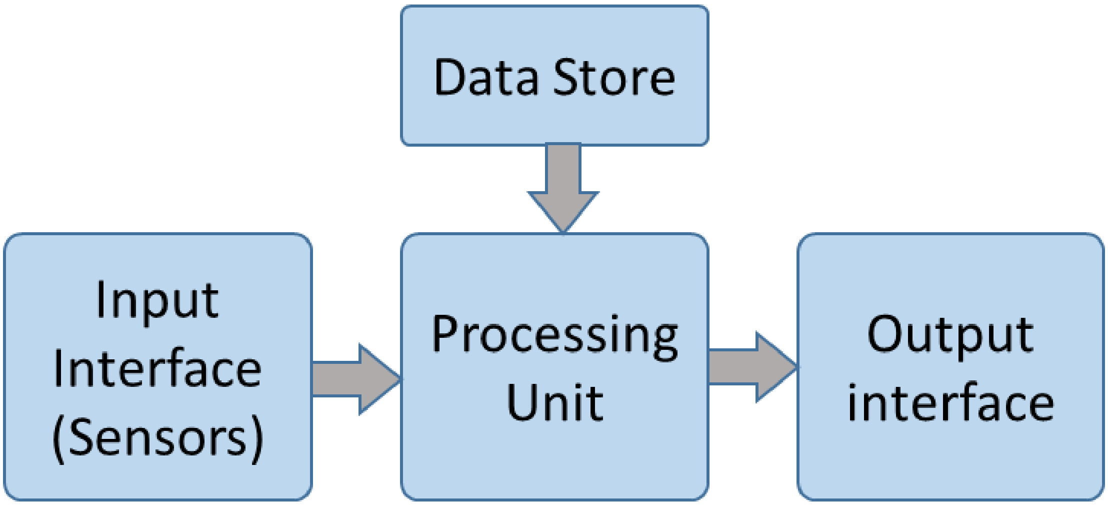
- They can be forgotten, lost, or stolen.

- 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:

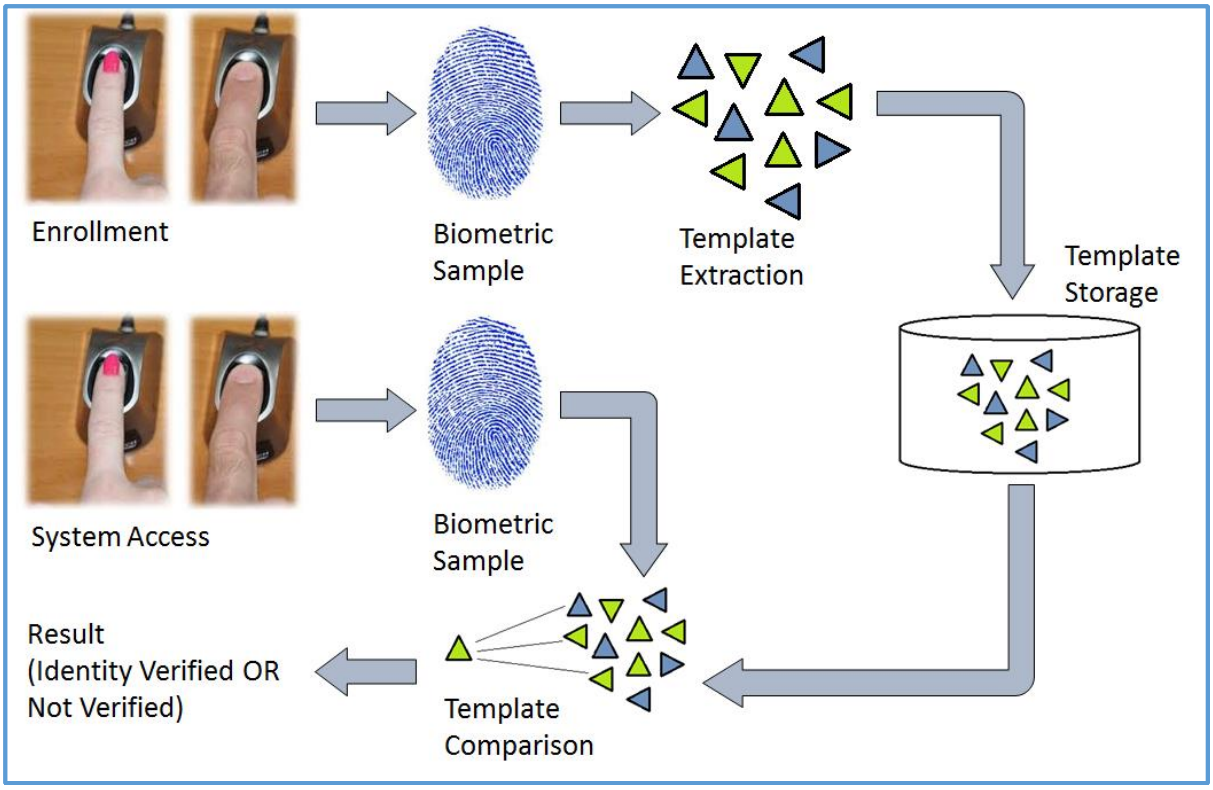
1. Acquire live sample from candidate. (using sensors)

2. Extract prominent features from sample. (using processing unit)

3. Compare live sample with samples stored in database. (using algorithms)

4. 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.

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

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.

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

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.

2. BIOMETRIC MODALITIES

A biometric modality is nothing but a category of a biometric system depending upon the type of human trait it takes as input.

The biometrics is largely statistical. The more the data available from sample, the more the system is likely to be unique and reliable. It can work on various modalities pertaining to measurements of individual's body and features, and behavioral patterns. The modalities are classified based on the person's biological traits.

Types of Biometric Modalities

There are various traits present in humans, which can be used as biometrics modalities. The biometric modalities fall under three types:

1. Physiological
2. Behavioral
3. Combination of physiological and behavioral modality

The following table collects the points that differentiate these three modalities:

Physiological Modality	Behavioral Modality	Combination of Both Modalities
This modality pertains to the shape and size of the body.	This modality is related to change in human behavior over time.	This modality includes both traits, where the traits are depending upon physical as well as behavioral changes.
For example: • Fingerprint Recognition • Hand Geometry Recognition system • Facial Recognition System • Iris Recognition System	For example: • Gait (the way one walks) • Rhythm of typing keys • Signature	For example: Voice Recognition It depends on health, size, and shape of vocal cord, nasal cavities, mouth cavity, shape of lips, etc., and the emotional status, age, illness (behavior) of a person.

• Hand Geometry Recognition System • Retinal Scanning System • DNA Recognition System		

In the subsequent chapters, we will discuss each of these modalities in greater detail.

3. PHYSIOLOGICAL MODALITIES

As depicted earlier, the physiological modalities are based on the direct measurement of parts of human body such as iris, fingerprint, shape, and position of fingers, etc.

There are some physical traits which remain unaltered throughout a person’s life. They can be an excellent resource for identification of an individual.

Fingerprint 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.

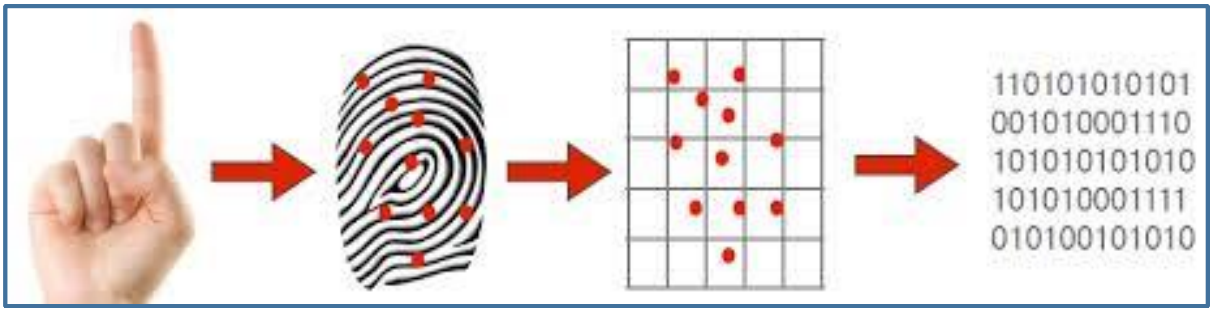
Every person has a unique fingerprint which is composed of ridges, grooves, and direction of the lines. There are three basic patterns of ridges namely, **arch**, **loop**, and **whorl**. The uniqueness of fingerprint is determined by these features as well as **minutiae features** such as bifurcation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

Fingerprint is one of oldest and most popular recognition technique. Fingerprint matching techniques are of three types:

1. **Minutiae Based Techniques:** In these minutiae points are found and then mapped to their relative position on finger. There are some difficulties such as if image is of low quality, then it is difficult to find minutiae points correctly. Another difficulty is, it considers local position of ridges and furrows; not global.

2. **Correlation Based Method:** It uses richer gray scale information. It overcomes problems of minutiae-based method, by being able to work with bad quality data. But it has some of its own problems like localization of points.

3. **Pattern Based (Image Based) Matching:** Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a stored template and a candidate fingerprint.



Merits of Finger Recognition System

- 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.

Demerits of Finger Recognition System

- 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.

Applications of Finger Recognition System

- Verification of driver-license authenticity.
- Checking validity of driving license.
- Border Control/Visa Issuance.
- Access control in organizations.

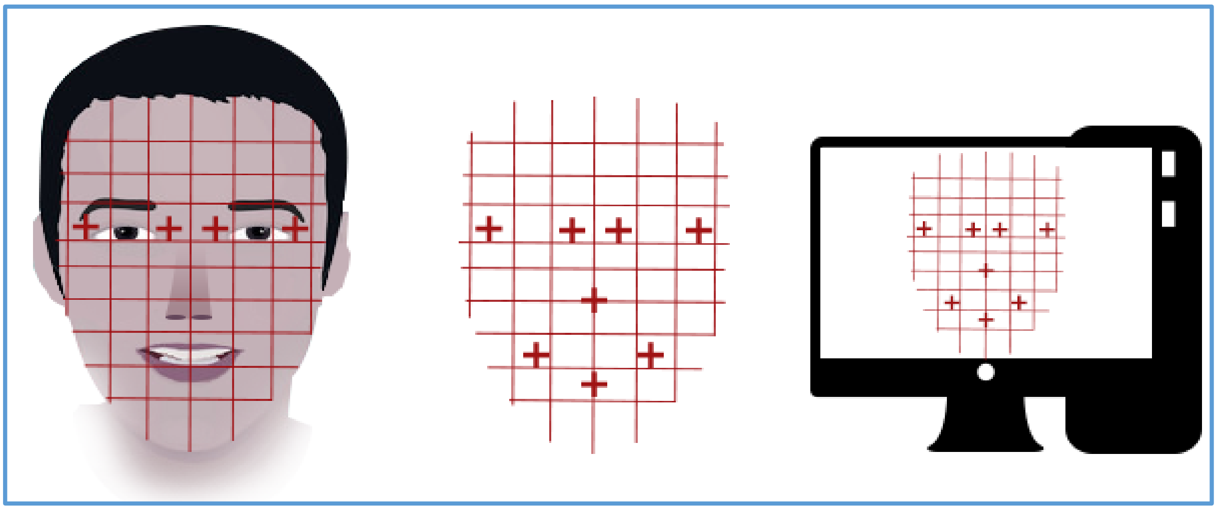
Facial Recognition System

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. Facial recognition is performed in the following ways:

- **Facial Metrics:** In this type, the distances between pupils or from nose to lip or chin are measured.

- **Eigen faces:** It is the process of analyzing the overall face image as a weighted combination of a number of faces.

- **Skin Texture Analysis:** The unique lines, patterns, and spots apparent in a person’s skin are located.



Merits of Facial Recognition System

- 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.

Demerits of Facial Recognition System

- 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.

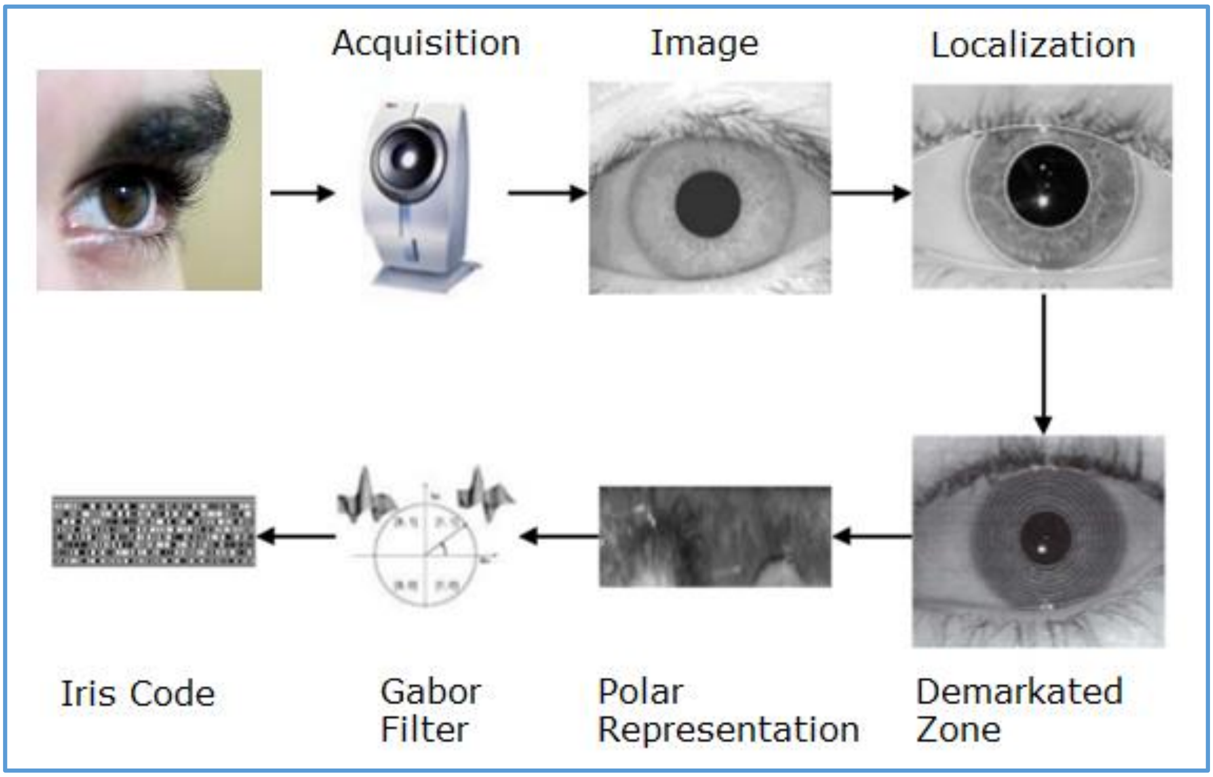
Applications of Facial Recognition System

- 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.

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



Merits of Iris Recognition System

- 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.

Demerits of Iris Recognition System

- 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.

Applications of Iris Recognition System

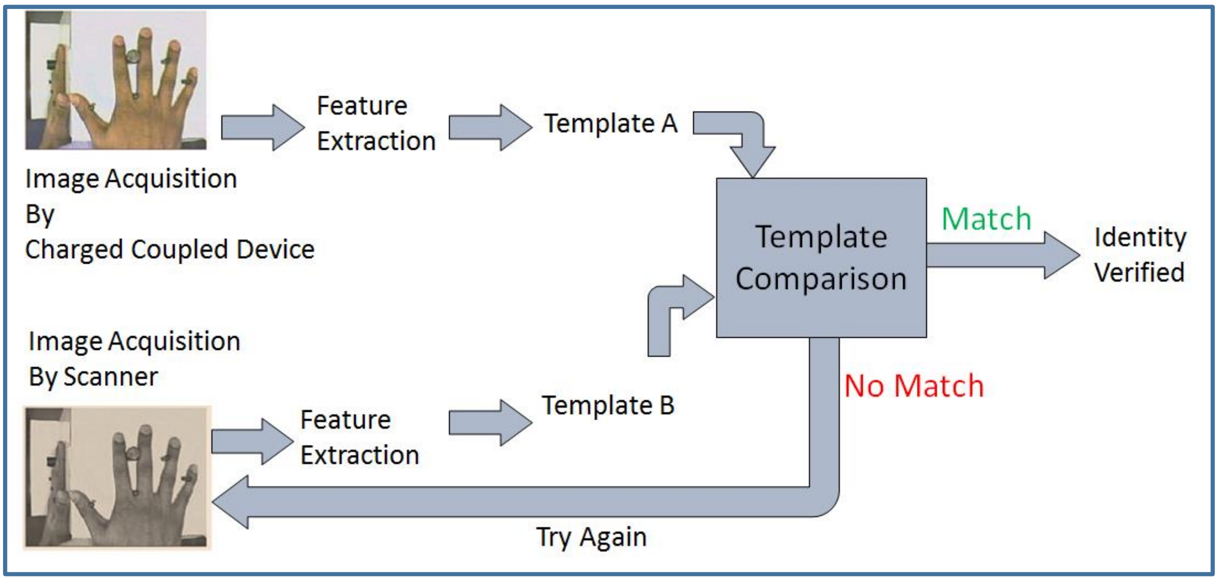
- National security and Identity cards such as *Adhaar* card in India.
- Google uses iris recognition for accessing their datacenters.

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. There are two Hand Geometry systems:

- **Contact Based:** a hand is placed on a scanner's surface. This placement is positioned by five pins, which guide the candidate hand to position correctly for the camera.

- **Contact Less:** In this approach neither pins nor platform are required for hand image acquisition.



Merits of Hand Geometry Recognition System

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

Demerits of Hand Geometry Recognition System

- 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.

Applications of Hand Geometry Recognition System

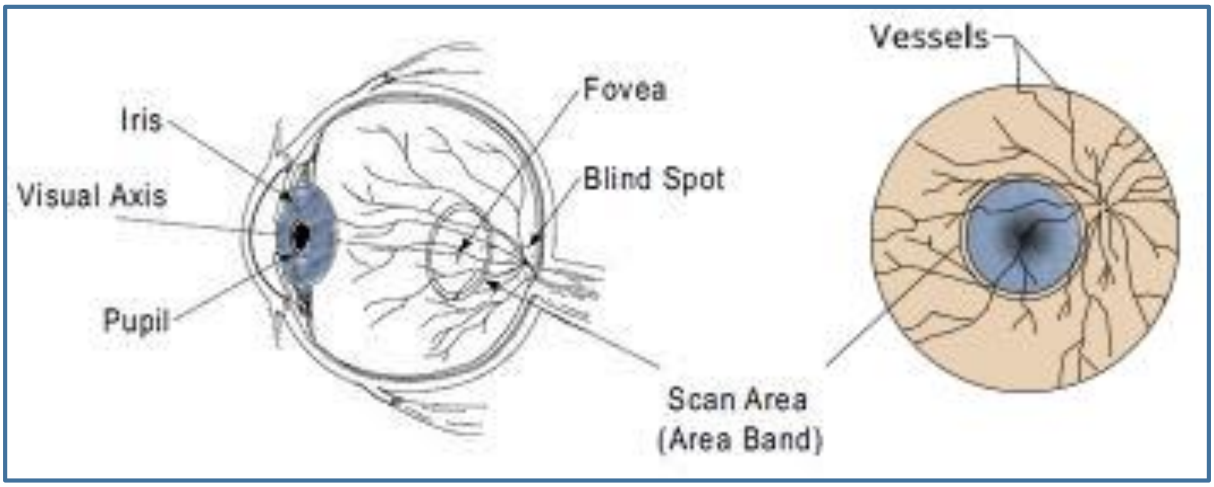
- Nuclear power plants and military use Hand Geometry Recognition for access control.

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.

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.

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.



Merits of Retinal Scanning System

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

Demerits of Retinal Scanning System

- 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.

Applications of Retinal Scanning System

- 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. There are number of sources from which DNA patterns can be collected such as blood, saliva, nails, hair, etc.

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:

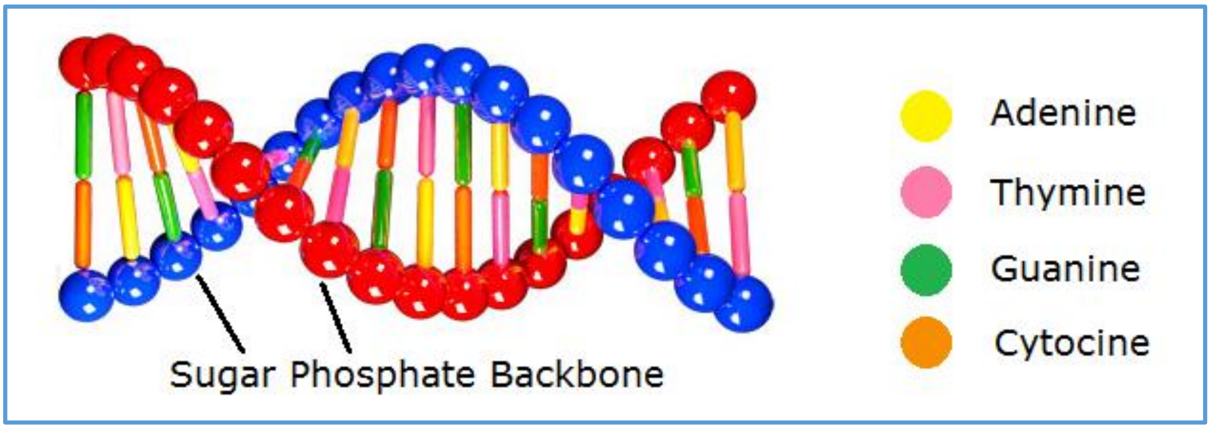
1. Separating the DNA from sample acquired from either of blood, saliva, hair, semen, or tissue.

2. Separating the DNA sample into shorter segments.

3. Organizing the DNA segments according to size.

4. 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.

Merit of DNA Recognition System

It provides the highest accuracy.

Demerits of DNA Recognition System

- 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.

Applications of DNA Recognition System

- It is mainly used to prove guilt or innocence.
- It is used in physical and network security.

4. BEHAVIORAL MODALITIES

Behavioral biometrics pertains to the behavior exhibited by people or the manner in which people perform tasks such as walking, signing, and typing on the keyboard.

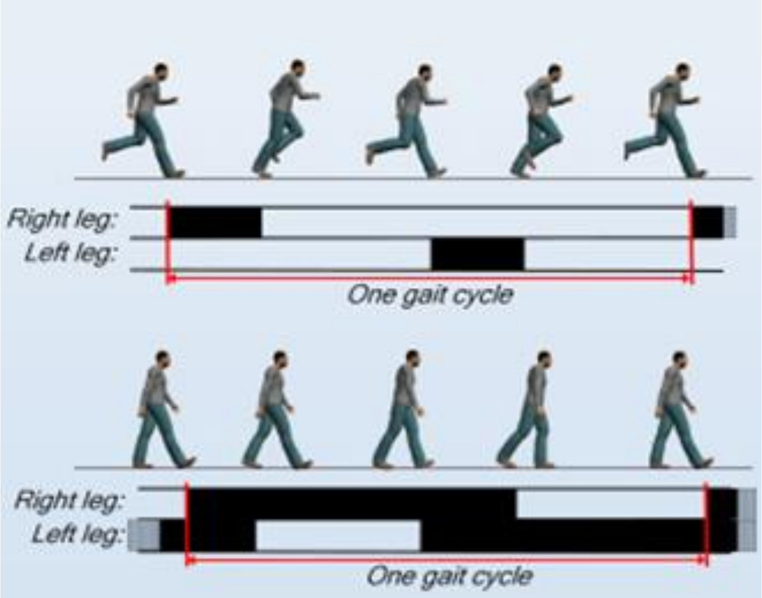
Behavioral biometrics modalities have higher variations as they primarily depend on the external factors such as fatigue, mood, etc. This causes higher FAR and FRR as compared to solutions based on a physiological biometrics.

Gait Recognition

Gait is the manner of a person's walking. People show different traits while walking such as body posture, distance between two feet while walking, swaying, etc., which help to recognize them uniquely.

A gait recognition based on the analyzing the video images of candidate's walk. The sample of candidate's walk cycle is recorded by Video. The sample is then analyzed for position of joints such as knees and ankles, and the angles made between them while walking.

A respective mathematical model is created for every candidate person and stored in the database. At the time of verification, this model is compared with the live sample of the candidate walk to determine its identity.



Merits of Gait Recognition System

- It is non-invasive.
- It does not need the candidate's cooperation as it can be used from a distance.

- It can be used for determining medical disorders by spotting changes in walking pattern of a person in case of Parkinson's disease.

Demerits of Gait Recognition System

- For this biometric technique, no model is developed with complete accuracy till now.
- It may not be as reliable as other established biometric techniques.

Application of Gait Recognition System

It is well-suited for identifying criminals in the crime scenario.

Signature Recognition System

In this case, more emphasis is given on the behavioral patterns in which the signature is signed than the way a signature looks in terms of graphics.

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.

Constraints of Signature Recognition System

- To acquire adequate amount of data, the signature should be small enough to fit on tablet and big enough to be able to deal with.
- The quality of the writing tablet decides the robustness of signature recognition enrollment template.
- The candidate must perform the verification processes in the same type of environment and conditions as they were at the time of enrollment. If there is a change, then the enrollment template and live sample template may differ from each other.

Merits of Signature Recognition System

- Signature recognition process has a high resistance to imposters as it is very difficult to imitate the behavior patterns associated with the signature.
- It works very well in high amount business transactions. For example, Signature recognition could be used to positively verify the business representatives involved in the transaction before any classified documents are opened and signed.
- 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.

Demerits of Signature Recognition System

- The live sample template is prone to change with respect to the changes in behavior while signing. For example, signing with a hand held in plaster.
- User need to get accustomed of using signing tablet. Error rate is high till it happens.

Applications of Signature Recognition System

- It is used in document verification and authorization.
- The Chase Manhattan Bank, Chicago is known as the first bank to adopt Signature Recognition technology.

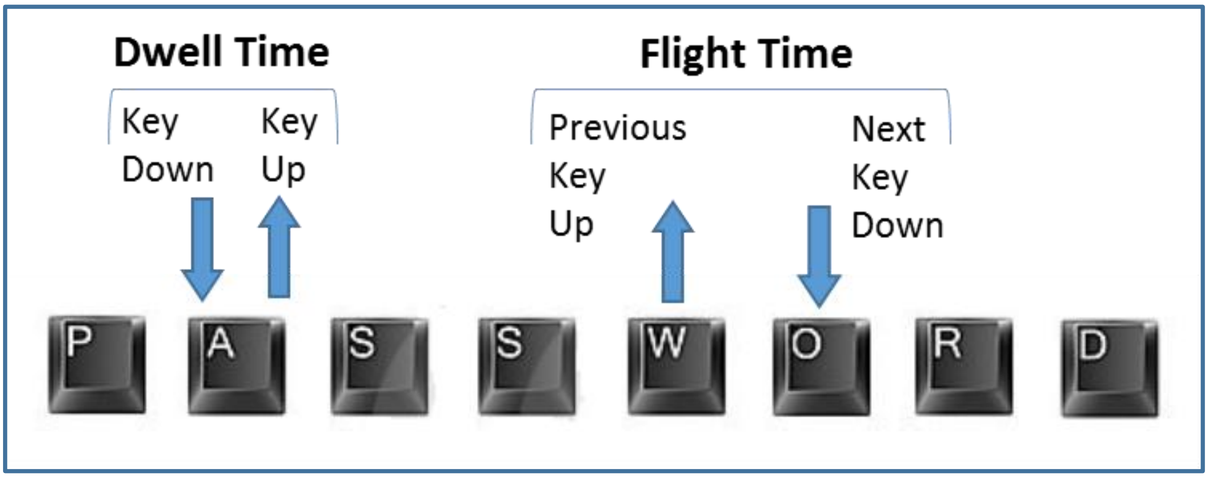
Keystroke Recognition System

During the World War II, a technique known as *Fist of the Sender* was used by military intelligence to determine if the Morse code was sent by enemy or ally based on the rhythm of typing. These days, keystroke dynamics the easiest biometric solution to implement in terms of hardware.

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.

There are two types of keystroke recognition:

1. **Static** – It is one time recognition at the start of interaction.
2. **Continuous** – It is throughout the course of interaction.

Application of Keystroke Dynamics

- 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.

Merits of Keystroke Recognition System

- 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.

Demerits of Keystroke Recognition System

- 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.

5. VOICE RECOGNITION

Voice recognition biometric modality is a combination of both physiological and behavioral modalities. Voice recognition is nothing but sound recognition. It relies on features influenced by:

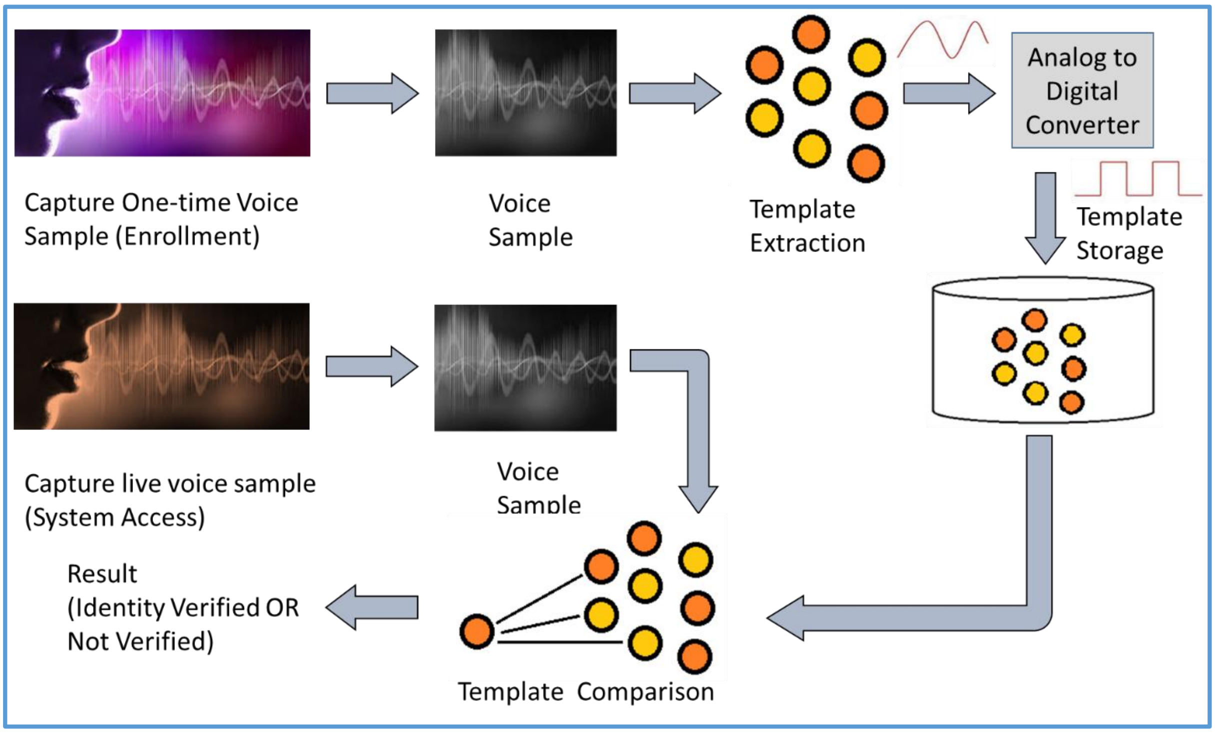
- **Physiological Component:** Physical shape, size, and health of a person's vocal cord, and lips, teeth, tongue, and mouth cavity.

- **Behavioral Component:** Emotional status of the person while speaking, accents, tone, pitch, pace of talking, mumbling, etc.

Voice Recognition System

Voice Recognition is also called Speaker Recognition. At the time of enrollment, the user needs to speak a word or phrase into a microphone. This is necessary to acquire speech sample of a candidate.

The electrical signal from the microphone is converted into digital signal by an Analog to Digital (ADC) converter. It is recorded into the computer memory as a digitized sample. The computer then compares and attempts to match the input voice of candidate with the stored digitized voice sample and identifies the candidate.


Capture One-time Voice Sample (Enrollment)
Voice Sample
Template Extraction
Analog to Digital Converter
Template Storage
Capture live voice sample (System Access)
Voice Sample
Result (Identity Verified OR Not Verified)
Template Comparison

Voice Recognition Modalities

There are two variants of voice recognition: **speaker dependent** and **speaker independent**.

Speaker dependent voice recognition relies on the knowledge of candidate's particular voice characteristics. This system learns those characteristics through voice training (or enrollment).

- The system needs to be trained on the users to accustom it to a particular accent and tone before employing to recognize what was said.
- It is a good option if there is only one user going to use the system.

Speaker independent systems are able to recognize the speech from different users by restricting the contexts of the speech such as words and phrases. These systems are used for automated telephone interfaces.

- They do not require training the system on each individual user.
- They are a good choice to be used by different individuals where it is not required to recognize each candidate's speech characteristics.

Difference between Voice and Speech Recognition

Speaker recognition and Speech recognition are mistakenly taken as same; but they are different technologies. Let us see, how:

Speaker Recognition (Voice Recognition)	Speech Recognition
The objective of voice recognition is to recognize WHO is speaking.	The speech recognition aims at understanding and comprehending WHAT was spoken.
It is used to identify a person by analyzing its tone, voice pitch, and accent.	It is used in hand-free computing, map, or menu navigation.

Merits of Voice Recognition

It is easy to implement.

Demerits of Voice Recognition

- It is susceptible to quality of microphone and noise.
- The inability to control the factors affecting the input system can significantly decrease performance.
- Some speaker verification systems are also susceptible to spoofing attacks through recorded voice.

Applications of Voice Recognition

- Performing telephone and internet transactions.
- Working with Interactive Voice Response (IRV)-based banking and health systems.
- Applying audio signatures for digital documents.
- In entertainment and emergency services.
- In online education systems.

6. MULTIMODAL BIOMETRIC SYSTEMS

All the biometric systems we discussed till now were unimodal, which take single source of information for authentication. As the name depicts, multimodal biometric systems work on accepting information from two or more biometric inputs.

A multimodal biometric system increases the scope and variety of input information the system takes from the users for authentication.

Why Multimodal Biometrics is Required?

The unimodal systems have to deal with various challenges such as lack of secrecy, non-universality of samples, extent of user's comfort and freedom while dealing with the system, spoofing attacks on stored data, etc.

Some of these challenges can be addressed by employing a multimodal biometric system.

There are several more reasons for its requirement, such as:

1. Availability of multiple traits makes the multimodal system more reliable.

2. A multimodal biometric system increases security and secrecy of user data.

3. A multimodal biometric system conducts fusion strategies to combine decisions from each subsystem and then comes up with a conclusion. This makes a multimodal system more accurate.

4. If any of the identifiers fail to work for known or unknown reasons, the system still can provide security by employing the other identifier.

5. Multimodal systems can provide knowledge about "liveliness" of the sample being entered by applying liveliness detection techniques. This makes them capable to detect and handle spoofing.

Working of Multimodal Biometric System

Multimodal biometric system has all the conventional modules a unimodal system has:

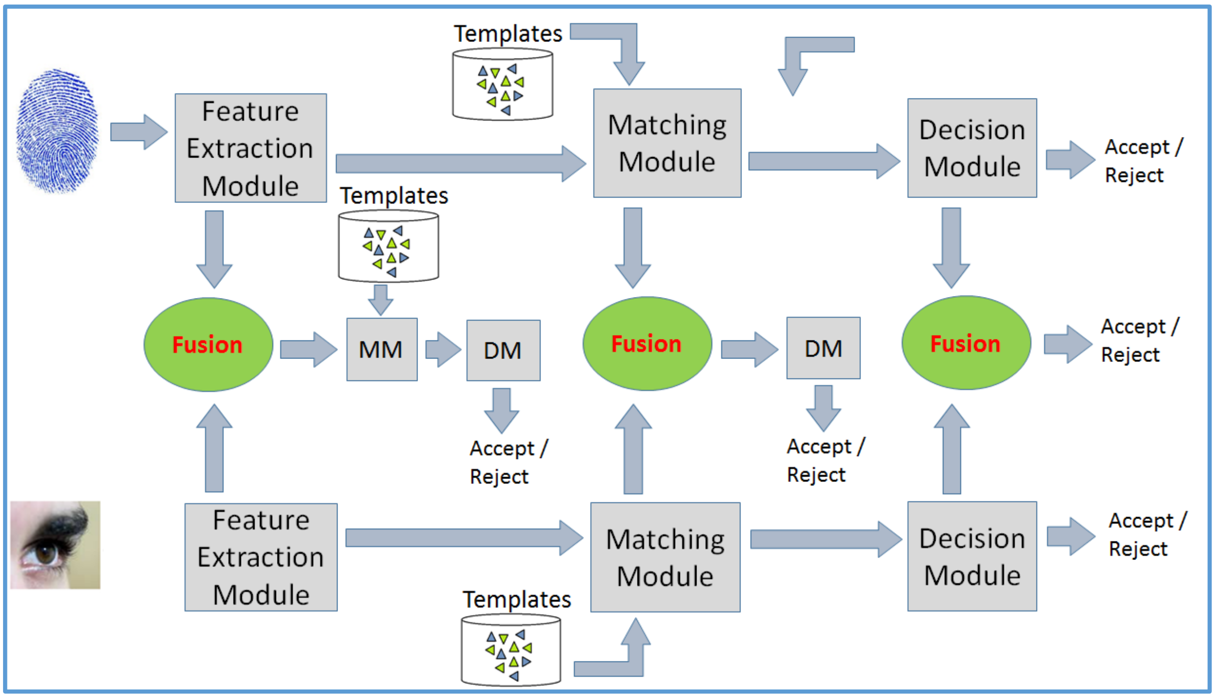
1. Capturing module
2. Feature extraction module
3. Comparison module
4. Decision making module

In addition, it has a fusion technique to integrate the information from two different authentication systems. The fusion can be done at any of the following levels:

1. During feature extraction.

2. During comparison of live samples with stored biometric templates.

3. During decision making.



The multimodal biometric systems that integrate or fuse the information at initial stage are considered to be more effective than the systems those integrate the information at the later stages. The obvious reason to this is, the early stage contains more accurate information than the matching scores of the comparison modules.

Fusion Scenarios in Multimodal Biometric System

Within a multimodal biometric system, there can be variety in number of traits and components. They can be as follows:

- Single biometric trait, multiple sensors.

- Single biometric trait, multiple classifiers (say, minutiae-based matcher and texture-based matcher).

- Single biometric trait, multiple units (say, multiple fingers).

- Multiple biometric traits of an individual (say, iris, fingerprint, etc.).

These traits are then operated upon to confirm user’s identity.

Design Issues with Multimodal Biometric Systems

You need to consider a number of factors while designing a multimodal biometric system:

- Level of security you need to bring in.
- The number of users who will use the system.
- Types of biometric traits you need to acquire.
- The number of biometric traits from the users.
- The level at which multiple biometric traits need integration.
- The technique to be adopted to integrate the information.
- The trade-off between development cost versus system performance.

7. BIOMETRIC MODALITY SELECTION

To be able to select a proper biometric system, you need to compare them on various aspects. You need to assess the suitability of the systems to your requirements in terms of convenience, system specifications and performance, and your budget.

You can select best suitable biometric system by studying various criteria for their effectiveness.

Criteria for Effective Biometric System

There are seven basic criteria for measuring effectiveness of a biometric system:

- **Uniqueness:** It determines how uniquely a biometric system can recognize a user from a group of users. It is a primary criterion.
- **Universality:** It indicates requirement for unique characteristics of each person in the world, which cannot be reproduced. It is a secondary criterion.
- **Permanence:** It indicates that a personal trait recorded needs to be constant in the database for a certain time period.
- **Collectability:** It is the ease at which a person's trait can be acquired, measured, or processed further.
- **Performance:** It is the efficiency of system in terms of accuracy, speed, fault handling, and robustness.
- **Acceptability:** It is the user-friendliness, or how good the users accept the technology such that they are cooperative to let their biometric trait captured and assessed.
- **Circumvention:** It is the ease with which a trait is possibly imitated using an artifact or substitute.

Comparison of Various Biometric Modalities

Let us compare all the biometric system in the following terms:

Biometric Characteristic	Univers ality	Uniquen ess	Perman ence	Collect-Ability	Perform ance	Accept-ability	Circum-vention
Finger Print	Medium	High	High	Medium	High	Medium	High
Face Recognition	High	Low	Medium	High	Low	High	Low
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Mediu m
Iris Recognition	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
DNA	High	High	Medium	High	High	Low	Low
Keystroke	High	Low	Low	High	Medium	High	High
Signature	Low	Low	Low	High	Low	High	Low
Voice	Medium	Low	Low	Medium	Low	High	Low

You can select an appropriate biometric system depending upon the criteria you need to deal with as shown in the table.

8. BIOMETRIC SYSTEM PERFORMANCE

Biometric system manufacturers claim high system performance which is practically difficult to achieve in actual operating environments. The possible reasons are, tests conducted in controlled environment setups, limitations on hardware, etc.

For example, a voice recognition system can work efficiently only in quiet environment, a facial recognition system can work fine if lighting conditions are controlled, and candidates can be trained to clean and place their fingers properly on the fingerprint scanners.

However, in practice, such ideal conditions may not be available in the target operating environment.

Performance Measurements

The performance measurements of a biometric system are closely tied to False Reject Rate (FRR) and False Accept Rate (FAR).

FRR is also known as **Type-I error** or False Non Match Rate (FNMR) which states the likelihood of a legitimate user being rejected by the system.

FAR is referred to as **Type-II error** or False Match Rate (FMR) which states the likelihood of a false identity claim being accepted by the system.

An ideal biometric system is expected to produce zero value for both FAR and FRR. Means it should accept all genuine users and reject all fake identity claims, which is practically not achievable.

FAR and **FRR** are inversely proportional to each other. If FAR is improved, then the FRR declines. A biometric system providing **high FRR ensures high security**. If the FRR is too high, then the system requires to enter the live sample a number of times, which makes it less efficient.

The performance of current biometrics technologies is far from the ideal. Hence the system developers need to keep a good balance between these two factors depending on the security requirements.

9. PATTERN RECOGNITION AND BIOMETRICS

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern **class**.

Pattern recognition is the science for observing, distinguishing the patterns of interest, and making correct decisions about the patterns or pattern classes. Thus, a biometric system applies pattern recognition to identify and classify the individuals, by comparing it with the stored templates.

Pattern Recognition in Biometrics

The pattern recognition technique conducts the following tasks:

- **Classification**: Identifying handwritten characters, CAPTCHAs, distinguishing humans from computers.
- **Segmentation**: Detecting text regions or face regions in images.
- **Syntactic Pattern Recognition:** Determining how a group of math symbols or operators are related, and how they form a meaningful expression.

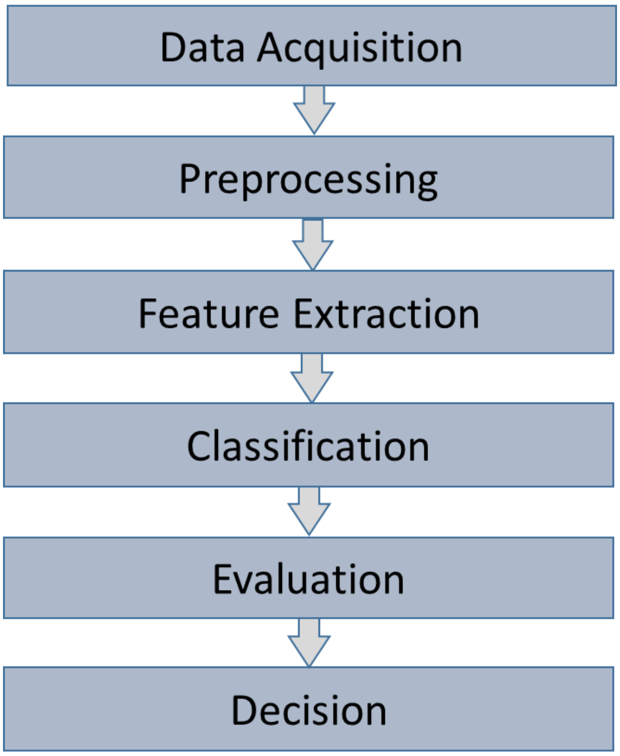
The following table highlights the role of pattern recognition in biometrics:

Pattern Recognition Task	Input	Output
Character Recognition (Signature Recognition)	Optical signals or Strokes	Name of the character
Speaker Recognition	Voice	Identity of the speaker
Fingerprint, Facial image, hand geometry image	Image	Identity of the user

Components of Pattern Recognition

Pattern recognition technique extracts a random pattern of human trait into a compact digital signature, which can serve as a biological identifier. The biometric systems use pattern recognition techniques to classify the users and identify them separately.

The components of pattern recognition are as follows:



Popular Algorithms in Pattern Recognition

The most popular pattern generation algorithms are:

Nearest Neighbor Algorithm

You need to take the unknown individual’s vector and compute its distance from all the patterns in the database. The smallest distance gives the best match.

Back-Propagation (Backprop) Algorithm

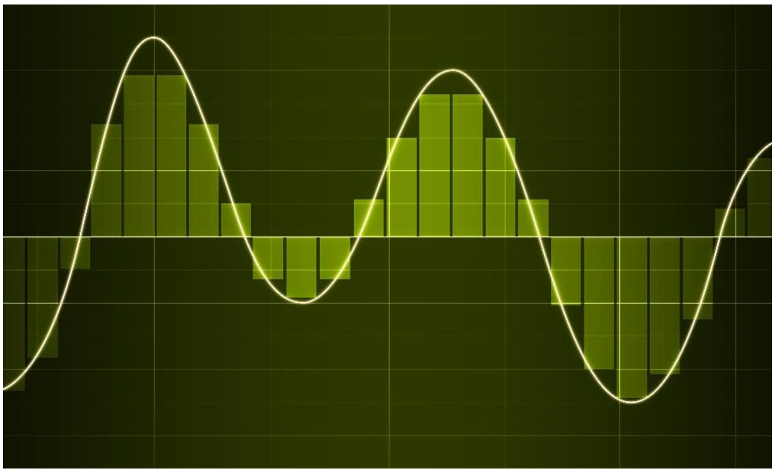
It is a bit complex but very useful algorithm that involves a lot of mathematical computations.

10. SIGNAL PROCESSING AND BIOMETRICS

There are various signals we can get in the real world such as sound, light, radio signals, biomedical signals from human body, etc. All these signals are in the form of a continuous stream of information, called analog signals. Human voice is a kind of signal we get from the real world and use as biometric input.

What is a Signal?

A signal is a measurable physical quantity containing some information, which can be conveyed, displayed, recorded, or modified.



Signal Processing in Biometrics

There are various reasons for processing signals. The biometric systems, require voice processing for various reasons:

- To extract meaningful information from the candidate's sample.
- To remove noise from the sample.
- To make the sample transmittable.
- To remove distortion of sample.

The analog signal processing module converts real world information such as sound wave in the form of 0s and 1s to make it understandable and usable by the contemporary digital systems such as biometric systems. The keystrokes, hand geometry, signature, and speech fall into the domains of signal processing and pattern recognition.

Digital Signal Processing Systems (DSPs)

There are two types of signals: **analog** and **digital**. The analog signals are uninterrupted, continuous stream of information whereas digital signal is a stream of 0s and 1s.

DSP systems are one of the important components of biometric systems, which convert analog signals into a stream of discrete digital values by sampling and digitizing using an Analog-to-Digital Converter (ADC).

DSPs are single-chip digital microcomputers, which process electrical signals generated by electronic sensors from cameras, fingerprint sensors, microphones, etc.

DSP in Biometrics

A DSP allows the biometric system to be small and easily portable, to perform efficiently and to be overall less costly.

The DSP architecture is built to support complex mathematical algorithms that involve a significant amount of multiplication and addition. The DSP can execute multiply/add in a single cycle with the help of the multiply/accumulate (MAC) hardware inside its Arithmetic Logic Unit (ALU).

It can also enhance the resolution of the captured image with the use of two-dimensional Fast Fourier Transforms (FFT) and finite IR filters.

11. BIOMETRICS AND IMAGE PROCESSING

Images have a huge share in this era of information. In biometrics, image processing is required for identifying an individual whose biometric image is stored in the database previously. Faces, fingerprints, irises, etc., are image-based biometrics, which require image processing and pattern recognition techniques.

For an image based biometric system to work accurately, it needs to have the sample image of user's biometric in a very clear and non-adulterated form.

Requirement of Image Processing in Biometrics

The image of user's biometric is fed into the biometric system. The system is programmed to manipulate the image using equations, and then store the results of the computation for each pixel.

To selectively enhance certain fine features in the data and to remove certain noise, the digital data is subjected to various image processing operations.

Image processing methods can be grouped into three functional categories:

Image Restoration

Image restoration mainly includes:

- Reducing noise introduced in the image at the time of acquiring sample.
- Removing distortions appeared during enrollment of biometric.

Image smoothing reduces noise in the image. Smoothing is carried out by replacing each pixel by the average value with the neighboring pixel. The biometric system uses various filtering algorithms and noise reduction techniques such as Median Filtering, Adaptive Filtering, Statistical Histogram, Wavelet Transforms, etc.

Image Enhancement

Image enhancement techniques improve the visibility of any portion or feature of the image and suppress the information in other parts. It is done only after restoration is completed. It includes brightening, sharpening, adjusting contrast, etc., so that the image is usable for further processing.

Feature Extraction

Two types of features are extracted from image, namely:

- **General features**

  The features such as shape, texture, color, etc., which are used to describe content of the image.

- **Domain-specific features**

  They are application dependent features such as face, iris, fingerprint, etc. Gabor filters are used to extract features.

When the features are extracted from the image, you need to choose a suitable classifier. The widely used classifier **Nearest Neighbor classifier**, which compares the feature vector of the candidate image with the vector of the image stored in the database.

B-Splines are approximations applied to describe curve patterns in fingerprint biometric systems. The coefficients of B-Splines are used as features. In case of iris recognition system, the images of iris are decomposed using Discrete Wavelet Transform (DWT) and the DWT coefficients are then used as features.

12. BIOMETRIC SYSTEM SECURITY

The operations of a biometric system depend heavily on the input devices that are subjected to operational limitations. At times, the devices themselves may fail to capture the necessary input samples. They may not capture the sample sufficiently. This makes the system unreliable and vulnerable.

The more vulnerable a biometric system is, the more insecure it is.

Biometric System Vulnerability

There are the two major causes of biometric system vulnerability:

System Failures

There are two ways in which a biometric system can fail to work:

- **Intrinsic failures** – They are failures such as non-working sensors, failure of feature extraction, matching, or decision making modules, etc.

- **Failures due to attacks –** They are due to loopholes in the biometric system design, availability of any computations to the attackers, insider attacks from unethical system administrators, etc.

Non-secure Infrastructure

The biometric system can be accessible to malicious users if its hardware, software, and user data are not safeguarded.

Risks with Biometric System Security

The security of a biometric system is important as the biometric data is not easy to revoke or replace. There are following prominent risks regarding security of biometric systems:

Risk of User Data Being Stolen

If the biometric system is vulnerable, the hacker can breach the security of it and collect the user data recorded in the database. It creates more hazards to privacy.

Risk of User Data Getting Compromised

After acquiring the biometric sample, the hacker can present a fake sample to the system. If user data is compromised, it remains compromised forever. The obvious reason is, user has only a limited number of biometrics and they are difficult to replace, unlike passwords or ID cards.

Though biometric data is encrypted and stored, it needs to be decrypted for matching purpose. At the time of matching a hacker may breach the security.

Biometric System Security

A number of solutions are proposed to address the biometric system security issue. Biometric templates are never stored in the raw form. They are encrypted; sometimes even twice.

In the case of biometrics, there are various resources involved such as humans (subjects or candidates), entities (system components or processes), and biometric data (information). The security requirements of **confidentiality**, **integrity**, **authenticity**, **non-repudiation**, and **availability** are essential in biometrics. Let us go through them briefly:

Authenticity

It is the quality or the state of being pure, genuine, or original, rather than being reproduced. Information is authentic when it is in the same state and quality when it was created, stored, or transferred.

There are two authenticities in a biometric system - **entity authenticity** and **data origin authenticity**. Entity authenticity confirms that all entities involved in the overall processing are the ones they claim to be. Data origin authenticity ensures genuineness and originality of data. For example, the biometrics data is captured with sensor devices. The captured data that came from a genuine sensor is not spoofed from a previous recording.

Confidentiality

It is limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized people. In cases of a biometric system, it mainly refers to biometric and related authentication information when it is captured and stored, which needs to be kept secret from unauthorized entities.

The biometric information should only be accessible completely to the person it belongs. During identification and variation, the accessing candidate needs to be restricted with appropriate security measures.

Integrity

It is the condition of being complete and unaltered that refers to its consistency, accuracy, and correctness. For a biometric system, the integrity should be high. Any malicious manipulations during operation and storage should be kept away or detected earliest by including its notification and correction.

Non-repudiation

It is identification of involved resources such as entities and components. It is also seen as accountability. For example, it prohibits a sender or a recipient of biometric information from denying having sent or received biometric information.

Availability

A resource has the property of availability with respect to a set of entities if all members of the set can access the resource. An aspect called **reachability** ensures that the humans or system processes either can or cannot be contacted, depending on user interests.

Attackers can make the system unusable for genuine users, thus preventing them from using authenticated applications. These attackers target the availability of the information.

Criteria for Generating Biometric Templates

Here are the criteria for generating biometric templates:

1. Ensuring that the template comes from a human candidate and is captured by a genuine sensor and software.

2. Securing a biometric template by encryption with irreversibility properties. This makes it difficult for hackers to compute the original biometric information from secure template.

3. Creating an **unlikable (unique)** biometric template. A biometric system should not be able to access the template of the same candidate recorded into another biometric system. In case if a hacker manages to retrieve a biometric template from one biometric system, he should not be able to use this template to gain access through another biometric system even though both verifications may be based on the same biometric template of the candidate. Further, an unlinkable biometric system should make it impossible to derive any information based on the relation between two templates.

4. Creating a **cancellable** and **renewable** template. It emphasizes on the ability to cancel or deactivate the compromised template and reproduce another one, in a similar manner that a lost or stolen smartcard can be reproduced.

5. The ‘renewable’ and ‘unlinkable’ characteristics are achieved through **salting techniques.** Salting adds randomly generated unique data known as ‘salt’ to the original information to make it distinct from the others.

6. Designing a biometric system accuracy with respect to both FAR and FRR.

7. Selecting a suitable encryption algorithm carefully. Some algorithms may amplify even small variations inherent in an individual’s biometric data, which can lead to higher FRR.

8. Using an important encryption technique such as **hashing method,** which is effective when a different permutation is applied with each template generation. Different permutations ensure the uniqueness of each template despite using the same input biometric data.

9. Employing an effective protection scheme to elevate the **performance** of the system.

A lot of research and development is being done towards the security and privacy of biometric data.