18CSE357E- BIOMETRICS

Elective
Academic Year 2023-2024 (ODD Semester)

Dr. M.K.VIDHYALAKSHMI
Assistant Professor/CTech

Mobile: 9443223066
Email: vidhyalm1@srmist.edu.in
Room: BEL 404 Lab

Course Outcomes (Cos):

The purpose of learning this course is to

- Understand the concept of Authentication using Biometrics
- Get knowledge on the basics of Biometric traits, Sensors and Data Acquition
- Get knowledge on design of Biometric Security Systems
- Introduce various feature extraction and matching techniques for different Biological traits
- Understand the real-time applications of Biometrics

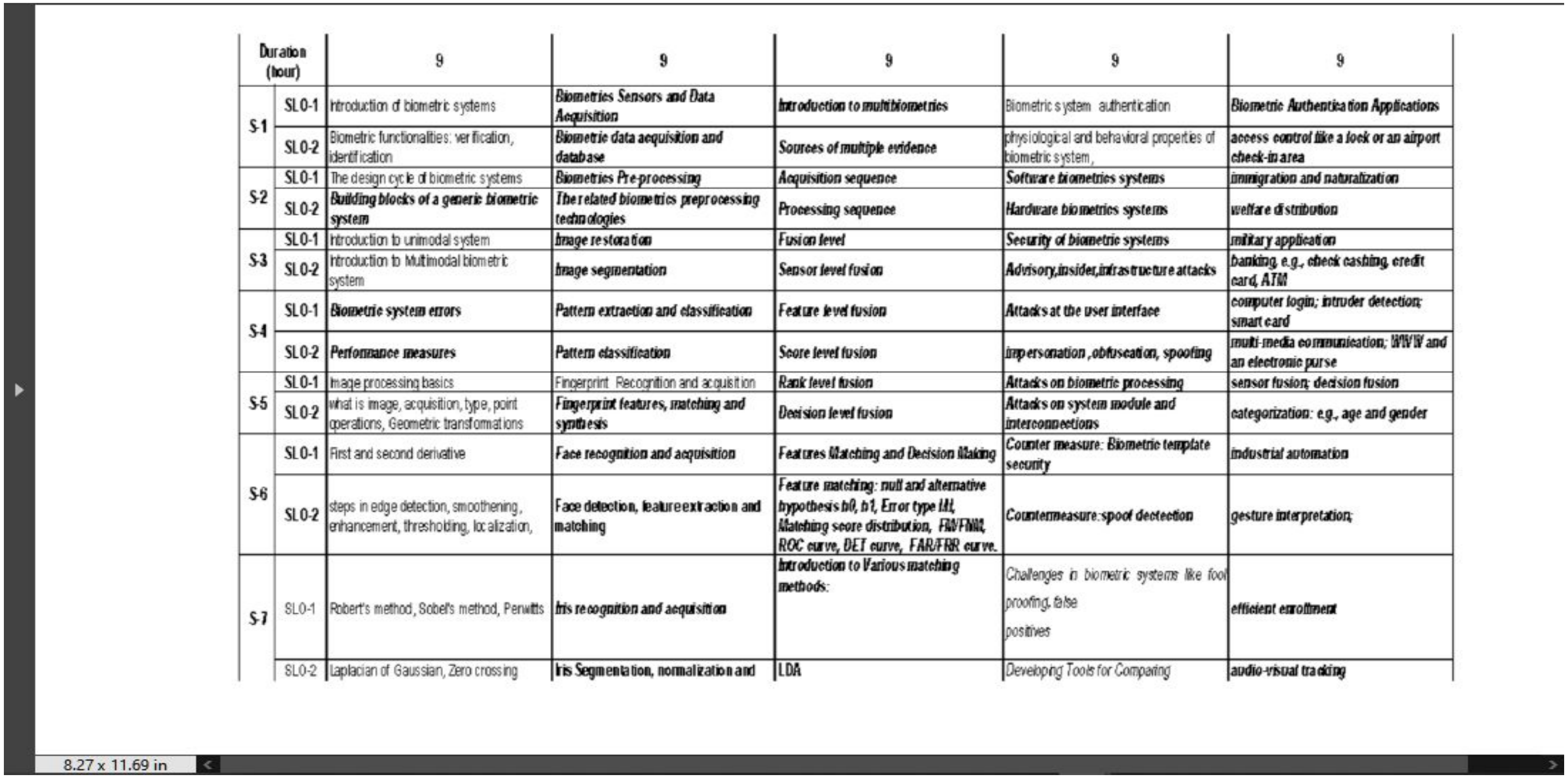
Learning Outcomes

At the end of this course, learners will be able to:

- *Acquire the knowledge on various biometric traits*
- *Acquire the ability to identify pattern recognition system and its features*
- *Understand the basic ideas about physical and behavioral biometric traits*
- *Apply the knowledge of biometrics on developing identification system.*
- *Apply the knowledge for designing biometric systems*
- *Acquire the knowledge on authentication systems for real time security applications*

Learning Resources

- **GCR Details**
  - Class Code:



Duration (hour)		9	9	9	9	9
S-1	SLO-1	Introduction of biometric systems	Biometrics Sensors and Data Acquisition	Introduction to multibiometrics	Biometric system authentication	Biometric Authentication Applications
	SLO-2	Biometric functionalities: verification, identification	Biometric data acquisition and database	Sources of multiple evidence	physiological and behavioral properties of biometric system,	access control like a lock or an airport check-in area
S-2	SLO-1	The design cycle of biometric systems	Biometrics Pre-processing	Acquisition sequence	Software biometrics systems	immigration and naturalization
	SLO-2	Building blocks of a generic biometric system	The related biometrics preprocessing technologies	Processing sequence	Hardware biometrics systems	welfare distribution
S-3	SLO-1	Introduction to unimodal system	Image restoration	Fusion level	Security of biometric systems	military application
	SLO-2	Introduction to Multimodal biometric system	Image segmentation	Sensor level fusion	Advisory,insider,infrastructure attacks	banking, e.g., check cashing, credit card, ATM
S-4	SLO-1	Biometric system errors	Pattern extraction and classification	Feature level fusion	Attacks at the user interface	computer login; intruder detection; smart card
	SLO-2	Performance measures	Pattern classification	Score level fusion	impersonation ,obfuscation, spoofing	multi-media communication; WWW and an electronic purse
S-5	SLO-1	Image processing basics	Fingerprint Recognition and acquisition	Rank level fusion	Attacks on biometric processing	sensor fusion; decision fusion
	SLO-2	what is image, acquisition, type, point operations, Geometric transformations	Fingerprint features, matching and synthesis	Decision level fusion	Attacks on system module and interconnections	categorization: e.g., age and gender
S-6	SLO-1	First and second derivative	Face recognition and acquisition	Features Matching and Decision Making	Counter measure: Biometric template security	industrial automation
	SLO-2	steps in edge detection, smoothening, enhancement, thresholding, localization,	Face detection, feature extraction and matching	Feature matching: null and alternative hypothesis h0, h1, Error type I,II, Matching score distribution, FM/FNM, ROC curve, DET curve, FAR/FRR curve.	Countermeasure:spoof dectection	gesture interpretation;
S-7	SLO-1	Robert's method, Sobel's method, Perwitts	Iris recognition and acquisition	Introduction to Various matching methods:	Challenges in biometric systems like fool proofing, false positives	efficient enrollment
	SLO-2	Laplacian of Gaussian, Zero crossing	Iris Segmentation, normalization and	LDA	Developing Tools for Comparing	audio-visual tracking

Learning Resources

Reference Books

- **Introduction to Biometrics** – James Wayman, - Springer
- **Feature Extraction and Image Processing for Computer Vision** – Mark S Necon – Elsevir
- **Digital Image Processing using Mtalab** – Rafael C, - Tata MC Graw Hill
- **Guide to Biometrics** – Rood M Bolie –Springer
- **Pattern Classification** – Richard Oduda – Wiley
- **Biometrics in Identity Management: Concepts to Applications** – Shimon K Modi

UNIT – I Contents

- Introduction to Biometric Systems
- Biometric Functionalities :Verification and Identification
- The Design Cycle of Biometric Systems
- Introduction to Unimodel Systems
- Introduction to multi-model Biometric Systems
- Biometric System Errors & Performance Measures

UNIT – I Contents

- Image Processing Basics
- First & Second Derivatives
- Steps in Edge Detection, Smoothing, enhancement, etc
- Robert's method, Sobel's method and Perwits Method
- Laplacian of Gaussian, Zero Crossing
- Low Level Feature Extraction, Describing Image Motion
- High Level Feature Extraction, Template Matching
- Hough Transforms for Lines, Circles and Ellipses

Session – 1 & 2

- **Introduction to Biometric Systems**
  - Biometric Functionalities :Verification and Identification
- **The design cycle of biometric systems**
  - The building blocks of generic biometric systems

Introduction to Biometric Systems

SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

Introduction to Biometric Systems

- What does biometrics mean?
- Why biometrics?
- What is biometrics used for
- What are the types of biometrics?
- Who invented biometrics? (History of biometrics)
- Is biometrics accurate and reliable

Introduction to Biometric Systems

- **Biometrics** can be defined as the means of identifying and authenticating individuals in a reliable and fast way through **unique biological characteristics**.
- It is the science of establishing the **identity** of an individual based on the physical, chemical or behavioural attributes of the person.
- Biometrics allows a person to be **identified** and **authenticated** based on recognizable and verifiable data, unique and specific.

Why Biometrics?

- **Needs**: For large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications
- The proliferation of web-based services (e.g., online banking)
- The deployment of decentralized customer service centres (e.g., credit cards)
- The main aim is to prevent impostors from accessing protected resources

History of Biometrics

- In the second century B.C., the Chinese emperor Ts'In was a authenticating specific seals with a fingerprint.
- Fingerprints were first used in a commercial setting in 1858 by William James Herschel, a British administrator in India. Having been put in charge of building roads in Bengal, he had his subcontractors sign contracts with their fingers.
- At the end of the 19th century, Bertillon, a French police officer, took the first steps in scientific policing.
- He used physical measurements of specific anatomical characteristics to identify reoffending criminals

Types of Biometrics

There are two types of biometrics:

#1. **Physiological measurements**

- They can be either **morphological** or **biological**.
- **Morphological** identifiers mainly consist of fingerprints, the hand's shape, the finger, vein pattern, the eye (iris and retina), and the face's shape.
- For **biological** analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics.

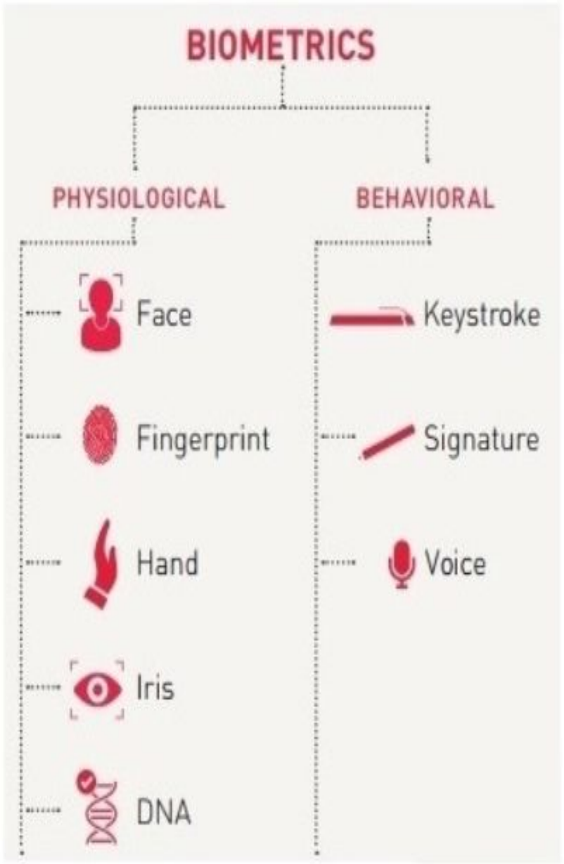
Types of Biometrics

#2. **Behavioral measurements**

The most common are:

- voice recognition,
- signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination),
- keystroke dynamics,
- the way we use objects,
- gait, the sound of steps,
- gestures, etc.

Types of Biometrics



Traditional Methods and Biometrics

- **Traditional methods** of establishing a person's identity
  - Knowledge- based (e.g., passwords) and
  - Token-based (e.g., ID cards) mechanisms
- **Drawbacks**: Representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security.
- **Dual-factor Authentication Scheme:**
- Biometrics is used to supplement ID cards and passwords thereby imparting an additional level of security.

Biometrics for Identity

Person Recognition in Identity Management

- The aim is to establish the association between an individual and his personal identity.
- One must be able to determine a person’s identity or verify the identity claim of an individual whenever required
- This process is known as **person recognition**.
- A person can be recognized based on

  (a) what he knows,

  (b) what he possesses extrinsically, and

  (c) who he is intrinsically (biometric recognition)

Biometrics for Identity

- The three different types of authentication
  - *Something you know* [**knowledge based system**]
    - password, PIN

  - *Something you have* [**token based system**]
    - Card key, smart card

  - *Something you are* **Biometric**

Attacks in Authentication Systems

Various types of Malicious Attacks on Authentication Systems

(a) client attack (e.g. guessing passwords, stealing tokens);

(b) host attack (e.g. accessing plain text ¯le containing passwords);

(c) eavesdropping (e.g. shoulder surfing for passwords);

(d) repudiation (e.g., claiming that token was misplaced);

(e) trojan horse attack (e.g., installation of bogus log-in screen to steal passwords); and

(f) denial of service (e.g., disabling the system by deliberately supplying an incorrect password several times).

Biometric Systems Advantages and Disadvantages

Advantages

- Uniqueness
- No need to remember password and pin
- Cannot be lost, stolen or forgotten
- Difficult to copy, share and distribute
- Person is required to be present for authentication

Disadvantages

- Violation of Privacy
- Need of significant computational resources
- Intra-class variation: Due to change in pose or age
- Vulnerable to spoof attacks

Traits, indicators, identifiers or *modalities*.

Physical/Behavioural Characteristics used in BS

- Fingerprint, face, hand/Finger geometry, iris, retina, signature, gait, palm-print, voice pattern, ear, hand vein, odour or the DNA information of an individual to establish identity
- These **characteristics** are referred to as ***traits*, *indicators*, *identifiers* or *modalities*.**

Traits, indicators, identifiers or *modalities*.

Different Traits

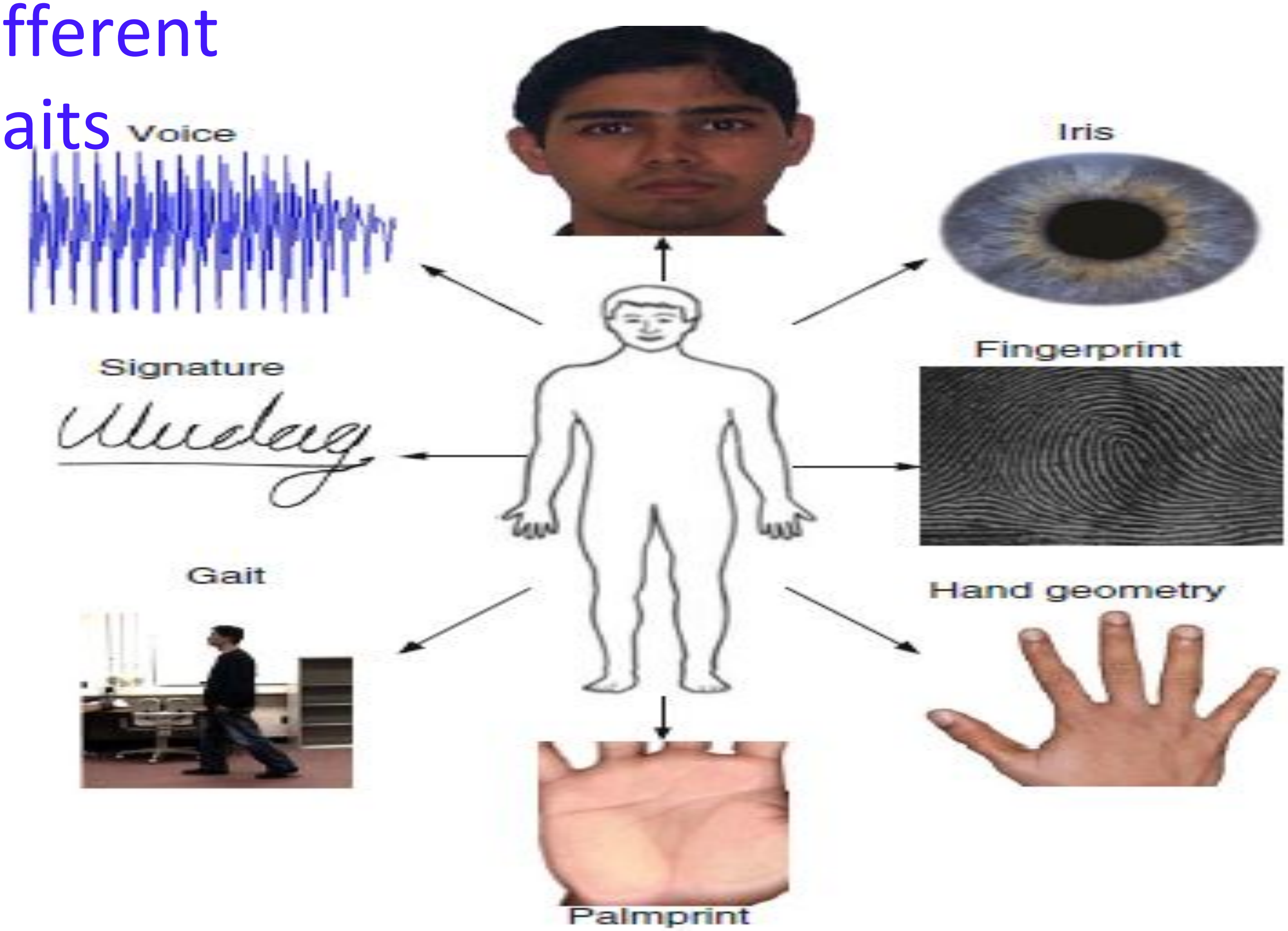


Fig. 1.2 Examples of body traits that have been used for biometric recognition. Physical traits

Operation of a Biometric System

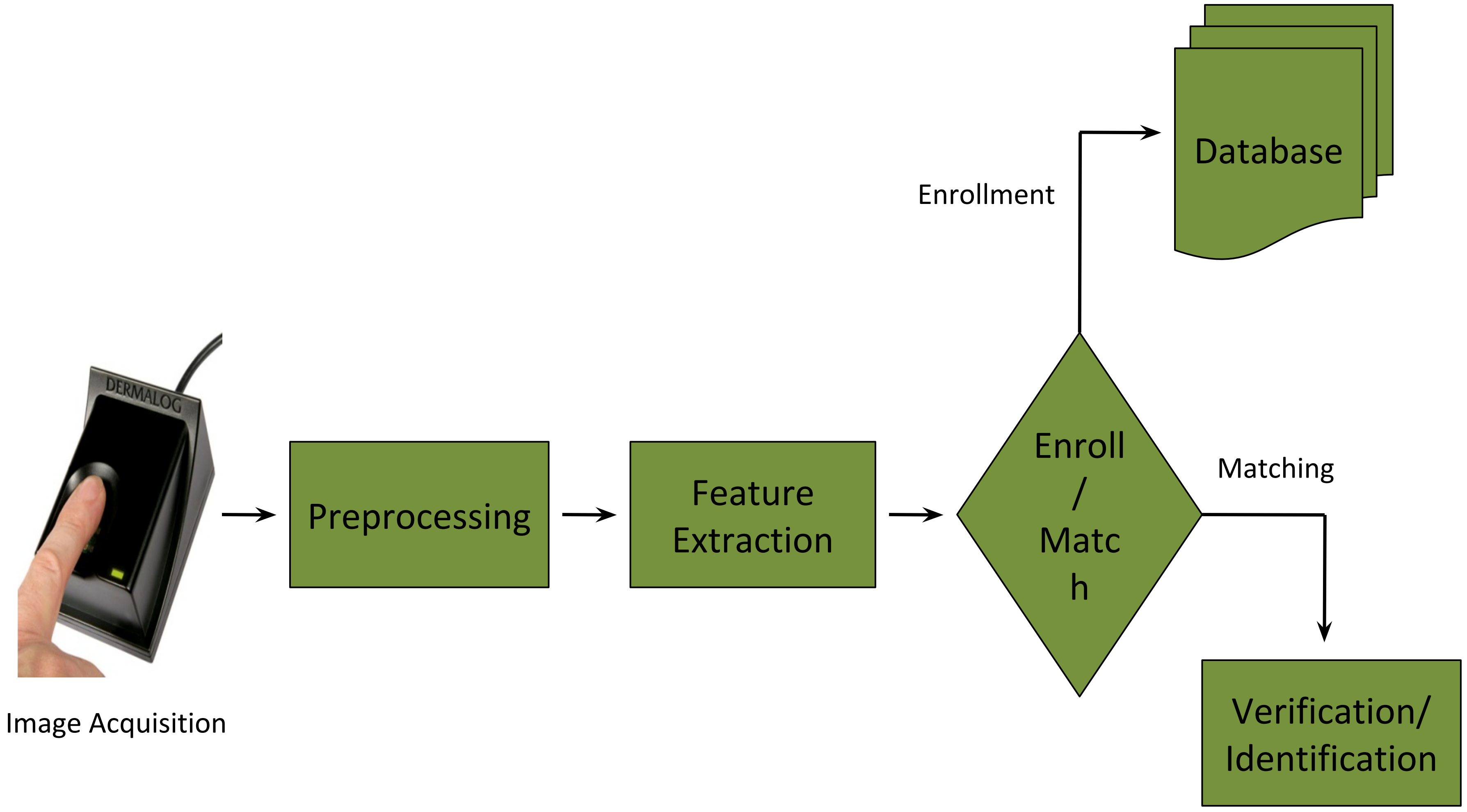
- A **Biometric System** is a **pattern recognition** system that **acquires** biometric data from an individual, **extracts** a salient feature set from the data, **compares** this feature set against the feature set(s) stored in the database, and **executes** an action based on the result of the comparison.

The main modules are

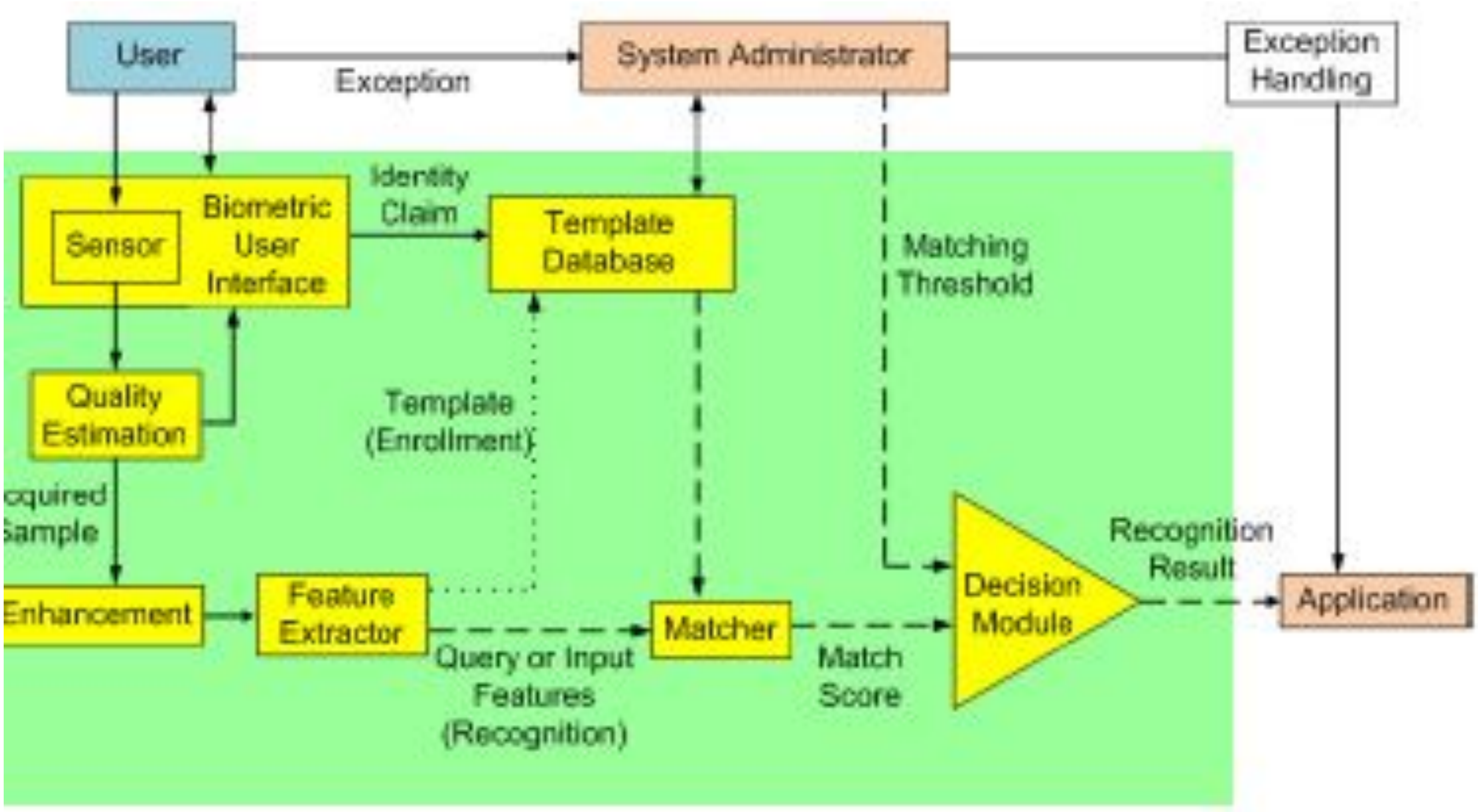
- a sensor module;
- a quality assessment
- feature extraction module;
- a matching module; and
- a database module.

Operation of a Generic Biometric System

A generic **biometric system**



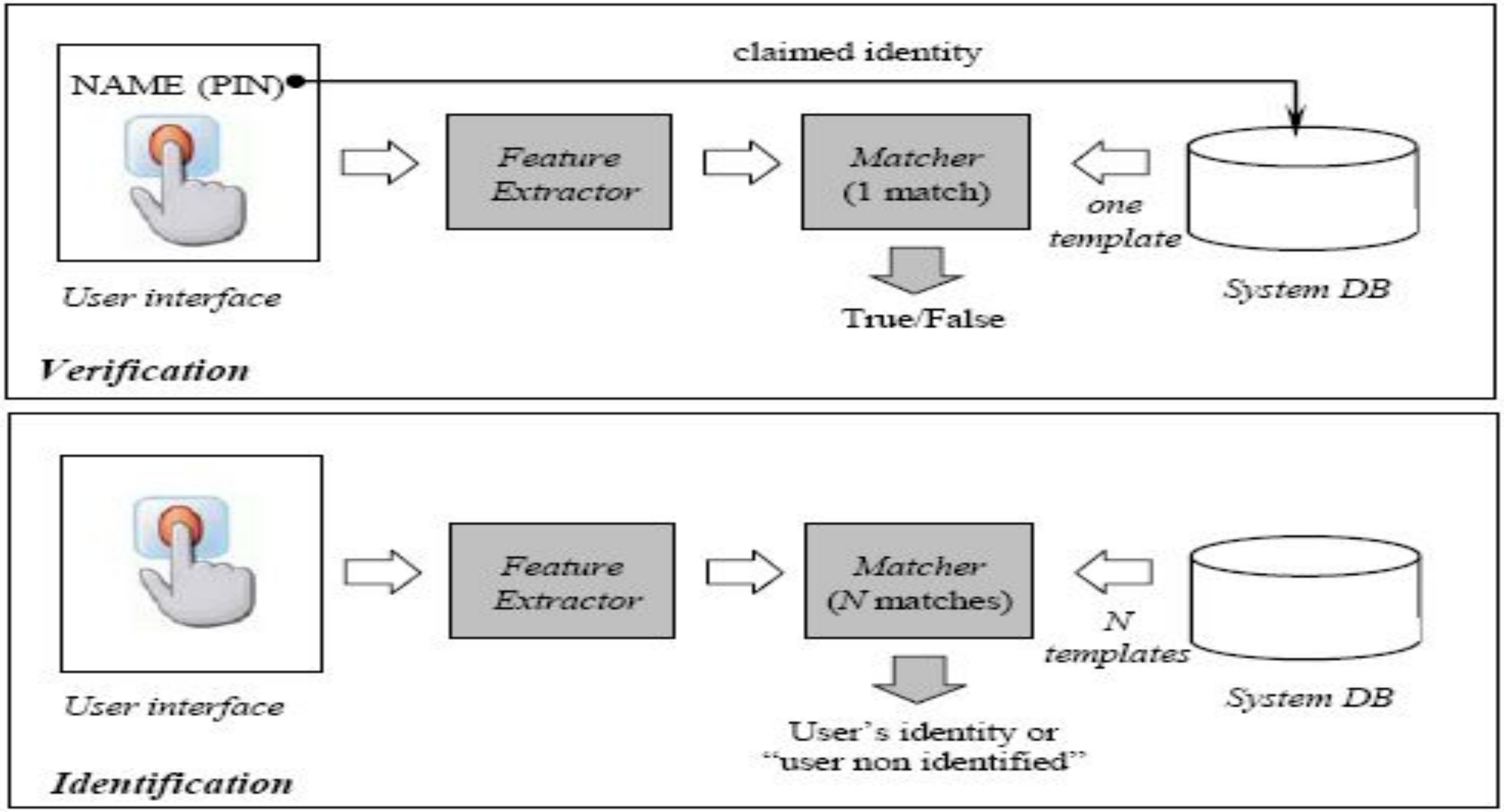
Basic building block of generic Biometric Systems



ig. 1.3 Basic building blocks of a generic biometric system.

Operation of a Biometric System

- Depending upon the application context, system operates in
  - **Verification Mode**: (1:1)
  - **Identification Mode**: (1:N)



Operation of a Biometric System

Verification Mode

- The system validates a **person’s identity** by comparing the captured biometric data with her own biometric template stored system database
- Eg: Does the biometric data belong to Ajay?

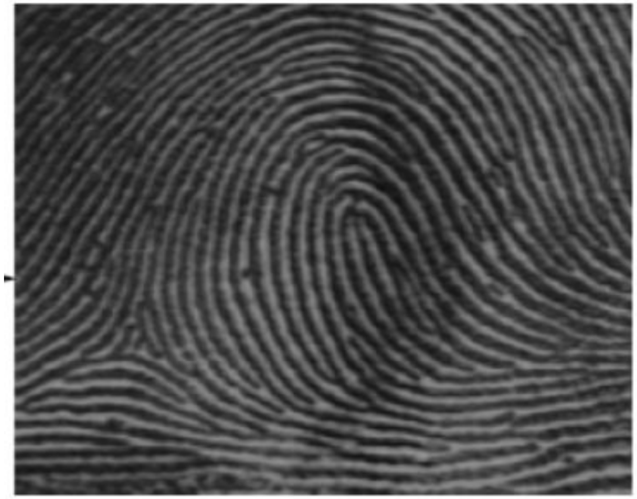
Identification mode

- The system recognizes an individual by searching the template of all the users in the database for a match.
- Eg: whose biometric data is this?

Sensor Module

- A suitable biometric reader or scanner is required to acquire the **raw biometric data** of an individual.
- To obtain Fingerprint images, for example, an optical Fingerprint sensor may be used to get the friction ridge structure of the Fingertip.
- The sensor module defines the ***human machine interface***

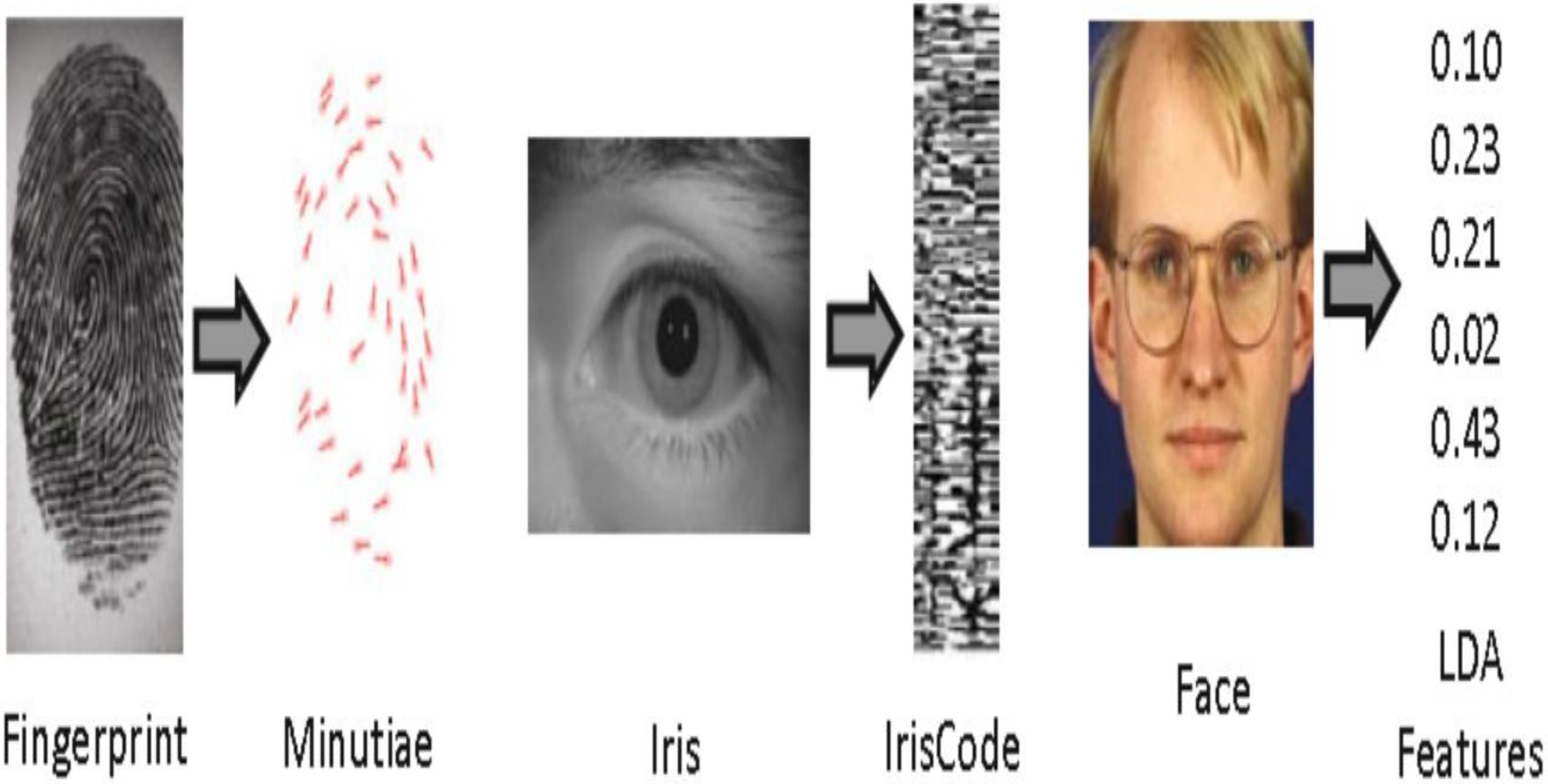
Fingerprint



Quality assessment and feature extraction module

- The sensor data is assessed in order to determine its **suitability** for further processing.
- Typically, the acquired data is **subjected to a signal enhancement algorithm** in order to improve its quality.
- A set of salient discriminatory features are extracted to represent the underlying trait. For example, the **position** and **orientation** of minutia points (local ridge and valley anomalies) in a fingerprint image are extracted by the feature extraction module in a fingerprint-based bio metric system.
- During enrolment, this **feature set** is **stored** in the **database** and is commonly referred to as a ***template***

Quality assessment and feature extraction module



System database module

- The database acts as the repository of bio-metric information.
- Raw biometric sample (i.e., the template) is stored in the database (possibly) along with some biographic information characterizing the user
- Some systems store **multiple templates** in order to account for the intra-class variations associated with a user.
- Face recognition systems, for instance, may store multiple templates of an individual, with each template corresponding to a different facial pose with respect to the camera.

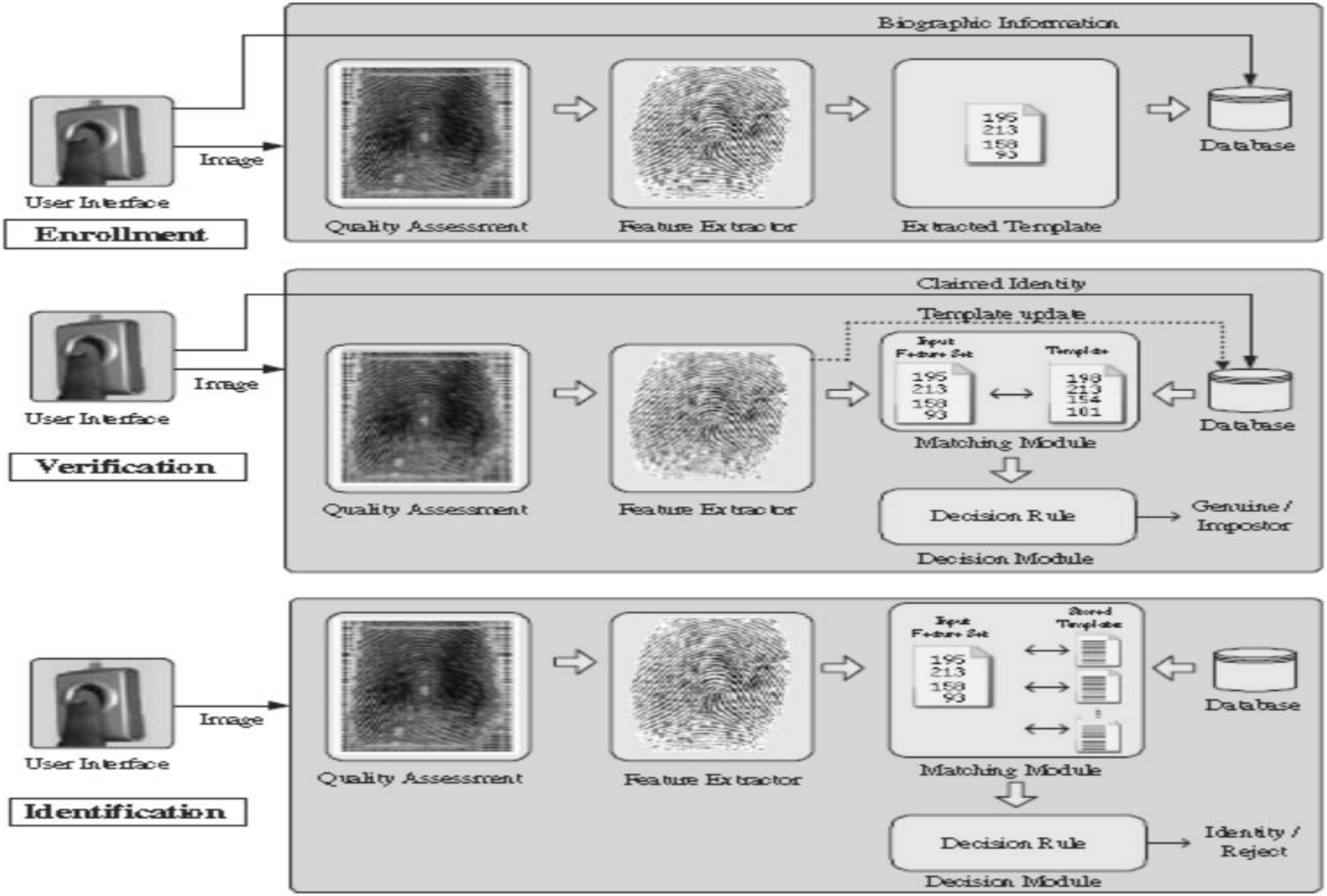
System database module

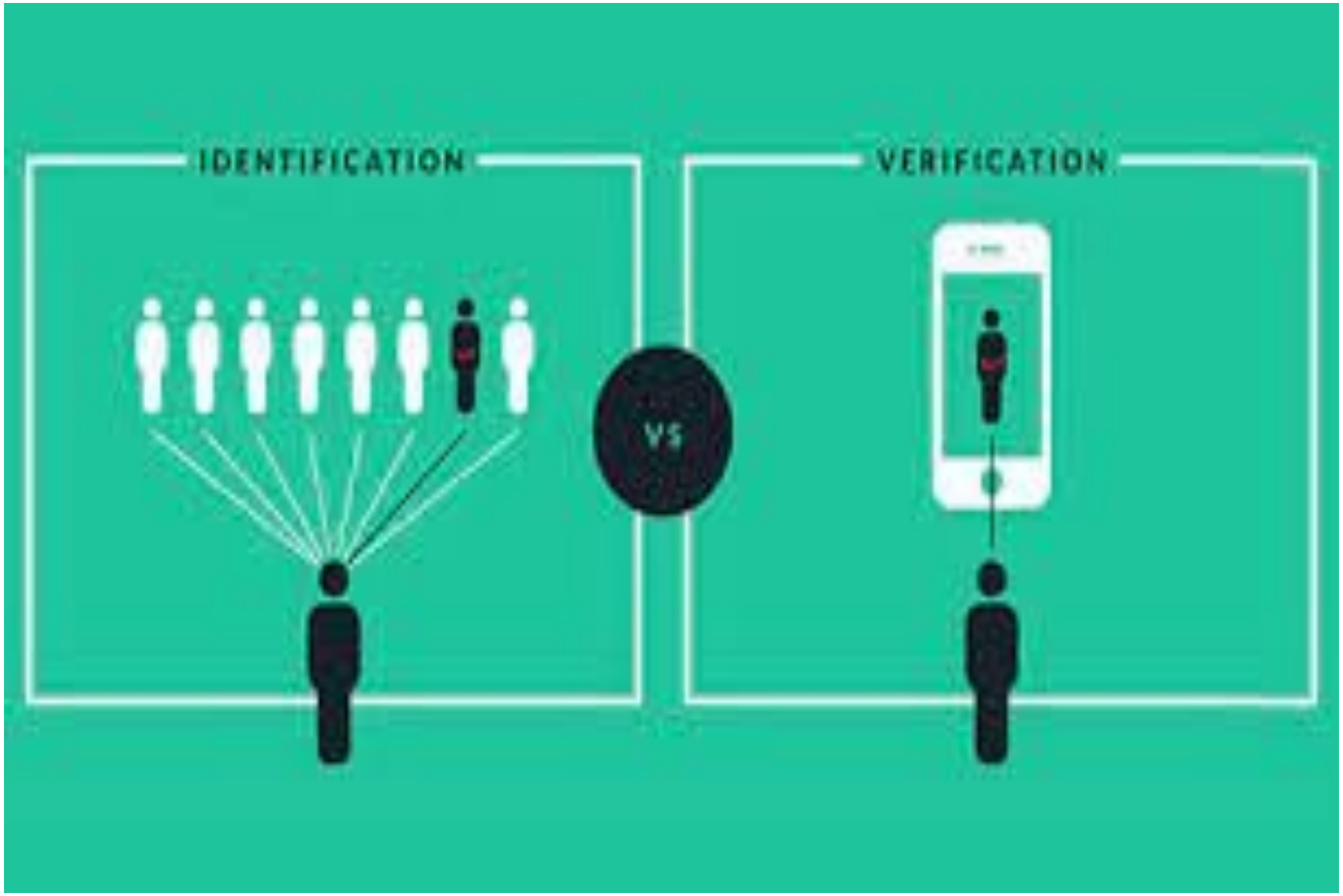
- The raw biometric images may also be stored in the database along with the templates during enrolment. Such images are often known as ***gallery images***, ***reference images***, ***stored images***, or ***enrolment images***.
- The images acquired during recognition are known as ***probe images***, ***query images***, or ***input images***

Matching and Decision-Making Module:

- The extracted features are compared against the stored templates to generate **match scores**.
- In a fingerprint-based biometric system, the number of matching minutiae between the input and the template feature sets is determined and a match score reported.
- The match score may be moderated by the quality of the presented biometric data.
- The **matcher module** also encapsulates a decision making module, in which the match scores are used to either validate a claimed identity or provide a ranking of the enrolled identities in order to identify an individual.

Biometric Functionalities




IDENTIFICATION
VS
VERIFICATION

Biometric Functionalities

- A biometric system can provide two types of identity management functionalities, namely, ***verification*** and ***identification***

Verification

- Here, the user claims an identity and the system verifies whether the claim is genuine, i.e., the system answers the question “Are you who you say you are?”.
- In this scenario, the query is compared only to the template corresponding to the claimed identity (a one-to-one match).
- Verification is typically used in applications where the goal is to **prevent unauthorized persons** from using the services
- Verification as the **two-category classification problem:**
- Given a claimed identity *I* and a query feature set $\mathbf{x}^{A}$, we need to decide if $(I,\mathbf{x}^{A})$ belongs to “genuine” or “impostor” class.

Biometric Functionalities

- Let {I, **x** *Ͼ* } be the stored template corresponding to identity *I*. Typically, $\mathbf{x}^{A}$ is compared with {I, **x** *Ͼ* } and a match score *s*, which measures the similarity between $\mathbf{x}^{A}$ and {I, **x** *Ͼ* } , is computed.
- The decision rule is given by

$$(I, \mathbf{x}^{A}) \in \begin{cases} \text{genuine}, & \text{if } s \geq \eta, \\ \text{impostor}, & \text{if } s < \eta, \end{cases}$$

- where η is a pre-defined threshold
- When the identity claim is deemed to be “genuine”, the user is allowed to access the services provided by the system

Biometric Functionalities

Identification

Biometric identification consists of determining the identity of a person.

- The aim is to capture an item of biometric data from this person. It can be a photo of their face, a record of their voice, or an image of their fingerprint.
- This data is then compared to the biometric data of several other persons kept in a database.

Biometric Functionalities

Identification

- Identification functionality can be further classified into **positive** and **negative** identification.
- In **positive identification**, the user attempts to positively identify himself to the system without explicitly claiming an identity.
- A positive identification system answers the question “Are you someone who is known to the system?” by determining the identity of the user from a **known set of identities**.
- In contrast, the user in a **negative identification** application is considered to be concealing his true identity (either explicitly or implicitly) from the system.
- Negative identification is also known as **screening** and the objective of such systems is to find out “Are you who you say you are not?”.

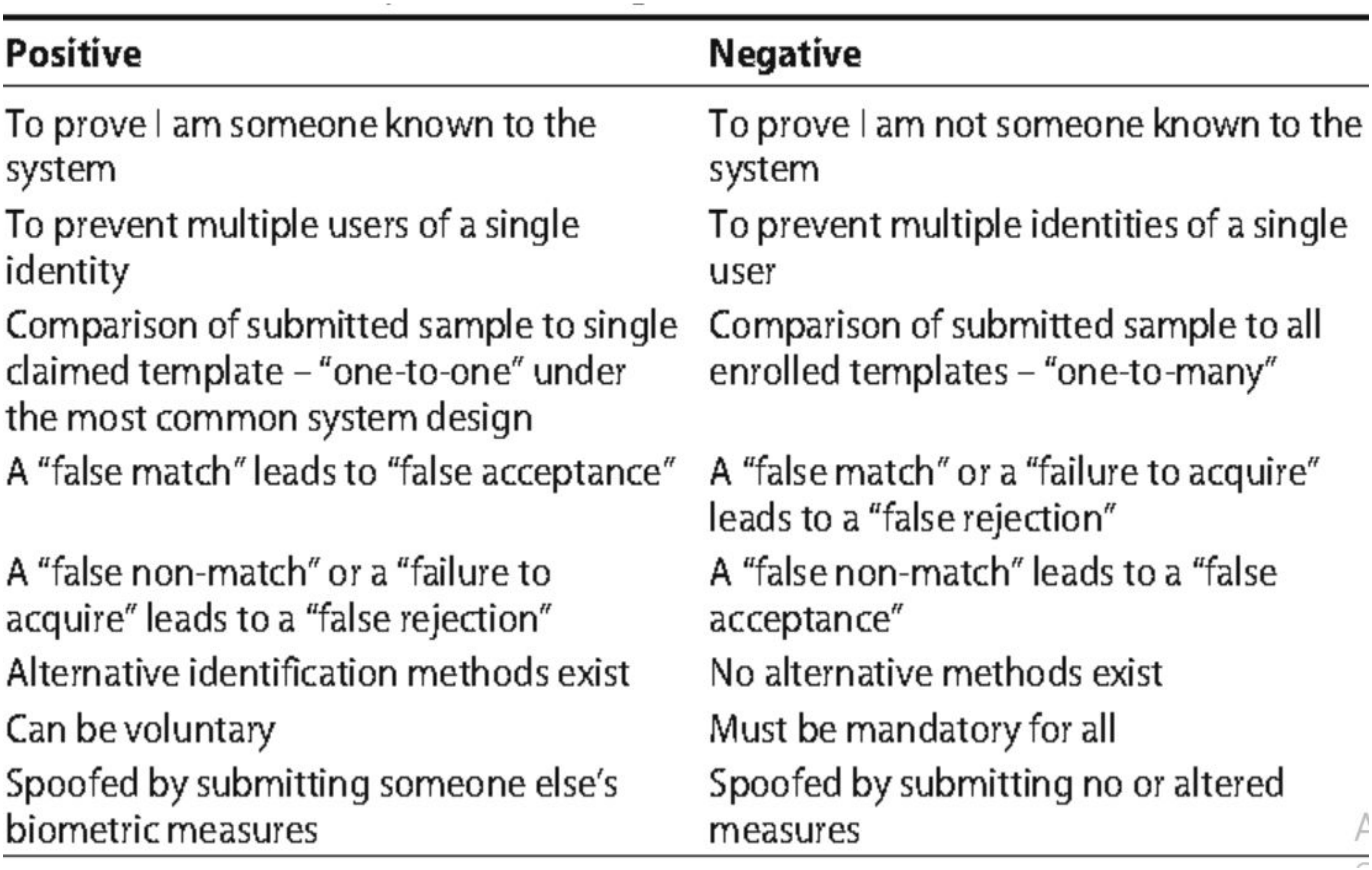
Biometric Functionalities

- The purpose of negative identification is to prevent a single person from using multiple identities.
- Hence, screening can be used to prevent the issue of **multiple credential records** (e.g., driver's licence, passport) assigned to the same person or to prevent a person from claiming multiple benefits under different names
- In both positive and negative identification, the user's biometric input is compared with the templates of all the persons enrolled in the database and the system outputs either the identity of the person whose template has the highest degree of similarity with the user's input.

Biometric Functionalities

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Differences between "Positive" & "Negative" Identification



Positive	Negative
To prove I am someone known to the system	To prove I am not someone known to the system
To prevent multiple users of a single identity	To prevent multiple identities of a single user
Comparison of submitted sample to single claimed template – "one-to-one" under the most common system design	Comparison of submitted sample to all enrolled templates – "one-to-many"
A "false match" leads to "false acceptance"	A "false match" or a "failure to acquire" leads to a "false rejection"
A "false non-match" or a "failure to acquire" leads to a "false rejection"	A "false non-match" leads to a "false acceptance"
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Spoofed by submitting someone else's biometric measures	Spoofed by submitting no or altered measures

Biometric Functionalities

- Formally, the problem of identification can be stated as follows:
- Given a **query feature set x**^{A}, we need to **decide** the **identity *I*** of the user, where *I* ∈ *{I*1*, I*2*, · · · , IN, IN*+1*}*. Here, *I*1*, I*2*, · · · , IN* correspond to the identities of the *N* users enrolled in the system and *IN*+1 indicates the case where no suitable identity can be determined for the given query. If **x** *C In* is the stored template corresponding to identity *In* and *sn* is the match score between **x**^{A} and **x***EIn*, for *n* = 1,2*, · · · ,N*, the decision rule for identification is,

$$\mathbf{x}^A \in \begin{cases} I_{n_0}, & \text{if } n_0 = \arg\max_{n} s_n \text{ and } s_{n_0} \geq \eta, \\ I_{N+1}, & \text{otherwise,} \end{cases}$$

- where η is a pre-defined threshold.
- The above decision rule is commonly known as ***open set identification***

Biometric Functionalities

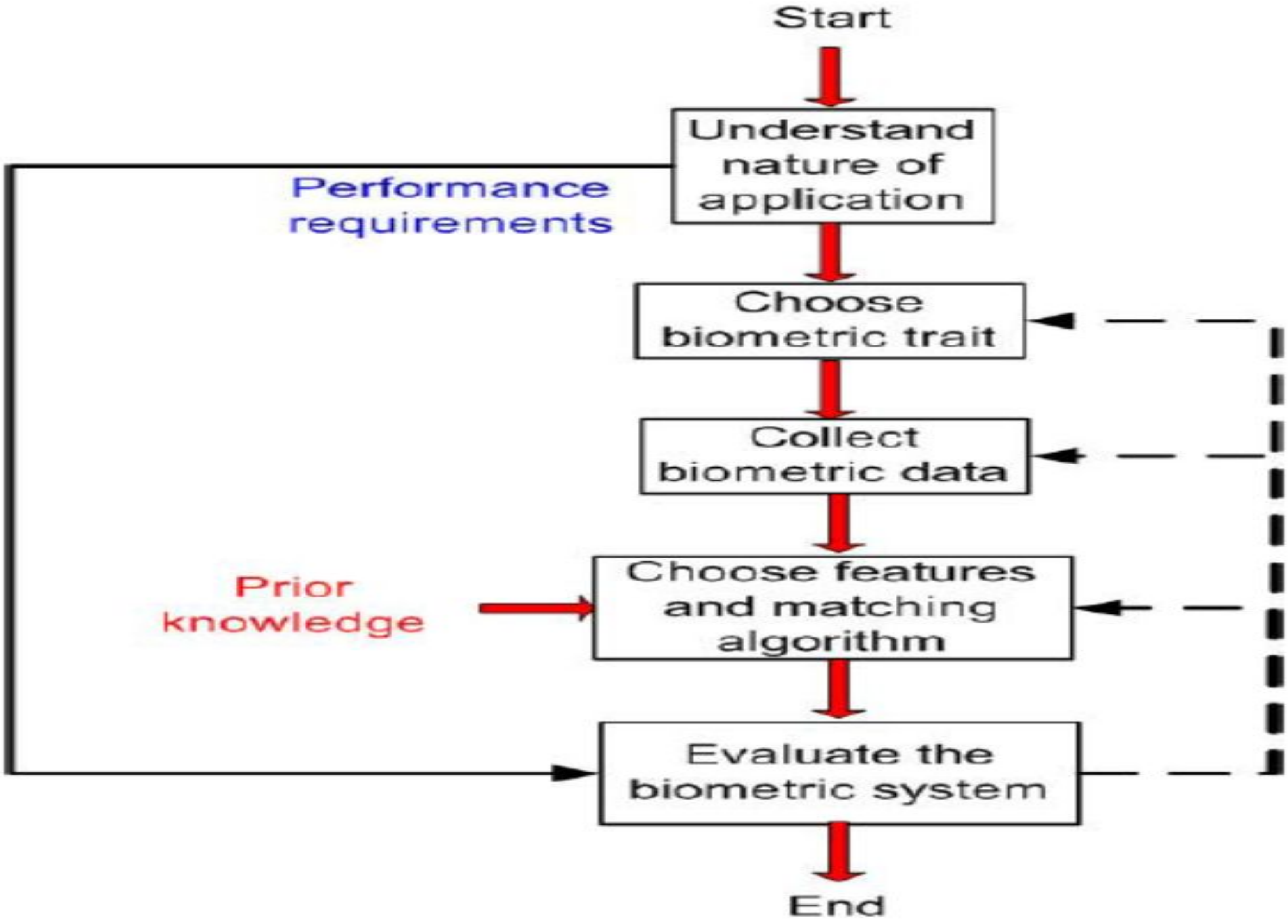
- It is also possible to **force the system to return one among the N enrolled identities**, irrespective of the value of sn0 . Such a scenario is called **closed set identification**.
- In some practical biometric identification systems (e.g., latent fingerprint matching), identification is **semi-automated**.
- A semi-automated biometric system outputs the identities of the **top *t* matches** (1 < *t* Ͼ *N*) and a human expert **manually determines** the identity (among the *t* selected identities) that best matches the given query.
- The value of *t* could be determined based on the **availability** and **throughput** of the human expert(s).

The Design Cycle of Biometric Systems

Major activities in the design of BS (Iterative)

- **Understanding** the **nature of the application** and the **performance requirements**
- **Choosing the right biometric trait(s)** for the application in hand
- **Collect biometric data** from a subset of target population
- **Design** or **train the core biometric modules**, including the feature extractor and the matcher
- **Evaluation procedure** to ensure that **it meets** the requirements of the application

The Design Cycle of Biometric Systems


Start
Understand nature of application
Performance requirements
Choose biometric trait
Collect biometric data
Prior knowledge
Choose features and matching algorithm
Evaluate the biometric system
End

A Taxonomy of Application Environments

- The **variations** in the application environment had a significant impact on the way the devices performed.
- In fact, accurate characterization of the **operational environment** is primary in selecting the **best biometric technology** and in predicting the **system's operational characteristics**.
- Depending on the **application context**, we may need to choose between the **verification** and **identification** functionalities

Factors influencing the Nature of the Application

1. Nature of the application

- Biometric applications can also be **classified** based on the following issues (Nature of the App).
  - **Cooperative** versus **non-cooperative user**
  - **Overt** versus **covert deployment**
  - **Habituated users** versus **non-habituated users**
  - **Attended** versus **unattended operation**
  - **Controlled** versus **uncontrolled operation**
  - **Open** versus **closed system**

Factors influencing the Nature of the Application

- **Cooperative versus non-cooperative users**
  - Eg. (Cooperative) - E-Banking
  - Eg. (Non-cooperative) – Terrorist’s behaviours in airport screening application
- **Overt** versus **Covert deployment**
  - If the user is **aware** that he is being **subjected** to biometric recognition, the application is categorized as **overt** (Finger Print Verification System)
  - If the user is **unaware**, the application is called **covert** (Facial Recognition)

Factors influencing the Nature of the Application

- **Habituated users** versus **non-habituated users**
  - If the enrolled users **interact** with the biometric system **quite frequently**, they tend to get habituated in providing their biometric data. (Login App in Computer Network)
  - A driver’s license application typically has **non-habituated** users since a driver’s license is renewed only once in a period of several years.
  - The familiarity of users with the system can affect recognition accuracy

Factors influencing the Nature of the Application

- **Attended** versus **unattended operation**
  - It refers to whether the process of biometric data acquisition in an application is **observed, guided**, or **supervised** by a human (e.g., a security officer).
  - An application may have an **attended enrollment** operation but **unattended recognition** operation
  - For example, a banking application may have a supervised enrollment when an ATM card is issued to a user, but the subsequent uses of the biometric system for the ATM transaction are not attended

Factors influencing the Nature of the Application

- **Controlled** versus **uncontrolled operation**: In a controlled environment, ambient **environmental conditions** such as temperature, pressure, moisture, lighting conditions, etc. can be moderated during the operation of a biometric system.
- Typically, indoor applications such as **computer network login** operate in a controlled environment, whereas outdoor applications such as keyless car entry or parking lot surveillance operate in an uncontrolled environment.
- This classification is also important for the system designer as a more rugged biometric sensor is needed for an uncontrolled environment

Factors influencing the Nature of the Application

- **Open** versus **closed system**: If a person’s **biometric template** can be used across **multiple applications**, the biometric system can be considered as **open**.
- For example, a user may use a fingerprint-based recognition system for entering secure facilities, computer network login, electronic banking, and bank ATMs.
- When all these applications use **separate templates** (databases) for each application, the system is considered **closed**.
- A closed system may be based on a **proprietary template** whereas an open system will need **standard data formats** and data compression methods to exchange and compare information between different systems

Factors influencing the Biometric Traits

2. Choice of biometric trait

- Each biometric trait has its **pros** and **cons** and, therefore, the choice of a biometric trait for a particular application depends on a variety of issues.
- In general, **seven factors** must be considered to **determine the suitability of a physical or a behavioural trait** to be used in a biometric application.

Factors influencing the Biometric Traits

1. **Universality**: It determines the **failure to enroll** (FTE) rate of the biometric system
2. **Uniqueness**: The given trait should be different across individuals comprising the user population. Otherwise, the **false match rate** (FAR or FPIR) of the biometric system would be high
3. **Permanence**: The biometric trait of an individual should be invariant **over a period of time** with respect to the matching algorithm, else, it will lead to a **high false non-match rate** (FRR or FNIR).

Factors influencing the Biometric Traits

4. Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause **inconvenience** to the individual.

- This factor significantly impacts the frequency of FTE and FTA failures and the recognition accuracy

5. **Performance**: The computational resources required to achieve that **accuracy** and the **throughput** requirements

6. Acceptability: Individuals in the target population that will utilize the application should be **willing to present** their biometric trait to the system

Factors influencing the Biometric Traits

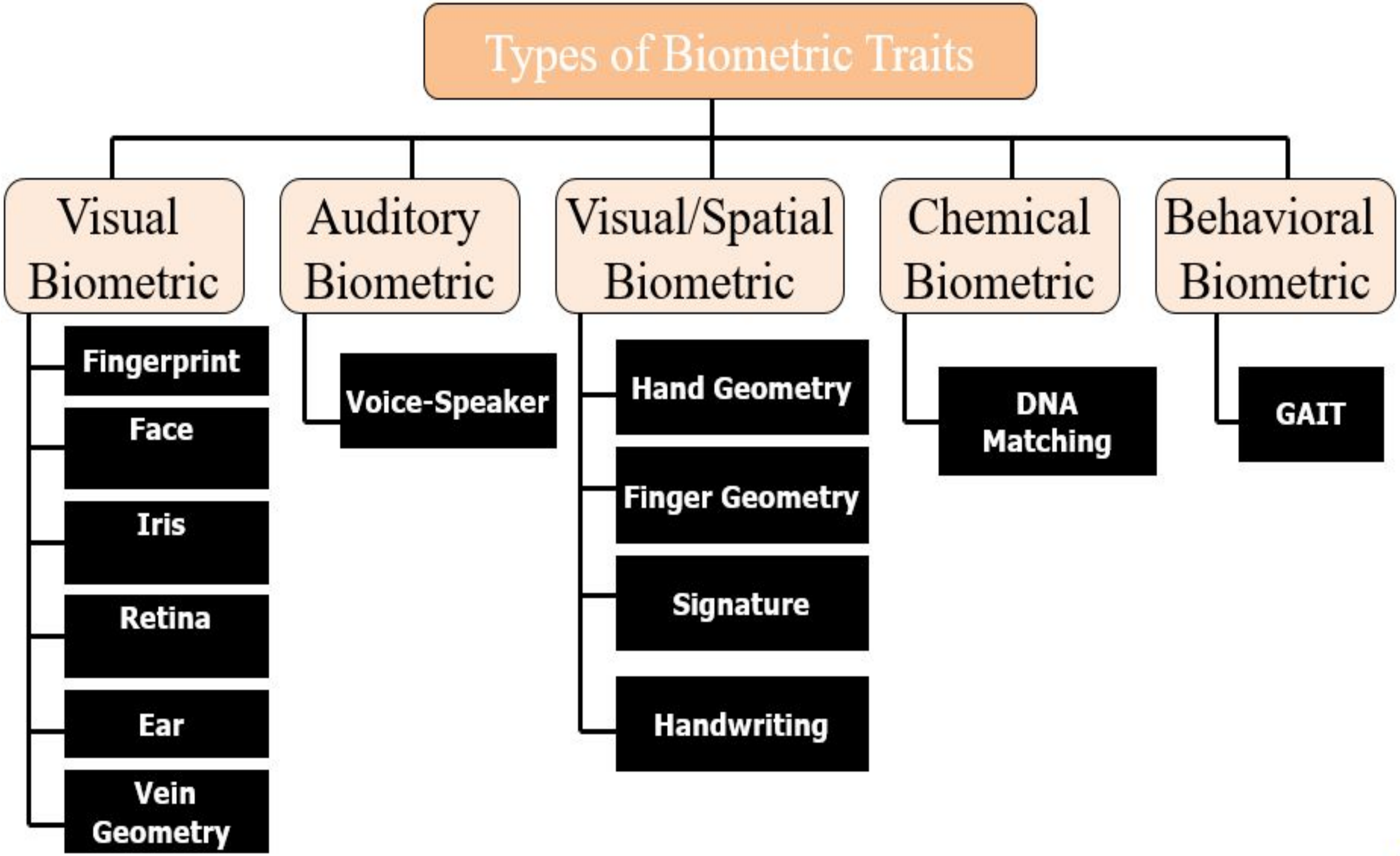
7. Circumvention: This refers to the ease with which the trait of an individual can be **imitated** using **artifacts** (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioural traits.

- It also refers to the process of **obfuscation**, where a user deliberately alters his biometric trait to evade recognition
- **No single biometric is expected to effectively meet all the requirements** (e.g., accuracy, practicality, cost) imposed by all applications (e.g., forensics, access control, govet benefits, etc.)

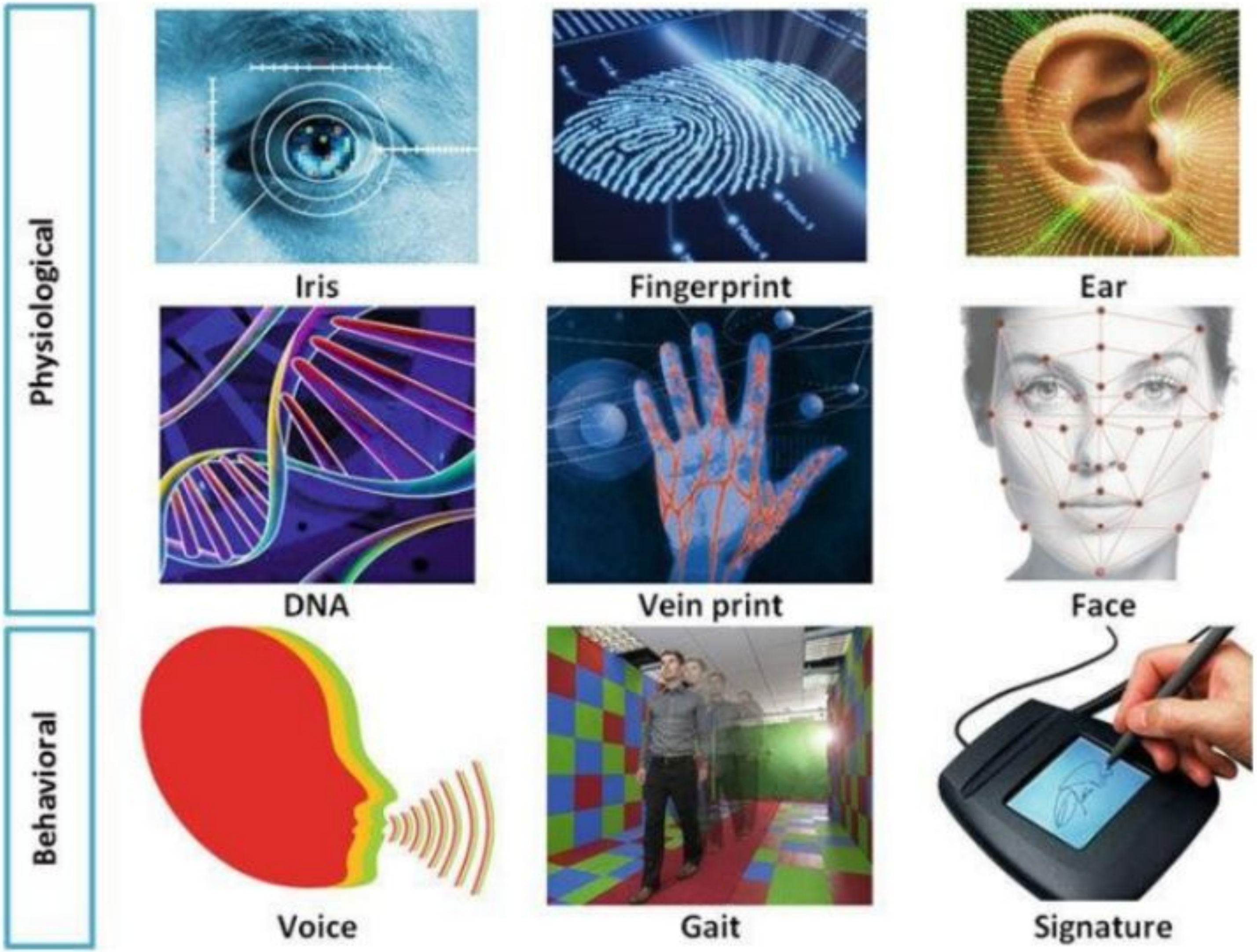
Commonly used biometric characteristics

- Fingerprint
- Palm print
- Iris
- Face
- Hand Geometry (Shape)
- Gait
- Ear
- Voice
- Keystroke
- Signature
- DNA
- Facial, hand, and hand vein infrared thermograms
- Odour
- Retinal Scan

Types of Commonly used Biometric Characteristics



Taxonomy of Commonly used Biometric Characteristics



The advantages of Physiological based biometric authentication mechanisms

Physiological biometrics:

- It does not take more than a few seconds to authenticate a person’s identity by fingerprint, face or voice.
- One does not need to remember complex passwords, keys, tokens or smart cards to validate his identity.
- The characteristics of this mechanism do not change e.g. Iris, fingerprint, DNA etc.
- 99% **accuracy and reliability** are being provided via distinctness in recognition.
- Social acceptance of using this mechanism is high.
- Hacking chances via using this are very less.

The advantages of using Behavioral based biometric authentication mechanisms

Behavioral biometrics:

- Behavioral biometric authenticate the users without the need to do some specific action.
- It collects the data for authentication dynamically.
- By using it, user can maintain privacy and avoid social awkwardness.
- It prevent identity theft and minimize the risk of online fraud.
- It is very authentic scheme and based on the user experience and individual skills.
- 90% accuracy is provided by this in recognition

The disadvantages of using these biometric authentication mechanisms

Physiological biometrics:

- Physiological Biometric authentication equipment is costly.
- People have to **wait in line** to get scanned to gain access which can cause delays.
- Slightly change in facial expression or obstruction due to hat, glasses or your finger is hurt or the voice is affected by cold couldn’t be recognized by the system.
- Dry, wet or dirty fingers can oscillate performance

The disadvantages of using these biometric authentication mechanisms

Behavioral biometrics:

- It has some effects on the privacy of individuals.
- Sometimes have problem in input methods such as ***phonetic*** may suffer from language problem.
- It would be difficult to identify **the gesture** if the movement slightly varies.
- It provides the less reliability than physiological bio metric behavior

The rationale for choosing Behavioral vs physiological biometric authentication mechanisms

Behavioral biometrics:

- Behavioral biometric authentication is preferred because the behavioral biometric system database is dynamic, making it more secure.
- It has less chance of being copied, stolen or reused by unauthorized personnel, unlike physiological biometrics.
- It does not require any specialized hardware that makes it economic friendly. These characteristics make behavioral biometrics a good option in high-security situation

The rationale for choosing Behavioral vs physiological biometric authentication mechanisms

Physiological biometrics:

- Physiological biometrics are hardware-dependent, unlike biometric behavior.
- Physiological biometric authentication provides accurate results compared to the behavioral mechanism.

Keeping these key points in mind, it is a better alternative to use physiological biometrics if the behavioral mechanism does not authenticate the user.

Physiological biometrics should be sufficient in environments where high protection is not required

The social issues in Biometric Authentication mechanism

- The biometric-based authentication system can be attacked by **Insider attacker** and stranger
- A **scammer** can make various attempts to spoof a legitimate user's biometric trait to bypass system security.
- The biometric data obtained by a person during the authentication process can vary significantly from the data used to produce the template during enrollment. That can have a big effect on the matching process.

Multi-Biometric Systems

- One way to improve the accuracy of biometric systems is to **use more than one biometric trait** in a recognition application.
- For example, the **face** and **iris** traits, or the **fingerprints** from all the ten fingers of an individual may be used together to resolve the identity of an individual.
- Such systems are known as ***multi-biometric systems*.**
- These systems are expected to be more accurate and reliable due to the **availability of multiple pieces of evidence**

Data Collection

- The collection of biometric data from a subset of the targeted population.
- This data is required both for **designing the feature extraction and matcher modules** as well as for the **evaluation** of the designed biometric system.
- Due to the involvement of human subjects, legal and privacy issues must also be considered and approval of organizations like the Institutional Review Board (IRB) is mandatory in many countries.
- This makes biometric data collection a time-consuming, relatively expensive, and cumbersome process

Data collection

Choice of features and matching algorithm

- Another important factor affecting the choice of features and matching algorithm is the **interoperability** between biometric systems
- For eg, it challenging to compare voice samples originating from **two different handset**
- The **performance** of face recognition algorithms is severely affected when the images used for comparison are captured using **different camera types.**

Evaluation

- It requires experts from a variety of fields, including statistics, computer science, engineering, business, and psychology, as well as system designers and the end user community
- In order to understand the performance of a biometric system, one must address the following questions
  - What are error rates of the given Biometric System for a given application?
  - What is the reliability, availability and maintainability of the system?
  - What are the vulnerabilities in the system? And so on

Evaluation

- The evaluation requires an independent third party to design, administer, and analyze the test.
- We can divide **the matching performance** evaluation of a biometric system into three stages

1. **Technology evaluation –** Compares different algorithms like Fingerprint Verification Competitions (FVC), the Fingerprint Vendor Technology Evaluation (FpVTE), the Face Recognition Vendor Tests (FRVT), the Face Recognition Technology (FERET) program, and the NIST Speaker Recognition Evaluations (SRE)

- These algorithms are **examples of biometric technology evaluations**.

Evaluation

2. Scenario evaluation - the **testing of the prototype** biometric systems is carried out in an environment that closely resembles the **real-world** application

3. **Operational evaluation -** is used to ascertain the **performance** of a complete biometric system in a **specific real-world application** environment on a **specific target population**.

Applications of Biometric Systems

Commercial applications such as

- computer network login,
- electronic data security,
- e-commerce, Internet access,
- ATM or credit card use,
- physical access control,
- mobile phone, PDA,
- health record management,
- distance learning, etc.

Applications of Biometric Systems

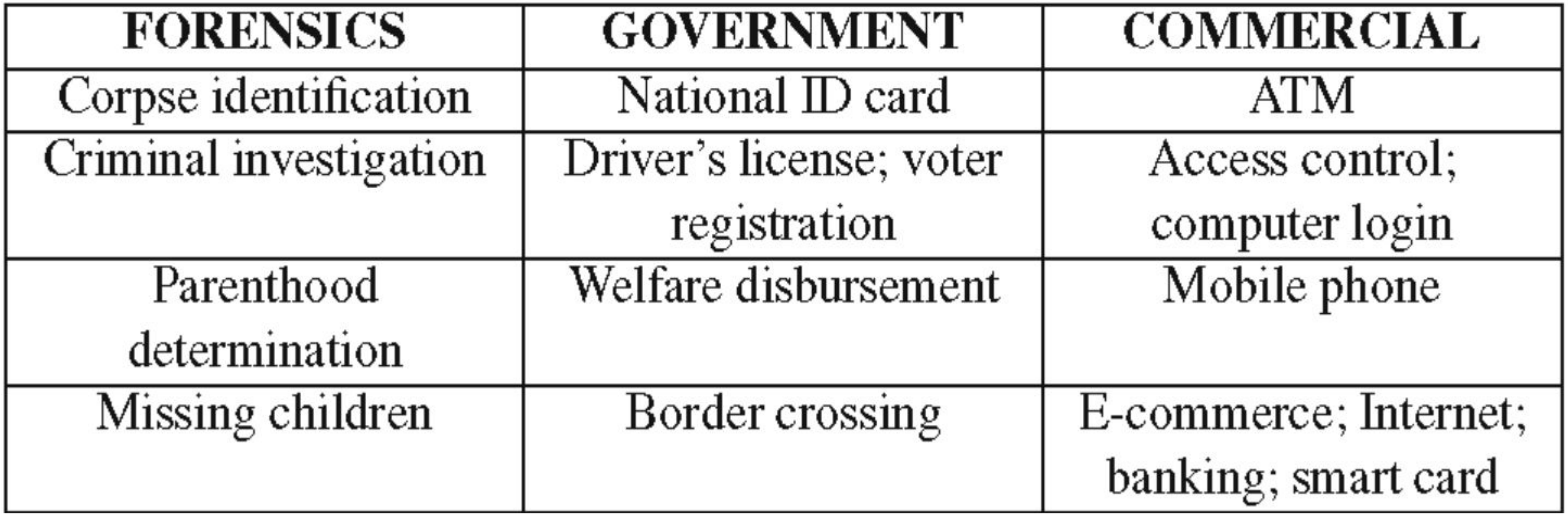
Government applications such as

- national ID card,
- managing inmates in a correctional facility,
- driver’s license,
- social security,
- welfare-disbursement,
- Border control,
- passport control, etc

Applications of Biometric Systems

Forensic applications such as

- Corpse identification,
- Criminal investigation,
- Missing children,
- parenthood determination, etc.



FORENSICS	GOVERNMENT	COMMERCIAL
Corpse identification	National ID card	ATM
Criminal investigation	Driver's license; voter registration	Access control; computer login
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

Session 3 and 4

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Introduction to Uni-model System
- Introduction to Multi-model Biometric System

- Biometric System Errors
- Performance Measures

Categories of Biometrics Systems

- Biometric System are basically categorized as
  - Unimodal
  - Multimodal

Uni-modal Systems

- Biometric systems that operate using any **single biometric** characteristic
- Less expensive and simple
- Unimodal Systems
  - Face
  - Fingerprint
  - Iris
  - Ear
  - Signature
  - Gait

Unimodal

Limitations of Unimodal Biometric System:

- Susceptibility of biometric sensor to noisy or bad data.
- The captured biometric trait might be distorted due to imperfect acquisition conditions.
- (Eg: In fingerprint recognition where a scanner is unable to read dirty fingerprints clearly and leads to false database match.)

Limitations

- It might not be compatible with **certain groups** of population
- (fingerprint images might not be properly captured for the elderly and young children because of faded fingerprints or underdeveloped fingerprint ridges.)
- Within a large population ,uni-modal biometrics is prone to **inner class similarities**
- (eg: **facial recognition** may not work correctly for **identical twins** as the camera might not be able to distinguish between two subjects leading to inaccurate matching.)

Limitations

- Unimodal biometrics systems are **vulnerable** to **spoof attacks** where the data can be imitated or forged.
- (fingerprint recognition systems can be easily spoofed using rubber fingerprints)

In a Nutshell, the Limitations are

- **Noisy Data**
  - Leads to false rejection
- **Inter-class similarity**
  - For Identical twins face recognition system will not work
- **Incompatible for subset of population**
  - Hard workers have poor fingerprint pattern
- **Vulnerable to spoofing**
  - Data can be imitated or forged
  - Example: Latent fingerprints
- **Accuracy**

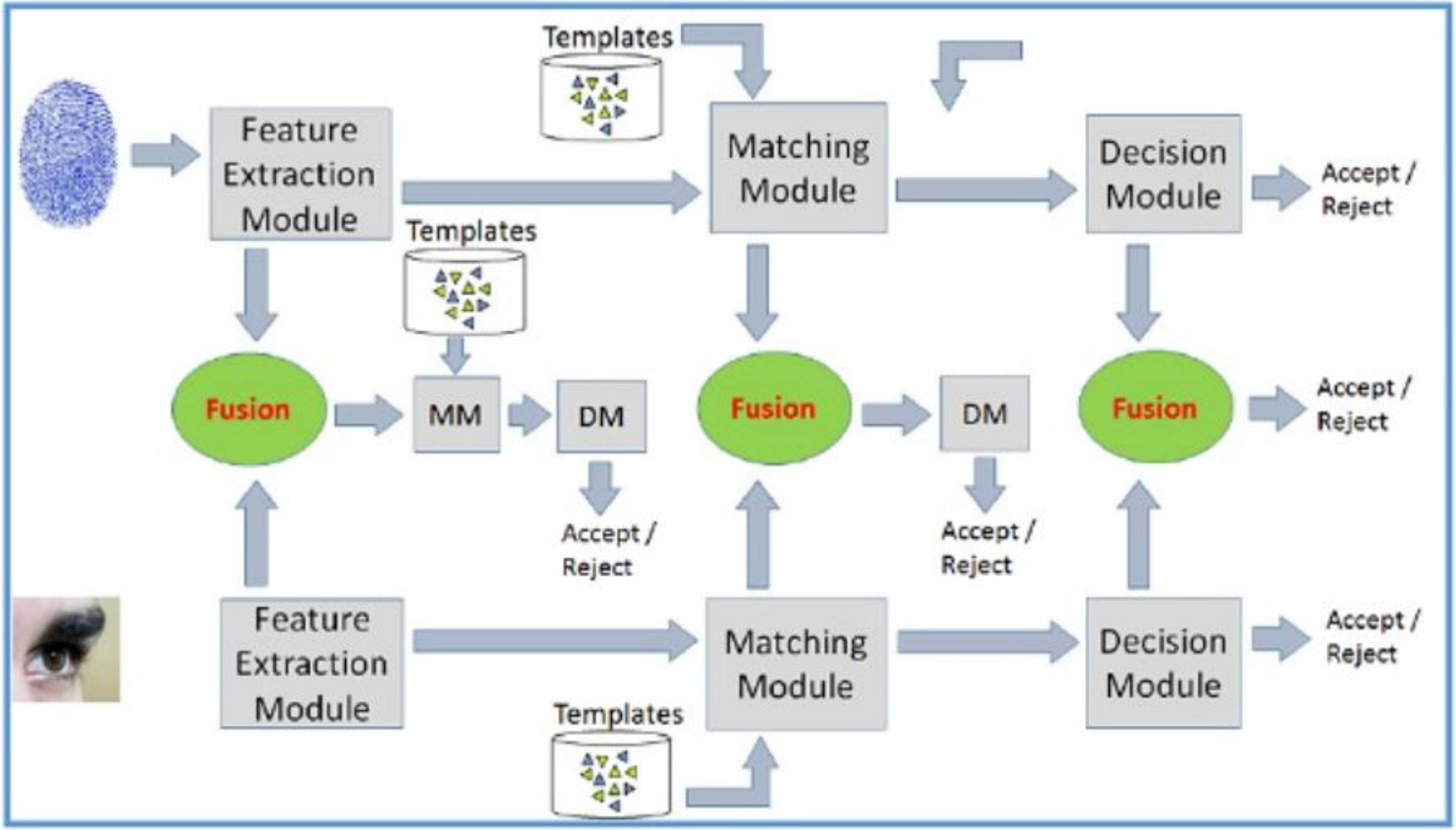
Multimodal Biometric System

- **A biometric system that uses more than one**
  - Classifier/ Algorithm
  - Sample
  - Sensor
  - Trait

Need of Multimodal Biometrics

- Reduces error rates of Unimodal System
- A secondary means of authentication
  - Poor quality sample from the sensor
  - Non-availability of data
- Combat spoof attacks such as fake fingers

Multimodal Biometric System

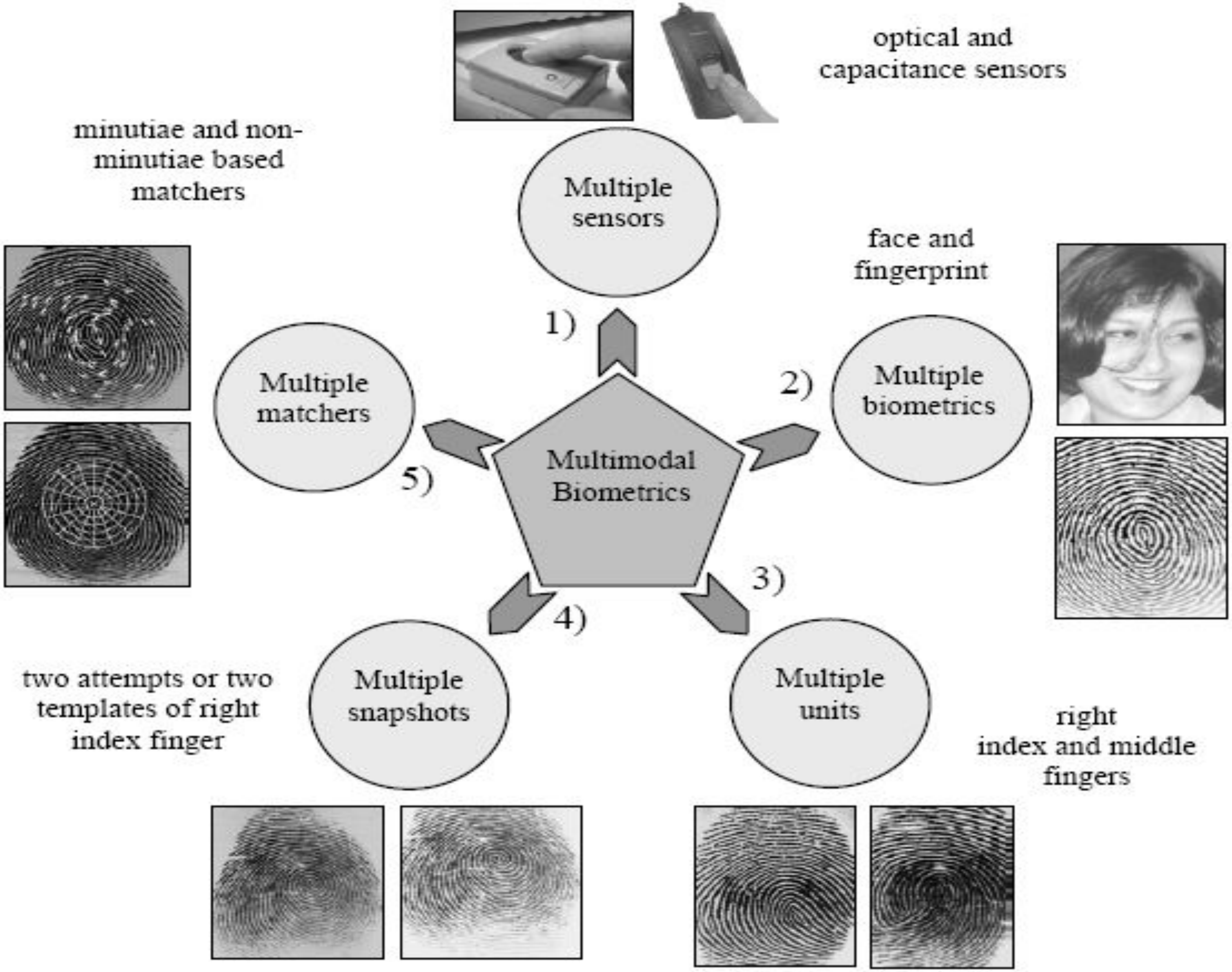


Multimodal Biometric System

- **Merge two or more** biometric technologies such as facial recognition ,fingerprint, iris scanning, hand geometry, voice recognition etc.
- Systems take input from single or multiple sensors for measuring two or more different biometric characteristics.
- Improving recognition rate, combining two or more biometric modalities might be more appropriate for different applications.

Integration Scenarios

- Multiple Sensors
- Multiple Biometrics
- Multiple units of same biometrics
- Multiple snapshots of same biometrics
- Multiple Classifiers


optical and capacitance sensors
Multiple sensors
1)
minutiae and non-minutiae based matchers
face and fingerprint
Multiple matchers
2)
Multiple biometrics
Multimodal Biometrics
5)
3)
4)
two attempts or two templates of right index finger
Multiple snapshots
Multiple units
right index and middle fingers

Types of Multimodal Biometric System

- **Multi algorithmic biometric system**: System take a single sensor and then process it using two or more different algorithms.
- **Multi instance biometric systems**: Systems use **one or more sensors** to capture samples of two or more different samples of same biometric trait.(Capturing images of multiple fingers)

Multi Sensorial Biometric Systems

- **Multi sensorial biometric systems**: system use two or more distinctly different sensors to capture the **same instance** of a biometric trait.
- Captured samples are then processes using **single algorithm** or **combination** of algorithm
- (eg: same facial image is captured using visible light camera and infrared camera fixed with particular frequency)

Fusion Strategies

- Multimodal biometric system requires integration of data of different modalities like face, fingerprint, retina, voice, iris, etc
- It can be done through a process called "**Fusion**"
- There are different fusion methods or strategies used in the multi-modal Biometric Systems

Different Fusion Strategies

- **Fusion prior to matching**
  - Sensor level fusion
  - Feature level fusion

- **Fusion after matching**
  - Match score fusion
  - Rank level fusion
  - Decision level fusion

Different Fusion Strategies (cont.)

Sensor level fusion

- We fuse the biometric traits coming from the **different sensors** such as fingerprint scanner, iris scanner, video camera etc. to form a merged biometric trait and process.
  - Raw data from the sensor(s) are combined.
  - This is referred to as image level or pixel level fusion.
  - Sensor level fusion can benefit multi-sample systems which capture multiple snapshots of the same biometrics.
  - For example, 2D face images of an individual obtained from several cameras can be combined to form a 3D model of the face.

Different Fusion Strategies (cont.)

- **Feature level fusion**: signals coming from different biometric channels are first processed after which the feature vectors are extracted separately from each biometric trait.
  - It refers to combine different feature sets extracted from multiple biometric sources.
  - When feature sets are homogeneous, a single resultant feature vector can be calculated as a weighted average of the individual feature vector
  - When the feature set are non-homogeneous , we can concatenate to form a single feature vector.

□

Different Fusion Strategies (cont.)

- **Match score fusion**: individual matching score is found, we then fuse the matching level to find composite matching score which will be used for classification.
  - Scores generated from different matching modules are combined to produce a single score.
  - Final decision is taken by considering the fused score.
  - Normalization and Similarity/ Dissimilarity Score
  - There are various approaches possible for combining the individual scores.
    - Product rule
    - Sum rule
    - Weighed sum rule
    - Max rule and median rule

Different Fusion Strategies (cont.)

Rank level fusion

For identification, output is the ranks of enrolled identities.

This fusion scheme is to consolidate the ranks of individual biometric systems to derive a fused rank for each identity.

It reveals less information than match scores. However, unlike match scores, the ranking output by multiple biometric systems are comparable.

No normalization is needed and this makes the rank level fusion schemes simpler to implement compared to the score level fusion techniques.

- Highest rank method
- Logistic regression method

Different Fusion Strategies (cont.)

Decision level fusion: Each biometric trait is first pre classified separately

Individual trait is first captured and then features are extracted from the captured trait.

- Decision level fusion is the highest level fusion of biometric evidences.
- Fusion is carried out at the abstract or decision level when only the decisions output by the individual biometric matchers are available.
- It logically combines accept/reject matching decisions of different matchers.
  - “AND” and “OR” rule
  - Majority voting
  - Weighted majority voting
  - Bayesian decision fusion

Advantages of Multimodal Biometric Systems

- Multimodal biometrics can reduce data distortion.
- Multimodal biometric systems are very difficult to spoof as compared to unimodal systems.
- Multimodal biometric systems are most robust, reliable and accurate as compared to unimodal systems.
- Multimodal systems overcome the various limitations of unimodal systems and hence are suitable to many industries such as healthcare, civil id and financial industries.

Biometric System Errors

- ***Uniqueness*** and ***permanence*** of the underlying biometric trait are the fundamental premises of BS
- Biometric identifier is said to be unique only if any two persons in the world can be differentiated based on the given identifier.
- A biometric trait is permanent if it does not change over the lifetime of an individual.
- Biometric systems rely only on the digital measurements of the body characteristics, and not the real physical traits.
- This process of measurement (sensing) introduces variations in the samples of the same biometric trait of a user obtained over a period of time.

Biometric System Errors

- The variability observed in the biometric feature set of an individual is known as ***intra-user variations*** or ***intra-class variations***.
- This variability may be due to reasons like imperfect sensing conditions (e.g., noisy fingerprint due to sensor malfunction), alterations in the user's biometric characteristics, changes in ambiant conditions (e.g., inconsistant illumination levels in face recognition applications), and variations in the user's interaction with the sensor (e.g., occluded iris)
- An ideal biometric feature set must exhibit small inter-user similarity and small intra-user variations

Biometric System Errors

- Two types of errors, namely, ***false non-match*** and ***false match***
- When the intra-user variation is large, two samples of the same biometric trait of an individual (mate samples) may not be recognized as a match, and this leads to a false non-match error.
- A false match occurs when two samples from different individuals (non-mate samples) are incorrectly recognized as a match due to large inter-user similarity.

Performance measures

- The basic measures of the accuracy of a biometric system are ***False Non-Match Rate*** (FNMR) and ***False Match Rate*** **(FMR)**.
- FNMR refers to the expected probability that two mate samples (samples of the same biometric trait obtained from the same user) will be falsely declared as a non-match.
- FMR is the expected probability that two non-mate samples will be incorrectly recognized as a match
- A FNMR of 5% indicates that on average, 5 in 100 authentication attempts by genuine users will not succeed.
- A False Match Rate of 0.02% indicates that on average, 1 in 5,000 authentication attempts by random impostors are likely to succeed

Performance measures

Verification system error rates

- In the context of biometric verification, FNMR and FMR are generally referred to as **False Reject Rate** (FRR) and **False Accept Rate** (FAR), respectively
- A **match score** is termed as a *genuine* or *authentic* score if it indicates the similarity between two mate samples.
- An ***impostor* score** measures the similarity between two non-mate samples
- Given a set of genuine and impostor match scores, FRR can be defined as the proportion of genuine scores that are less than the threshold η and
- FAR can be defined as the fraction of impostor scores that are greater than or equal to η.

Performance measures

- we will use the labels ω0 and ω1 to denote the impostor and genuine classes, respectively. Let *p*(*s*/ω1) and *p*(*s*/ω0) be the probability density functions of the genuine and impostor scores, respectively
- The FAR and FRR of the biometric system are given by

$$FAR(\eta) = p(s \geq \eta | \omega_0) = \int_{\eta}^{\infty} p(s|\omega_0)\,ds,$$

$$FRR(\eta) = p(s < \eta | \omega_1) = \int_{-\infty}^{\eta} p(s|\omega_1)\,ds.$$

- If the threshold is increased, FAR will decrease but the FRR will increase and vice versa.
- Hence, for a given biometric system, it is not possible to decrease both these errors simultaneously by varying the threshold.

Performance measures

- The **Genuine Accept Rate** (GAR) or **True Accept Rate** (TAR) can be used as an alternative to FRR

$$GAR(\eta) = p(s \geq \eta | \omega_1) = 1 - FRR(\eta).$$

Users

- **Four categories of users** are usually defined in the biometrics (Doddington's zoo)
- ***Sheep*** represent users whose biometric feature sets are very distinctive and exhibit low intra-class variations. Therefore, these users are expected to have low false accept and false reject errors.
- ***Goats*** refer to users who are prone to false rejects. The biometric feature sets of such users typically exhibit large intra-class variations

Performance measures

- ***Lambs*** are users whose biometric feature set overlaps extensively with those of other individuals.
- The biometric feature sets of these users have high inter-user similarity.
- Thus, a randomly chosen user (from the target population) has a higher probability of being accepted as a lamb than as a sheep.
- The false accept rate associated with these users is typically high

Performance measures

- ***Wolves*** indicate individuals who are successful in deliberately manipulating their biometric trait (especially behavioural traits) in order to impersonate legitimately enrolled users of a system.
- Since the wolves make a concerted effort to adopt the identity of another user, such an effort is often referred to as an ***adversary attack*** and it can increase the FAR of a system
- Examples include forging the signature of another user or mimicking someone else’s voice

Performance measures

- The ***Failure to Enroll*** *(FTE)* rate denotes the proportion of users that cannot be successfully enrolled in a biometric system
- This necessitates the design of robust and efficient user interfaces that can assist an individual both during enrollment and recognition
- The fraction of authentication attempts in which the biometric sensor cannot capture the sample presented to it is known as ***Failure to Capture*** (FTC) or ***Failure to Acquire*** (FTA) **rate**
- Thus, periodic sensor maintenance is instrumental for the efficient functioning of a biometric system

Performance measures

- The performance of a biometric system may also be summarized using other single-valued measures such as the **Equal Error Rate** (EER) and the **d-prime value**
- The EER refers to that point in a Detection Error Tradeoff-DET (or) Receiver Operating Characteristic - ROC curve where the FAR equals the FRR; a lower EER value, therefore, indicates better performance.
- The **d-prime value** (*d*) measures the separation between the means of the genuine and impostor probability distributions in standard deviation units and is defined as

$$d' = \frac{\sqrt{2}\,|\,\mu_1 - \mu_0\,|}{\sqrt{\sigma_1^2 + \sigma_0^2}},$$

Performance measures

- where μ1 (μ0) and σ1 (σ0) are the mean and standard deviation, respectively, of the genuine (impostor) score distributions.
- A higher d-prime value indicates better performance.
- Another single valued performance measure is known as the F-Ratio, which is defined as

$$\text{F-ratio} = \frac{\mu_1 - \mu_0}{\sigma_1 + \sigma_0}$$

- If the genuine and impostor distributions are Gaussian, then the EER and F-ratio are related according to the following expression where

$$\text{EER} = \frac{1}{2} - \frac{1}{2}\text{erf}\left(\frac{\text{F-ratio}}{\sqrt{2}}\right) \qquad \text{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,dt$$

Performance measures

- **Identification system error rates**
- Suppose that a biometric identification system, with N identities enrolled, outputs a set of identities corresponding to the top t matches $(1 \leq t\ N)$.
- The **identification rank** is defined as the rank of a user’s correct identity in the top t matches returned by the identification system.
- There are two types of identification system errors. A **false positive identification** occurs when an identity is returned for a user not enrolled in the system.
- This is analogous to the false match case in biometric verification

Performance measures

- The expected proportion of identification transactions by users not enrolled in the system, where an identity is returned, is known as **the *false positive identification rate*** (FPIR).
- The FPIR depends both on the size of the enrollment database (*N*) and the threshold (η)
- **False negative identification** refers to a scenario where the transacting user is enrolled in the database, but his correct identity is not among those returned by the system.

Performance measures

- The expected proportion of identification transactions by users enrolled in the system in which the user’s correct identity is not returned is called the ***false negative identification rate*** (FNIR).
- FNIR depends on the size of the enrolment database (*N*), the threshold (η) used for the match scores, and the number of identities *t* returned by the identification system.
- A quantity related to the FNIR is the ***true positive identification rate*** (TPIR), which is the expected proportion of identification transactions by users enrolled in the system, where the user’s correct identity is among the *t* identities returned by the system. Therefore, FNIR = 1− TPIR

End of Part 1 (UNIT 1)