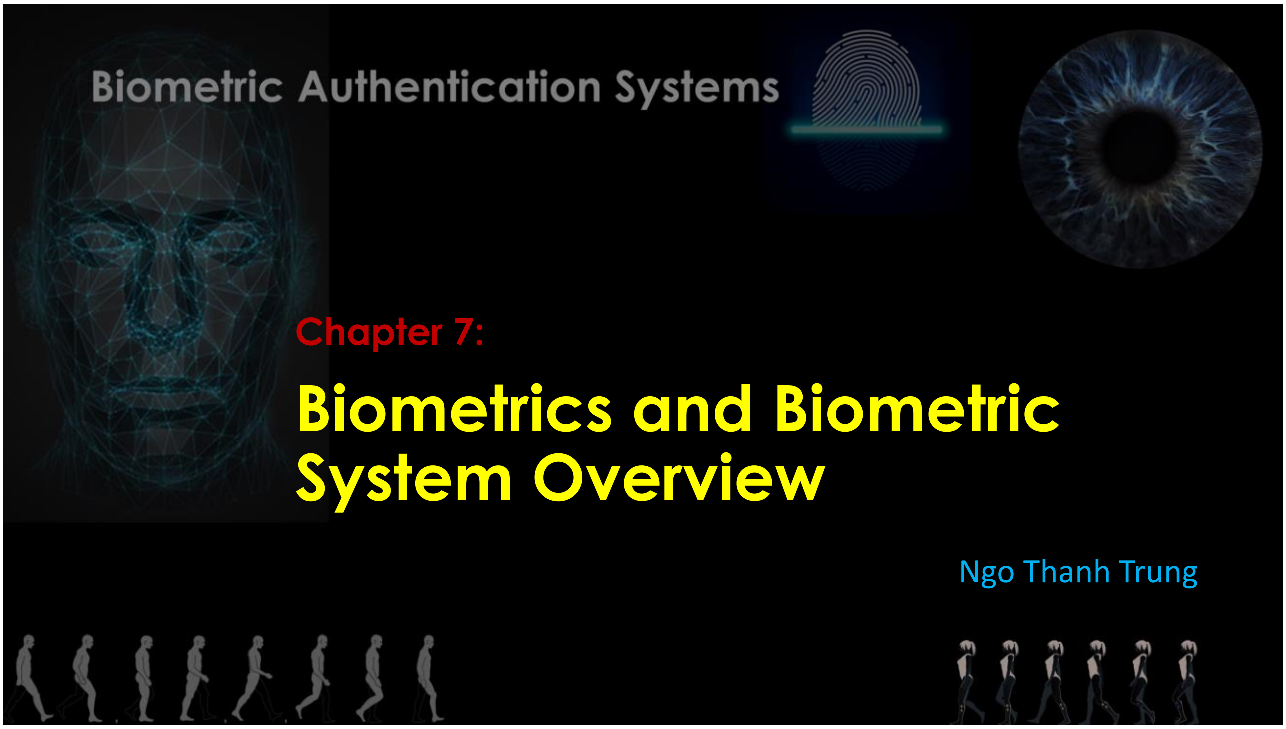


Biometric Authentication Systems

Chapter 7:

Biometrics and Biometric System Overview

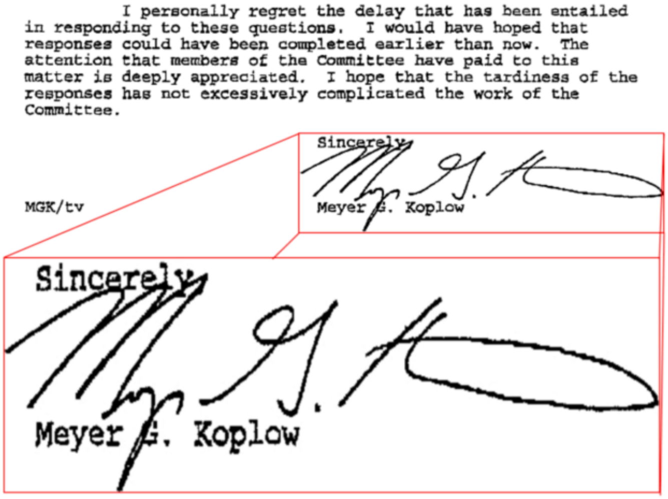
Ngo Thanh Trung

Identity verification everyday

- Show the id card to the police

Identity verification everyday

- Signature



I personally regret the delay that has been entailed in responding to these questions. I would have hoped that responses could have been completed earlier than now. The attention that members of the Committee have paid to this matter is deeply appreciated. I hope that the tardiness of the responses has not excessively complicated the work of the Committee.

Sincerely,

Meyer G. Koplow

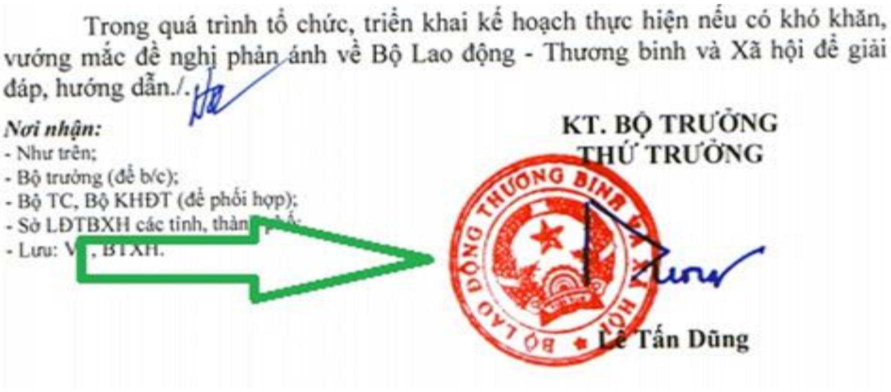
MGK/tv

Sincerely,

Meyer G. Koplow

Identity verification everyday

- Signature and stamp



Trong quá trình tổ chức, triển khai kế hoạch thực hiện nếu có khó khăn, vướng mắc đề nghị phản ánh về Bộ Lao động - Thương binh và Xã hội để giải đáp, hướng dẫn./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Bộ TC, Bộ KHĐT (để phối hợp);
- Sở LĐTBXH các tỉnh, thành phố;
- Lưu: VT, BTXH.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ LAO ĐỘNG THƯƠNG BINH VÀ XÃ HỘI

Lê Tấn Dũng

Identity verification everyday

- Bank transaction

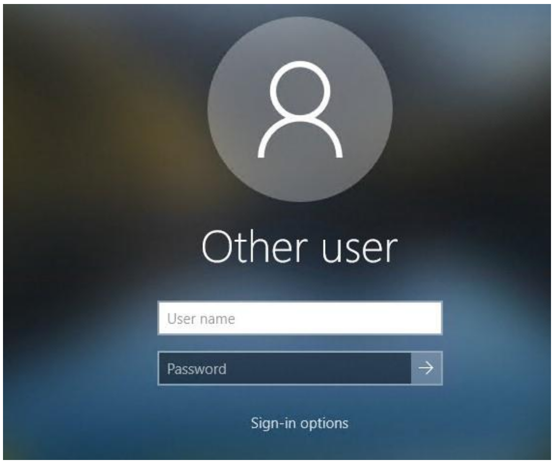
Identity verification everyday

- Listen to the voice of a person at the other end of the phone line

Adobe Stock | #371413230

Identity verification everyday

- Personal device login



Authentication

- There are traditional ways of verifying the identity of a person:
  - Possessions (keys, passports, smartcards , …)
  - Knowledge
  - Secrete
    - Secret (passwords, pass phrases, …)
    - Non-secret (user Id, mothers maiden name, favorite color)
  - Biometrics
    - Physiological (fingerprints, face, iris, …)
    - Behavioral (walking, keystroke pattern, talking, …)

New password must be different than previous password.

Reset Your Password

Almost done. Enter your new password, and you're good to go.

New password Show

••••••••••••••

Your password is secure and you're all set!

Authentication

- There are traditional ways of verifying the identity of a person:
  - Possessions (keys, passports, smartcards , …)
  - Knowledge
  - Secrete
    - Secret (passwords, pass phrases, …)
    - Non-secret (user Id, mothers maiden name, favorite color)
  - Biometrics
    - Physiological (fingerprints, face, iris, …)
    - Behavioral (walking, keystroke pattern, talking, …)

These methods can be easily shared or lost!!!!!!!!!

New password must be different than previous password.

Reset Your Password

Almost done. Enter your new password, and you're good to go.

New password

Show

•••••••••••••••

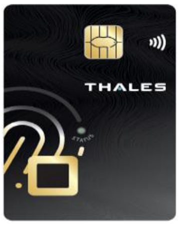
Your password is secure and you're all set!

Biometrics system are getting more popular

Face lock

Fingerprint lock

vain lock

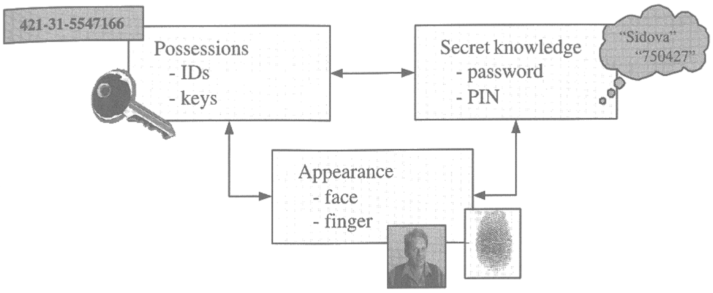


Biometric card

iris lock

More secure systems

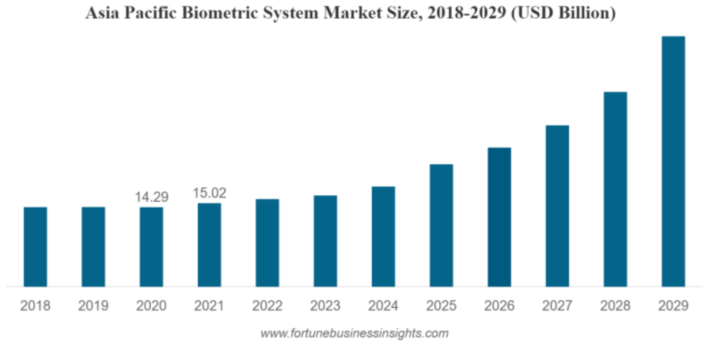
- The authentication methods are sometimes combined
  - User id + password
  - ATM card + password
  - Passport + face picture and signature



Rise in Demand of Biometrics Systems

Transparency Market Research: biometrics technology usage is increasing globally, the biometrics market:

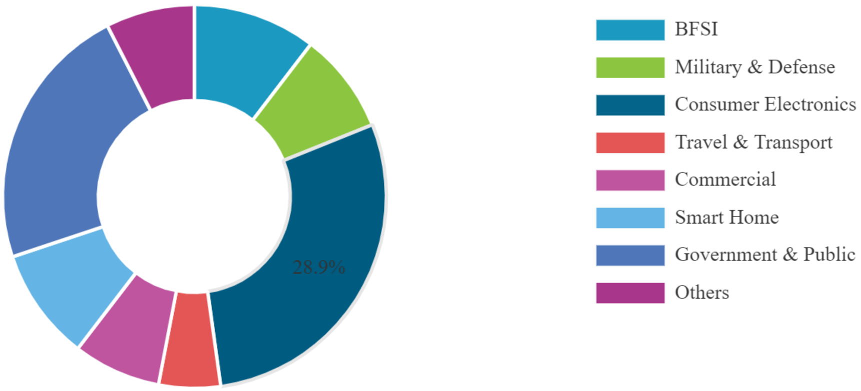
- $39.62 billion in 2021
- to reach $136.18 billion by 2031
- annual growth rate of 13.3% between 2022 and 2031,


Asia Pacific Biometric System Market Size, 2018-2029 (USD Billion)

www.fortunebusinessinsights.com

Market share

Global Biometric System Market Share, By End-user, 2021



www.fortunebusinessinsights.com

Driving facts

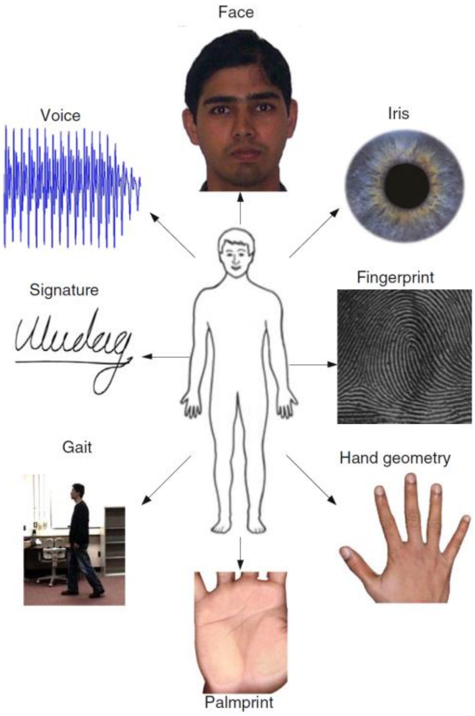
- Increasing demand for automation
- Increasing demand for security and surveillance
- Increasing incidents of crimes, e.g., fraud and phishing
- Technology development
- Covid 19

Outline

1. What is Biometrics?
2. Types of Biometrics
3. Types of Biometric Recognition
4. Biometric Systems
5. Biometric System Errors
6. Performance measures
7. Choice of biometric traits

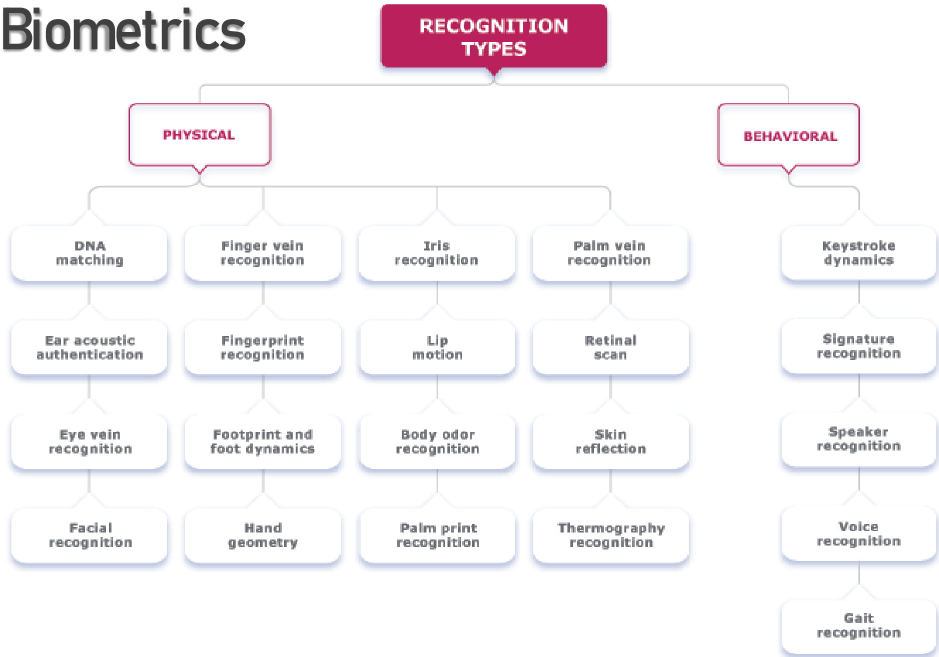
1-What is biometrics?

- A measurable **physical characteristic** or **personal behavioral trait** used to recognize the identity, or verify the claimed identity, of an applicant.



2- Types of Biometrics

- **Physical**
- **Behavioral**



RECOGNITION TYPES

PHYSICAL

DNA matching

Finger vein recognition

Iris recognition

Palm vein recognition

Ear acoustic authentication

Fingerprint recognition

Lip motion

Retinal scan

Eye vein recognition

Footprint and foot dynamics

Body odor recognition

Skin reflection

Facial recognition

Hand geometry

Palm print recognition

Thermography recognition

BEHAVIORAL

Keystroke dynamics

Signature recognition

Speaker recognition

Voice recognition

Gait recognition

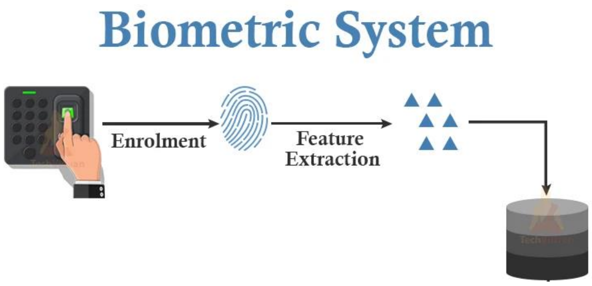
2-Biometric Systems

- **Definition**:
  - Biometric systems are **using biometrics to authenticate or identify a person**. A system **collects** biometric characteristics unique to every person. These biometric characteristics are then directly linked to verify or identify the individual.

- Two phases:
  - Biometric enrollment
  - Recognition

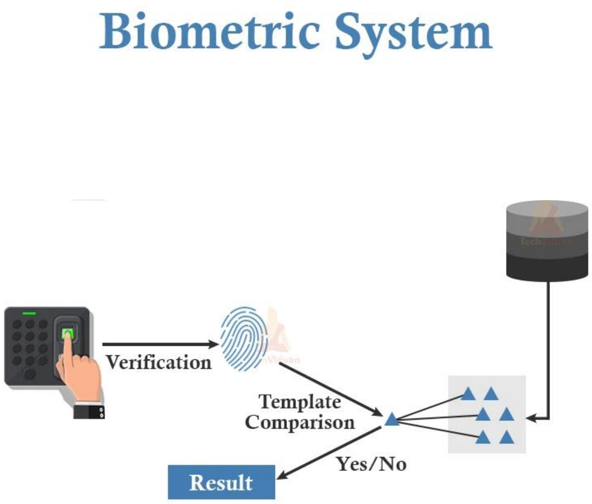
2-Biometric Systems

- **Definition**:
  - Biometric systems are **using biometrics to authenticate or identify a person**. A system **collects** biometric characteristics unique to every person. These biometric characteristics are then directly linked to verify or identify the individual.
- Two phases:
  - Biometric enrollment
  - Recognition

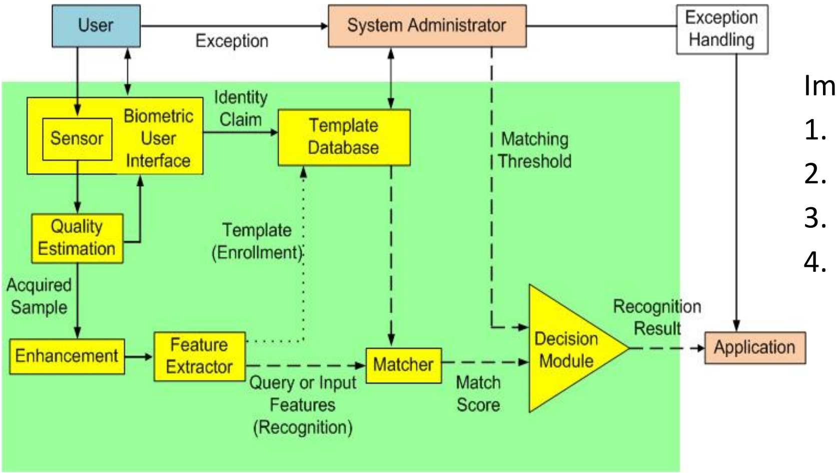


3-Biometric Systems

- **Definition**:
  - Biometric systems are **using biometrics to authenticate or identify a person**. A system **collects** biometric characteristics unique to every person. These biometric characteristics are then directly linked to verify or identify the individual.
- Two phases:
  - Biometric enrollment
  - Recognition



More details of Biometric Systems



Important Biometric Subsystems

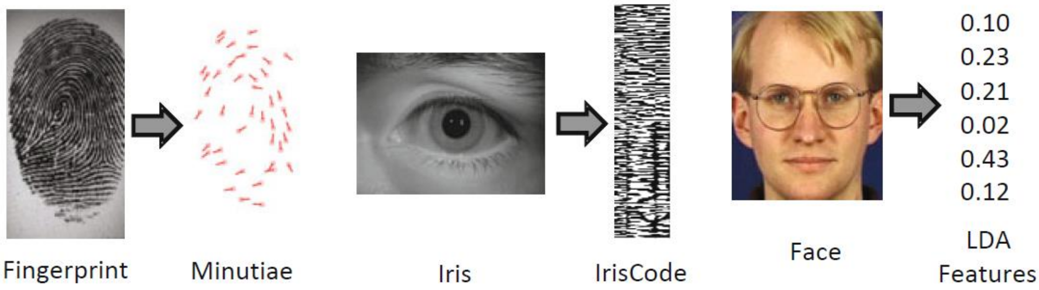
1. Biometric enrollment
2. Feature extractors
3. Template database
4. Feature Matchers

3.1 Biometrics Enrollment

- Biometric sensors
- Requirements:
  - Good human-machine interface
  - Quick acquisition
  - Good quality
- Quality of biometric samples
  - Depends on the characteristics of sensors
  - Most sensors, raw biometric data in the form of 2D images (finger prints, face, iris, gait,…)
    - Resolution
    - framerates
    - sensitivity

Examples of fingerprint resolution

3.2 Feature extraction



Fingerprint

Minutiae

Iris

IrisCode

Face

0.10
0.23
0.21
0.02
0.43
0.12

LDA
Features

- Preprocessing:
  - Quality assessment
  - Segmentation
  - enhancement
- Feature extraction:
  - Compact but expressive representation of biometric samples
  - Biometric traits

3.3 Biometric database

- Store templates (biometrics traits or features) of enrolled biometrics samples
- Raw data (such as images) can also be stored in the database with templates during enrollment, they can be referred as
  - Gallery images
  - Reference images
  - Enrollment images

  While the test images acquired during recognition phase are called
  - probe images
  - query images
  - input images

3.3 Biometric database

- Personal information
  - Name
  - Personal identification number
  - Address, vv.

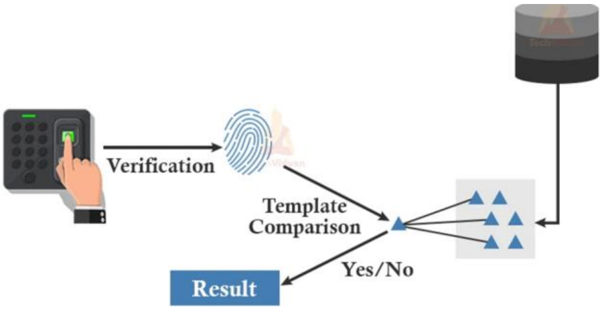
2.3 Biometric database

- Centralized database
  - More secure through physical isolation
  - But it is also a target for attacking

- Decentralized database

3.4 Biometric matcher

- Compare **query features** vs. **stored templates** to generate match score



4- Types of Biometric Recognition

- A standard biometric system has two functionalities
  - Verification or Authentication
  - Identification

4.1 Verification (Authentication)

- The system has to answer the question
  - “Are you who you say you are?”

- Identity claim:
  - PIN
  - Name
  - A token (eg., smartcard)

- Examples:
  - Smartphone login with finger

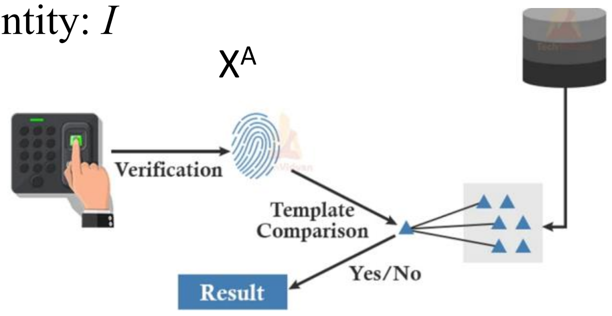
4.1 Verification (Authentication)

User A

claimed identity: I

X^A

X^E_I



User A

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

4.2 Identification

- Identification can be further classified into **positive** and **negative** identification by the questions:
  - Positive: “**Are you someone who is known to the system**?”
  - Negative: “**Are you who you say you are not**?”.

- Positive identification example: computer login with face recognition or fingerprint

4.2 Identification

- Negative identification example:
  - At the border control (airport), the officers have to check whether you are someone in the "watch-list"

4.2 Identification

- In both identification, user's biometric input is compared with templates of all the persons enrolled in the database to find the identity with highest similarity.

- Open-set identification:

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

database $\{\underbrace{I_1, I_2, \cdots, I_N}_{\text{Enrolled identity}}, \underset{\text{unsuitable identity}}{\underset{\searrow}{I_{N+1}}}\}.$

4.2 Identification

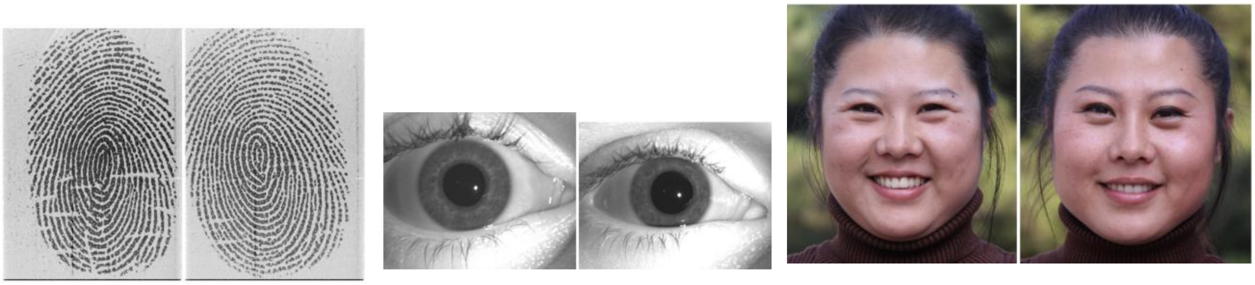
- Close-set identification: the output identity is known

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

database $\{\underbrace{I_1, I_2, \cdots, I_N}_{\text{Enrolled identity}}, \underset{\text{unsuitable identity}}{\cancel{I_{N+1}}}\}.$

5. Biometric System Errors

- Science of biometric recognition is based on two fundamental premises with a biometric trait:
  - Uniqueness
  - Permanence



Biometrics of twins

5. Biometric System Errors

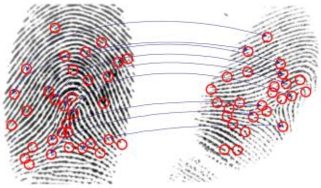
- However, these two premises are seldom true.
- Because
  - Physical trait may not be unique
  - Biometrics may change overtime

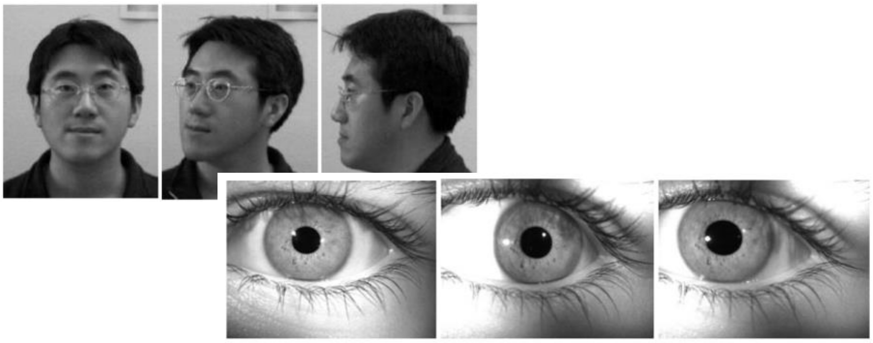
Stage 1: unilateral involvement; early masking of facial expression; affected arm in semiflexed position with tremor.
Stage 2: bilateral involvement with early postural changes; slow, shuffling gait with decreased excursion of legs.
Stage 3: pronounced gait disturbances and moderate generalized disability; postural instability with tendency to fall

37

Variation of biometric traits

- Intra-user variations (or intra-class variations). This is due to reasons:
  - Imperfect sensing conditions (eg., noise, system errors)
  - Alteration in biometric characteristics
  - Changes in ambient conditions (eg., inconsistent illumination)
  - Variations in the interaction with the sensor,....

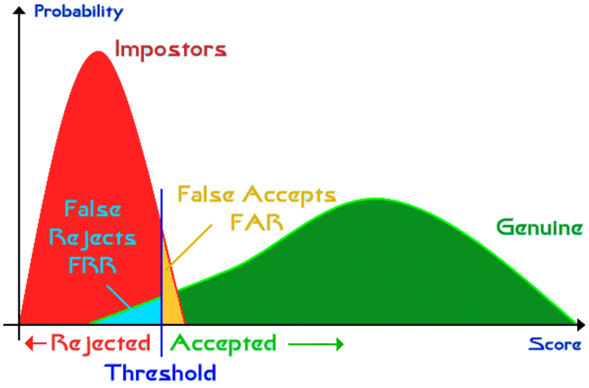




6. Performance measures

- In biometric verification, there are two popular metrics
  - False Rejection Rate (FRR) and False Acceptance Rate (FAR), also
  - False Non-match Rate (FNMR) and False Match Rate (FMR)

  which are computed based on the genuine and imposter match score distribution

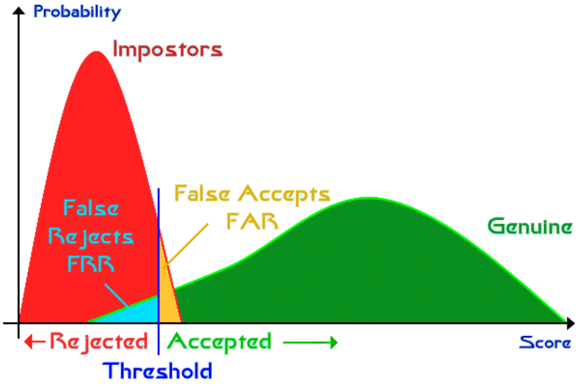


6. Performance measures

- Given a threshold η:

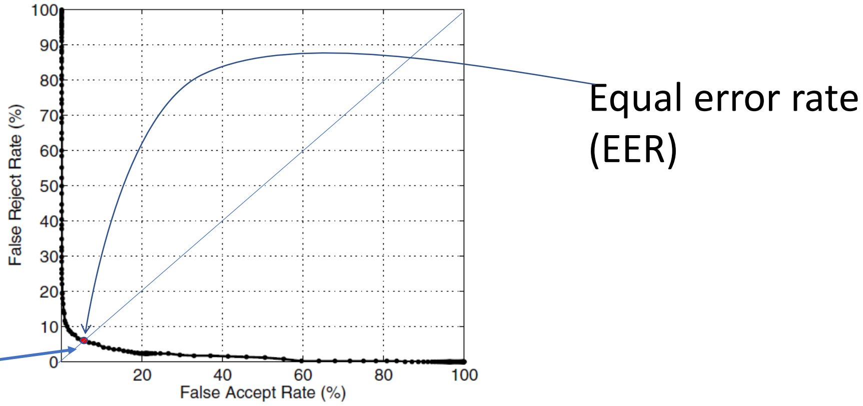
$$FAR(\eta) = p(s \geq \eta | \omega_0) = \int_{\eta}^{\infty} p(s|\omega_0)ds,$$

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



6. Performance measures

- When changing the threshold η, we have variation of FAR(η) and FRR(η)

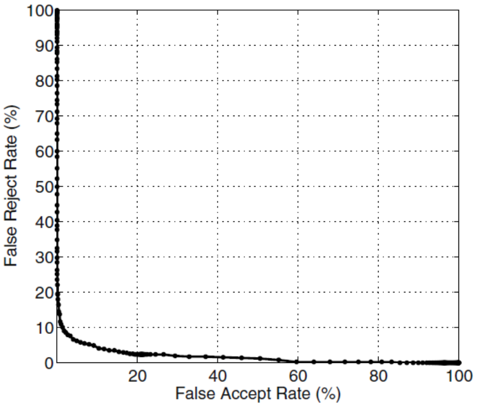


Equal error rate (EER)

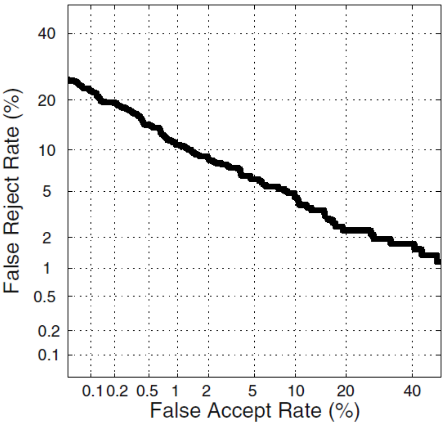
Area under curve (AUC)

Detection Error Tradeoff (DET) curve

6. Performance measures



Biometric system 1

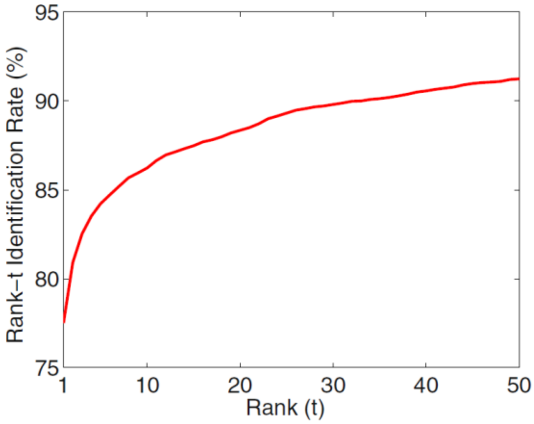


Biometric system 2

Which system has better performance?

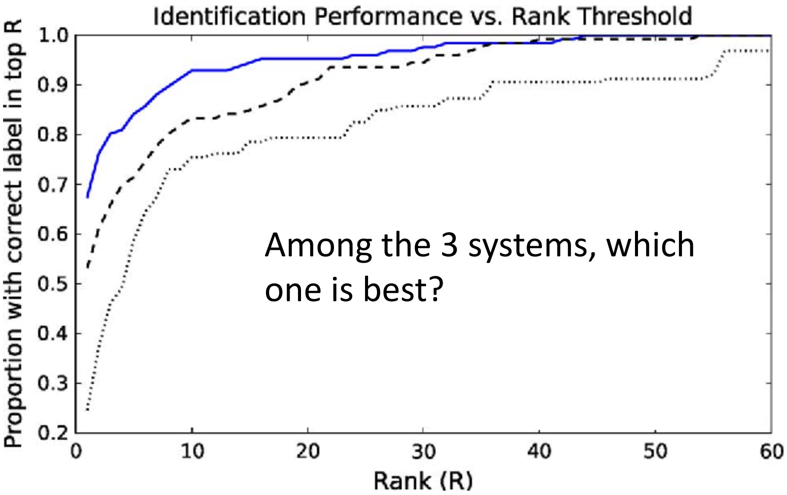
6. Performance measures

- In biometric identification, the output can be top t matches (1 ≤t≤N)
- The metric is called Rank(t).



6. Performance measures

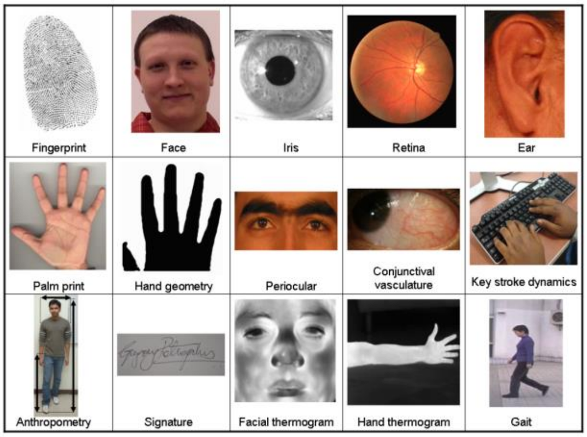
- Identification system



Among the 3 systems, which one is best?

7. Choice of biometric traits

- Number of biometric traits are being used in real applications. Each trait has its pros and cons.
- In general 7 factors should be considered:
  - **Universality**
  - **Uniqueness**
  - **Permanence**
  - **Measurability**
  - **Performance**
  - **Acceptability**
  - **Circumvention**



Popular biometric traits