ISEL

INSTITUTO SUPERIOR
DE ENGENHARIA DE LISBOA

PROCESSAMENTO DE IMAGEM E BIOMETRIA

IMAGE PROCESSING AND BIOMETRICS

2. **FUNDAMENTALS OF BIOMETRIC SYSTEMS**

Summary

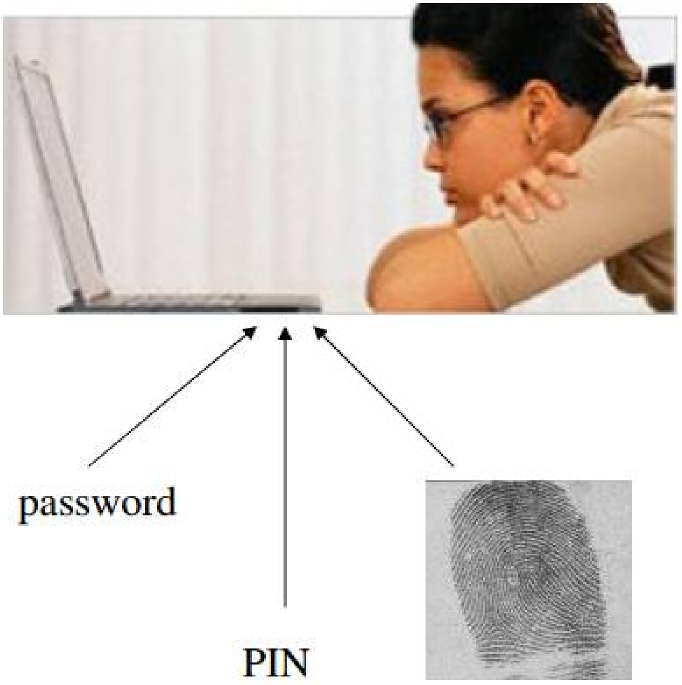
- Biometrics
- Biometric Traits
- Biometric Systems

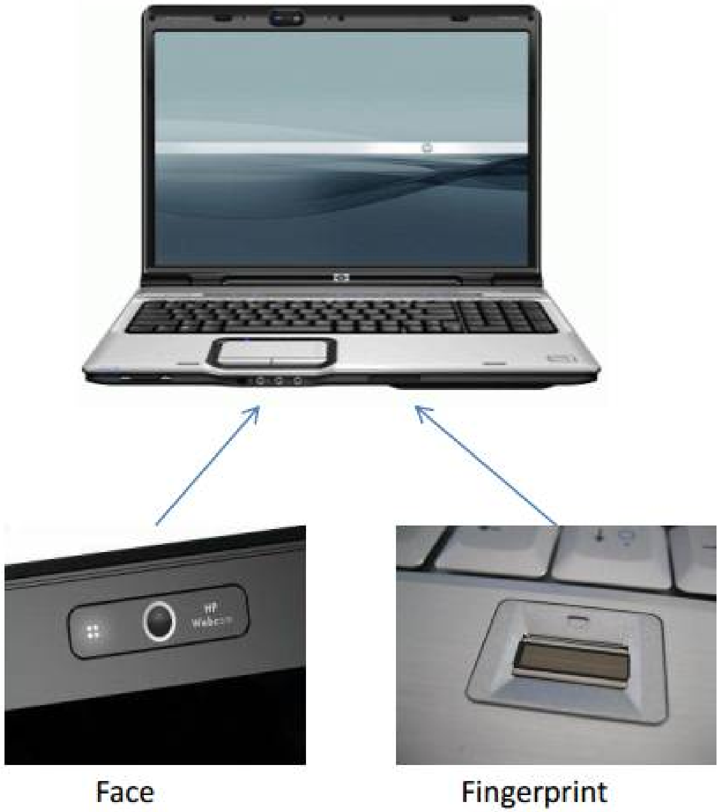
Biometrics (1)

- Biometrics is derived from two Greek words
  - *bio* (life)
  - *metric* (to measure)
  - It analyzes a person’s physiological and/or behavioral characteristics
  - The characteristics should be unique to each person/individual
  - The characteristics should be collectable by some device

Biometrics (2)

- Instead of performing identity verification by what the user *knows*, it is done by what the user *is* or how he/she *behaves*





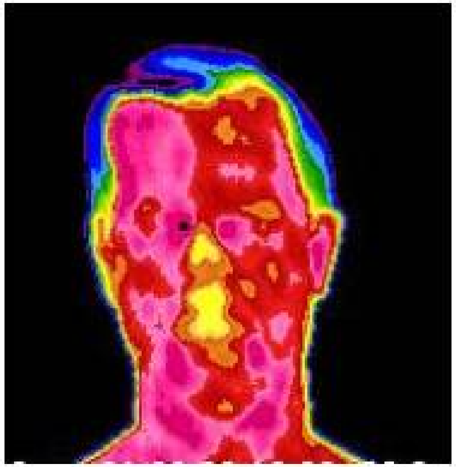
Biometrics (3)

- *Biometrics* are automated methods of recognizing a person based on a physiological or behavioral characteristic

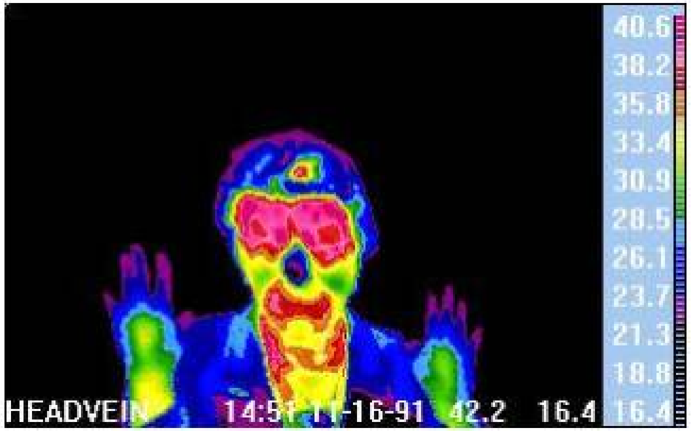
- *Biometrics* is the science of establishing the identity of an individual based on physical, chemical, or behavioral attributes of the person

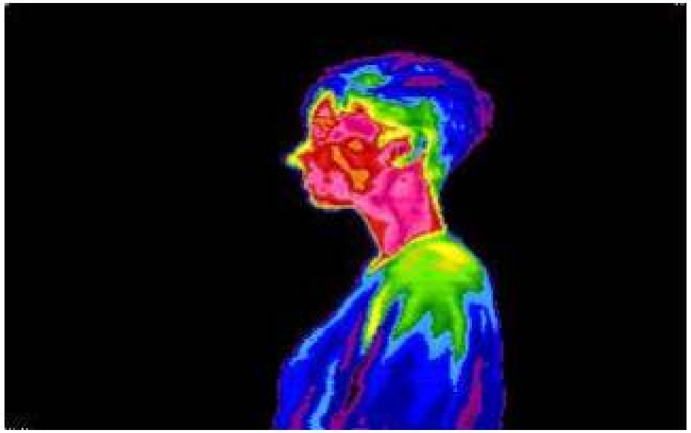
A. Jain, P. Flynn, A. Ross, “Handbook of Biometrics,” Springer, 2007

Biometric Traits (1)

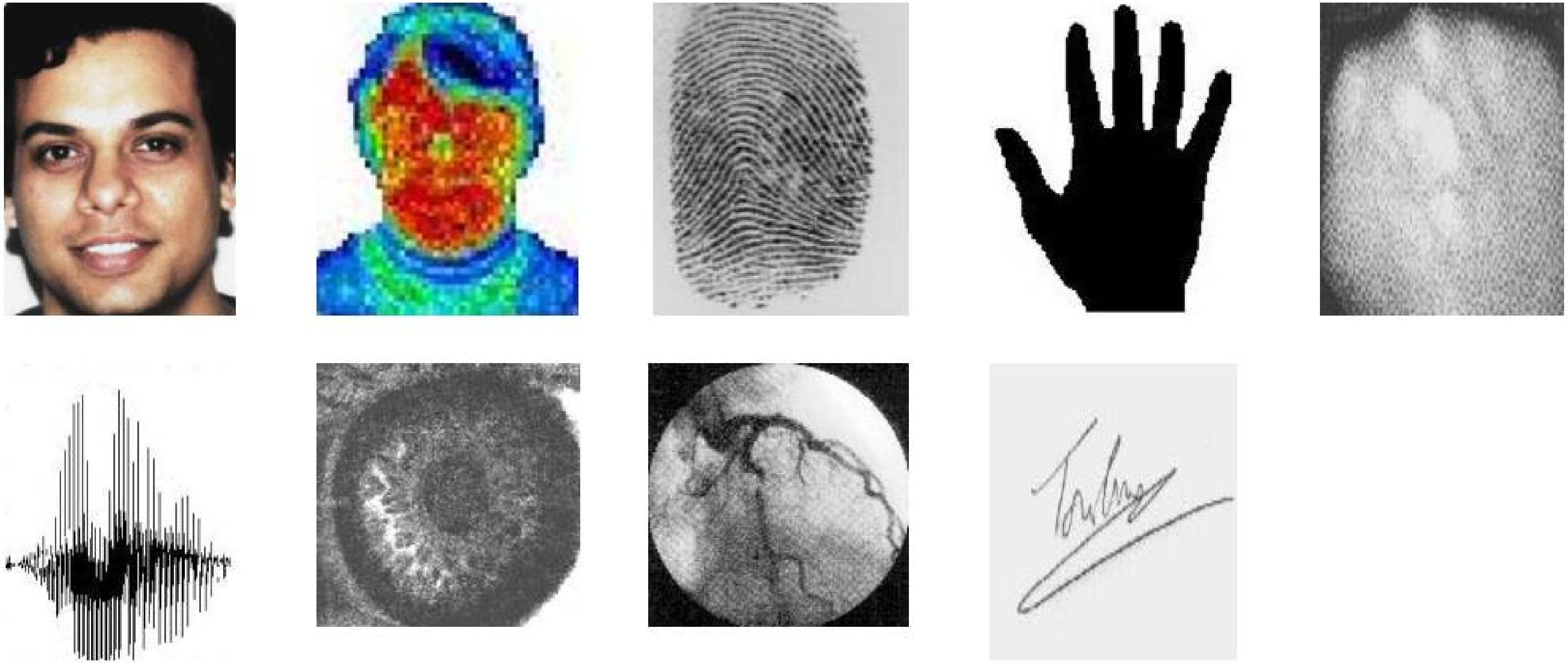


Biometric Traits (2)

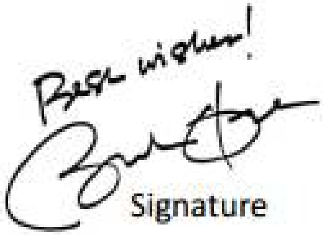




Biometric Traits (3)

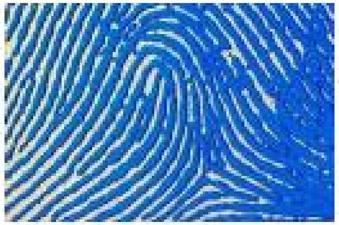


Biometric Traits (4)

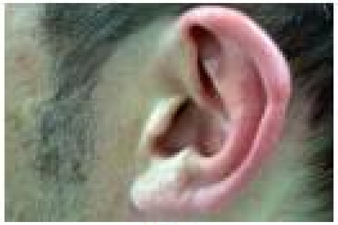

Best wishes!

Signature

Gait

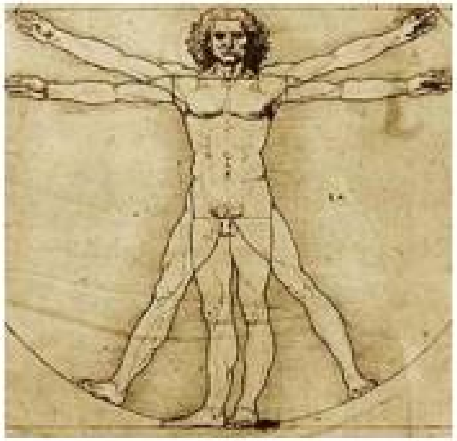


Fingerprint



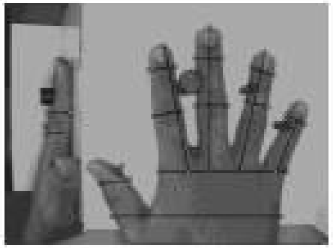
Ear

Face



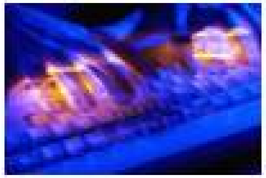
Iris

Hand
Geometry

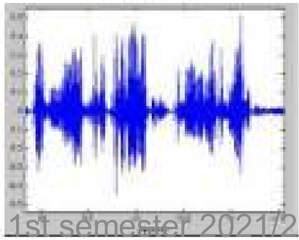


Facial
Thermogram

Keystroke
Dynamics

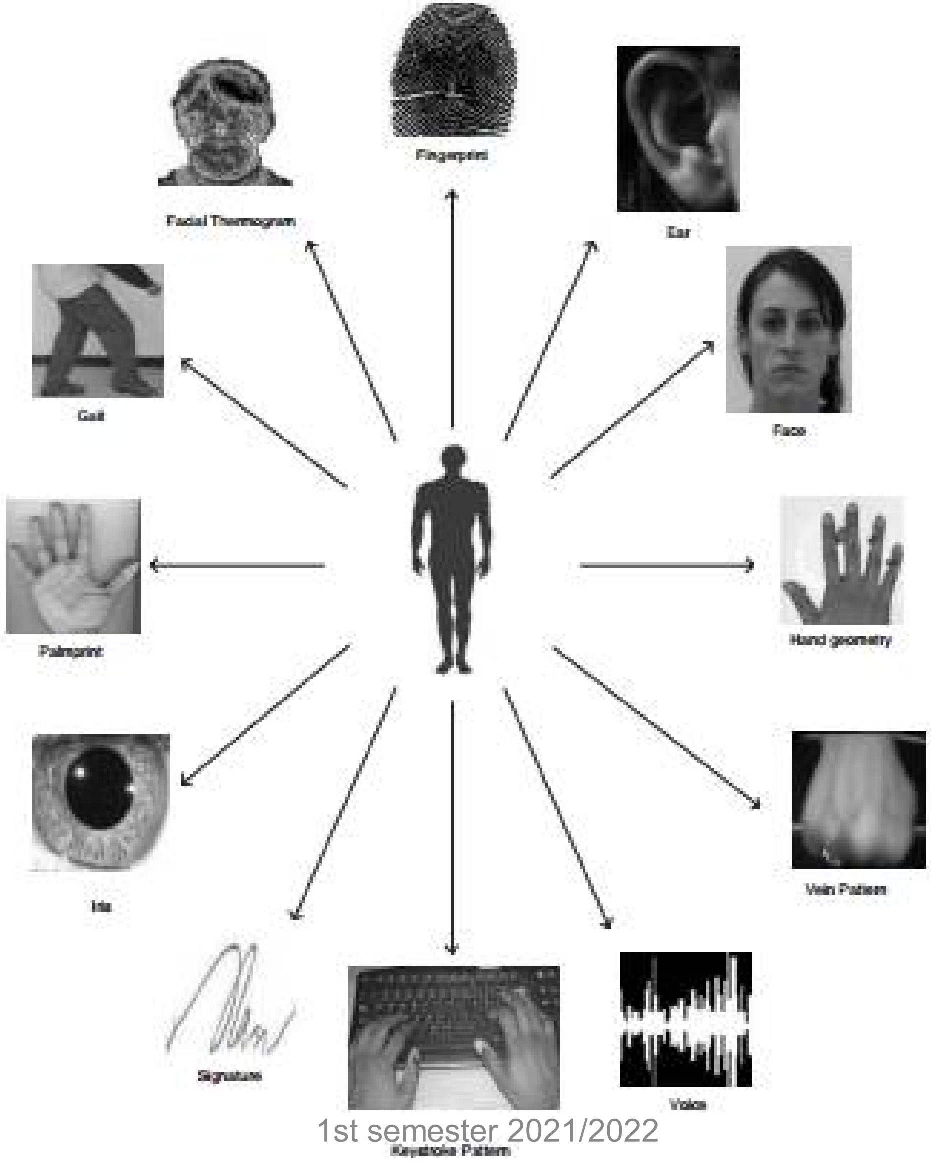


Voice



Vein Pattern

Biometric Traits (5)



Biometric Traits (6)

Accepted biometrics:

- voice
- hand geometry
- gait
- ear
- face
- iris
- retina
- infrared facial thermogram
- hand vein thermogram
- key stroke
- *fingerprint*
- *signature*
- *DNA*

Biometric Traits (7)

What biological measurements qualify to be a biometric?

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- ***Universality -*** each person should have the characteristic
- ***Distinctiveness -*** any two persons should be sufficiently different in terms of the characteristic
- ***Permanence -*** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time
- ***Collectability -*** the characteristic can be measured quantitatively

A. Jain, A. Ross, S. Prabhakar, An Introduction to Biometric Recognition, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004

Biometric Systems (1)

- A Biometric System

is a pattern recognition system

that uses some

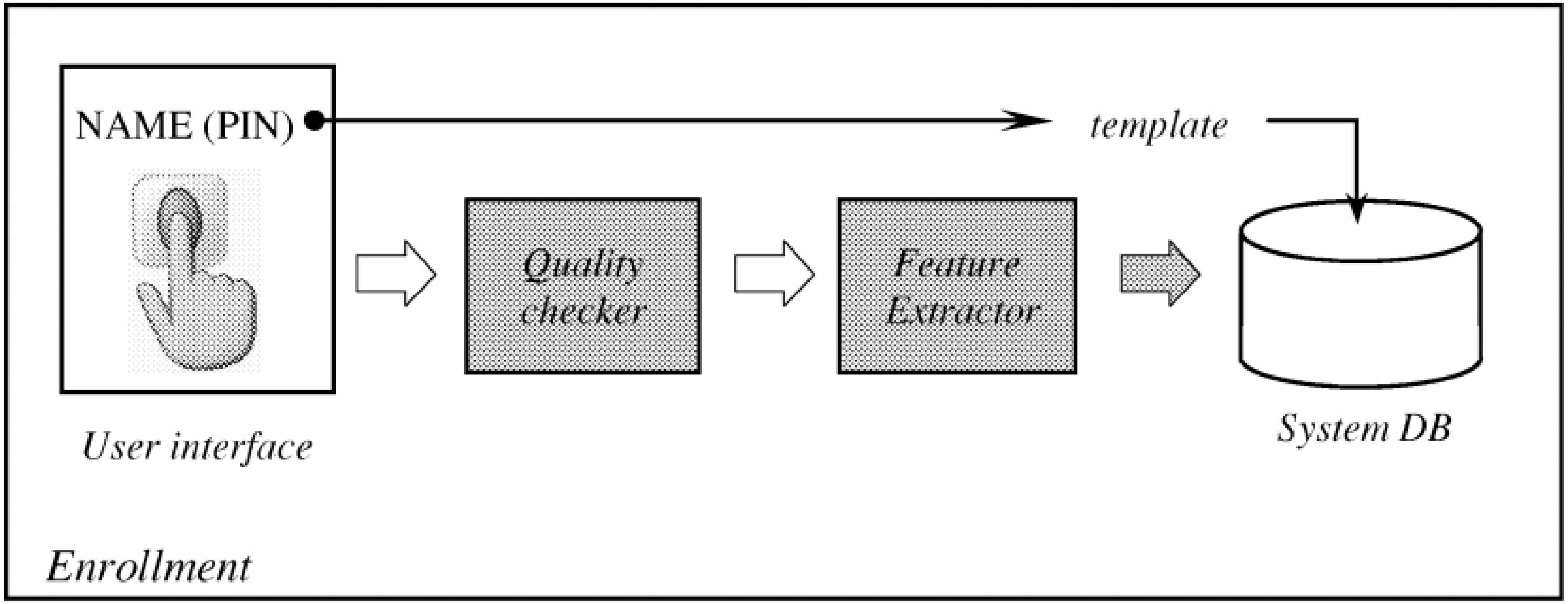
biometric trait to perform user verification/identification

Biometric Systems (2)

- A biometric system is a pattern recognition system
- It acquires biometric data from an individual
- Extracts salient feature sets from the data
- Compares this feature set against the feature set(s) stored in the database
- Executes an action based on the result of the comparison

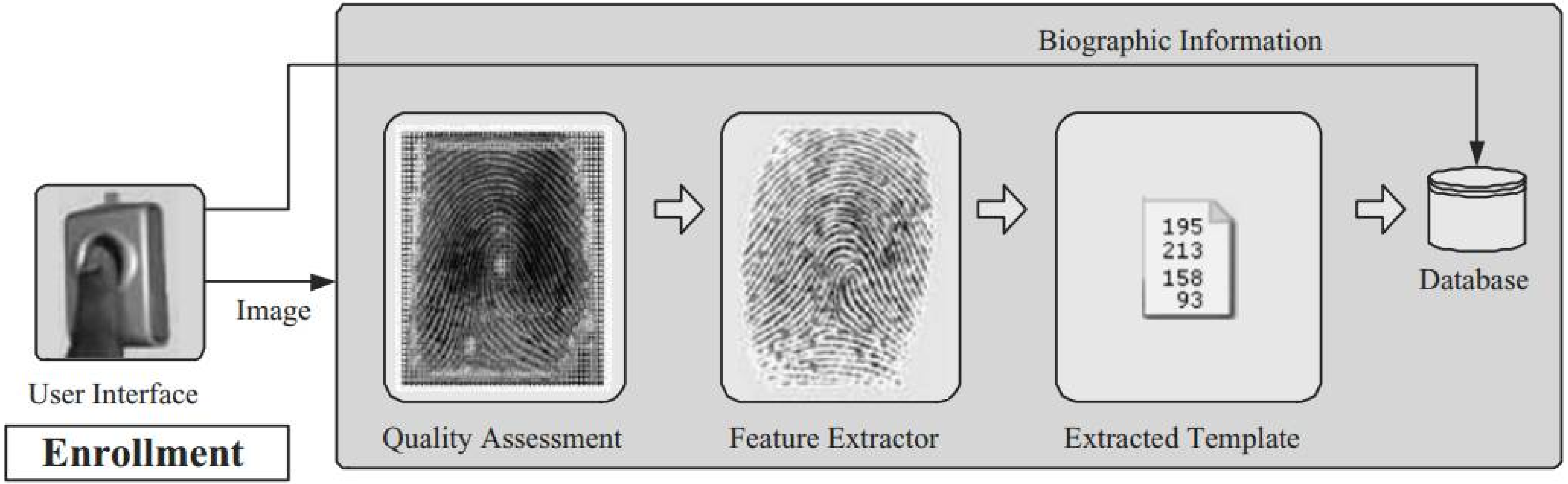
Biometric Systems (3)

- It works on two phases:
  1) **Enrollment**
  2) Verification/Identification



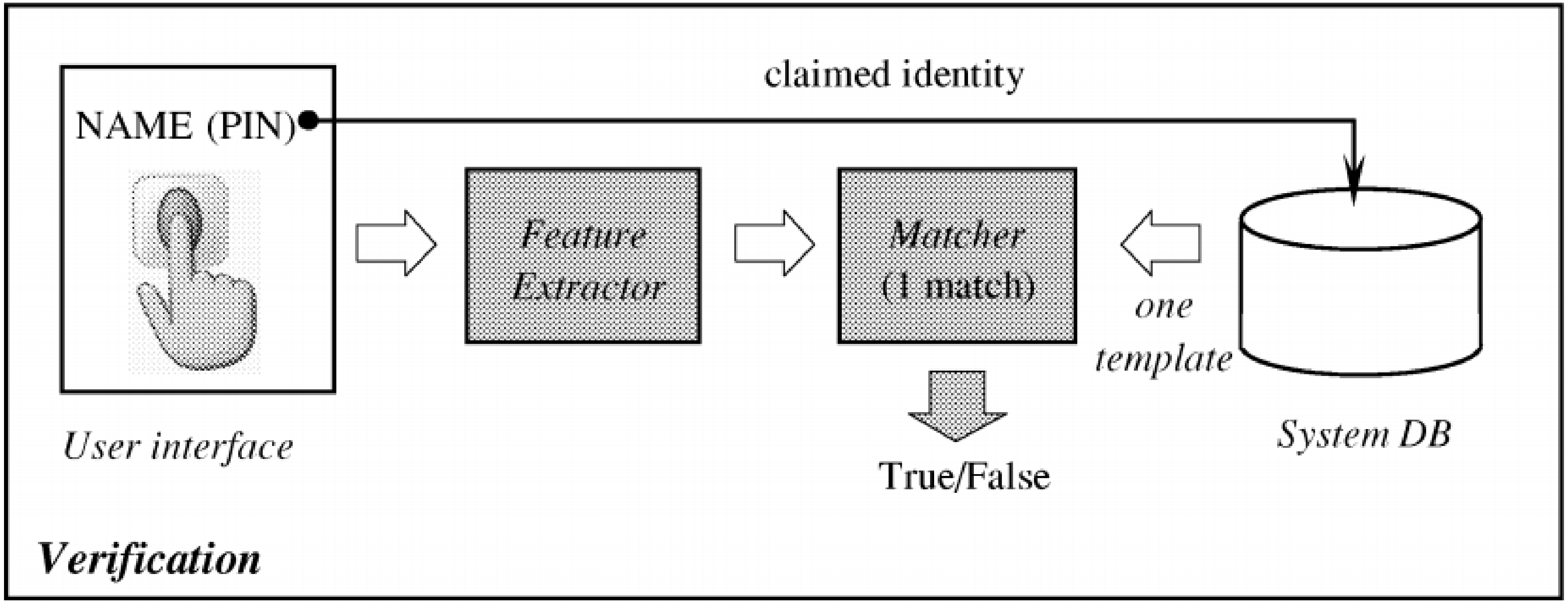
Biometric Systems (4)

- It works on two phases:
  1) **Enrollment**
  2) Verification/Identification



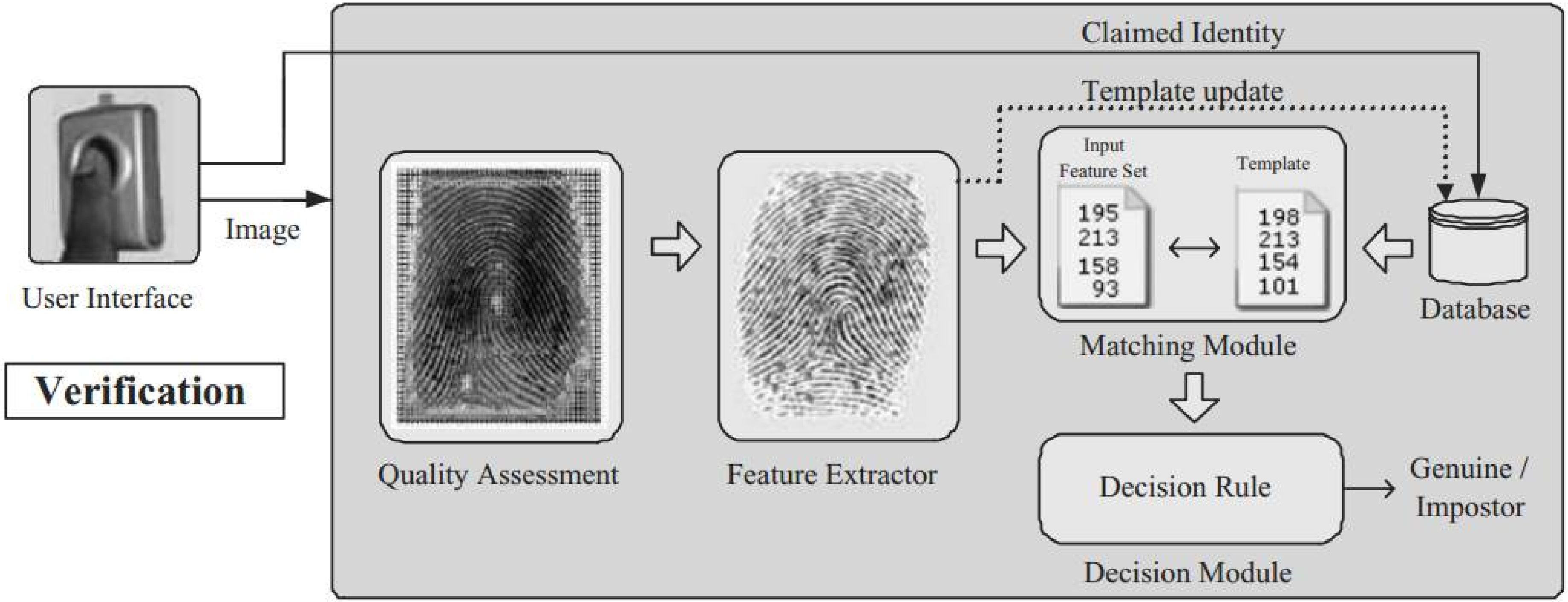
Biometric Systems (5)

- It works on two phases:
  1) Enrollment
  2) **Verification/Identification**



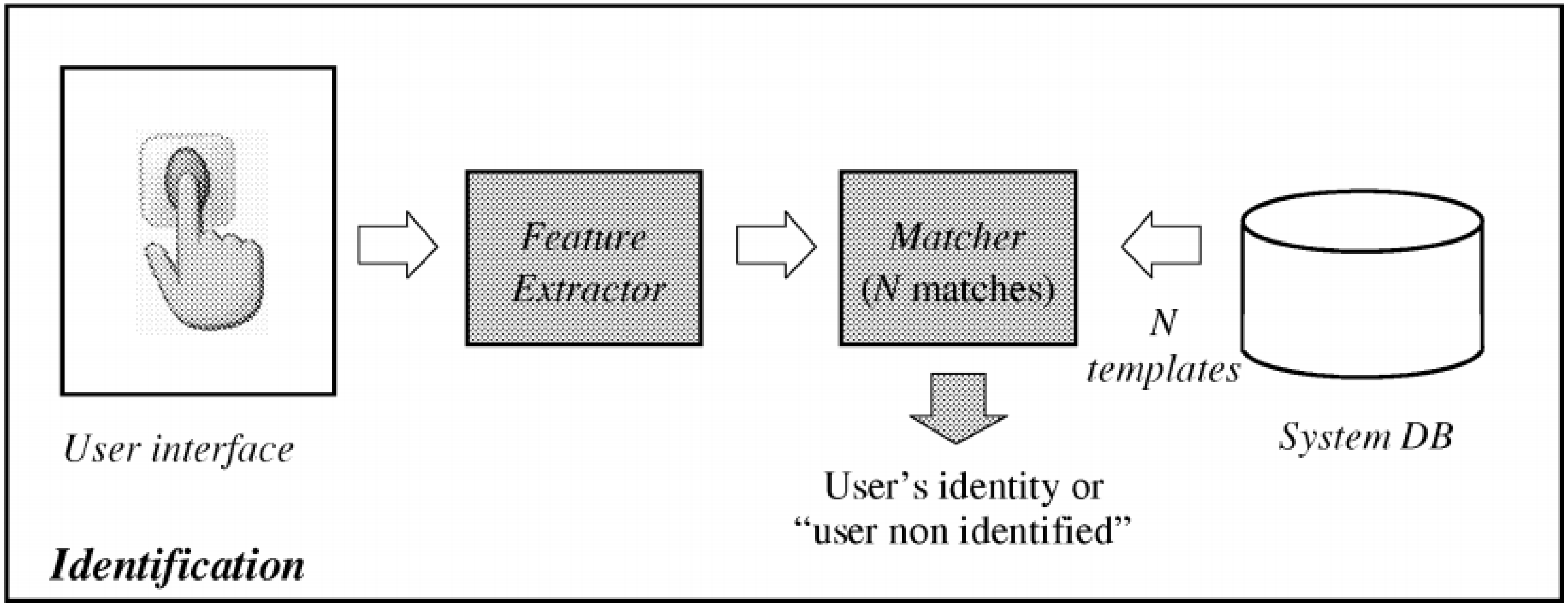
Biometric Systems (6)

- It works on two phases:
  1) Enrollment
  2) **Verification/Identification**



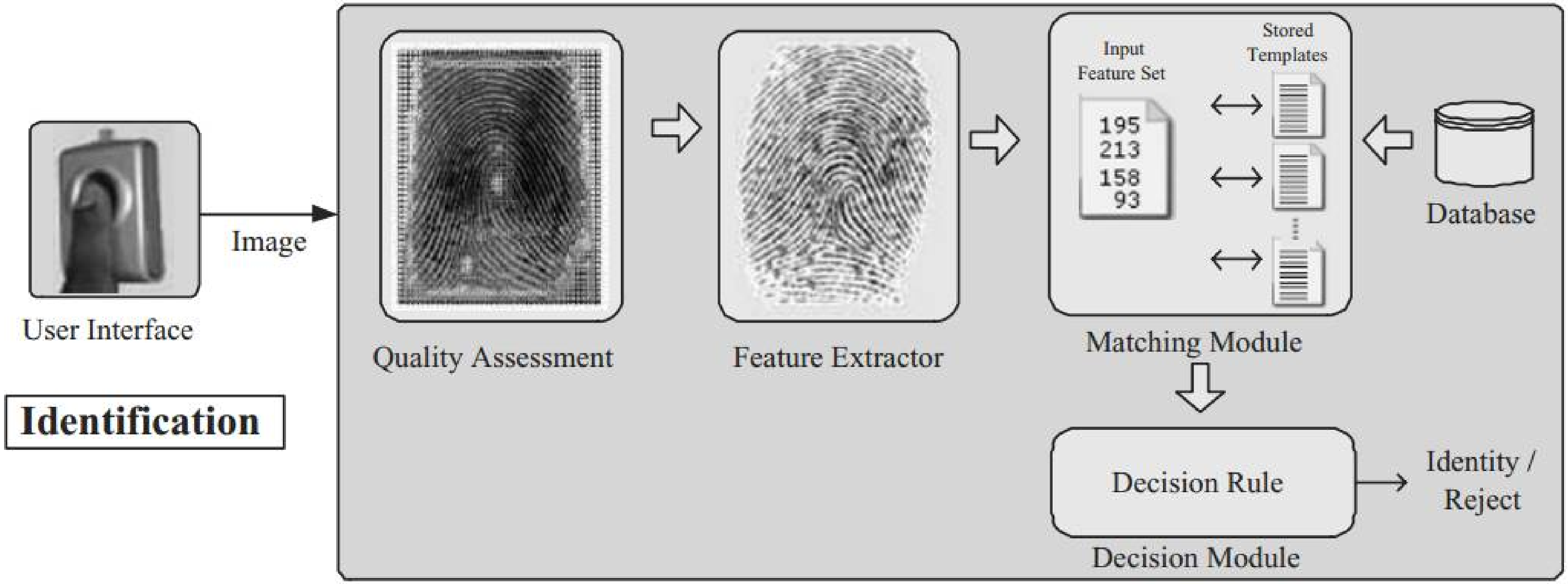
Biometric Systems (7)

- It works on two phases:
  1) Enrollment
  2) **Verification/Identification**



Biometric Systems (8)

- It works on two phases:
  1) Enrollment
  2) **Verification/Identification**



Biometric Systems (9)

Some other issues, on biometric systems:

- ***Performance***
- the achievable recognition accuracy and speed
- the resources required to achieve the desired recognition accuracy and speed
- the operational and environmental factors that affect the accuracy and speed

- ***Acceptability***
- the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives

- ***Circumvention***

How easily the system can be fooled using fraudulent methods

Biometric Systems (10)

A practical biometric system should:

- meet the specified recognition accuracy, speed, and resource requirements
- be harmless to the users
- be accepted by the intended population
- be sufficiently robust to various fraudulent methods and attacks to the system

A. Jain, A. Ross, S. Prabhakar, An Introduction to Biometric Recognition, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004

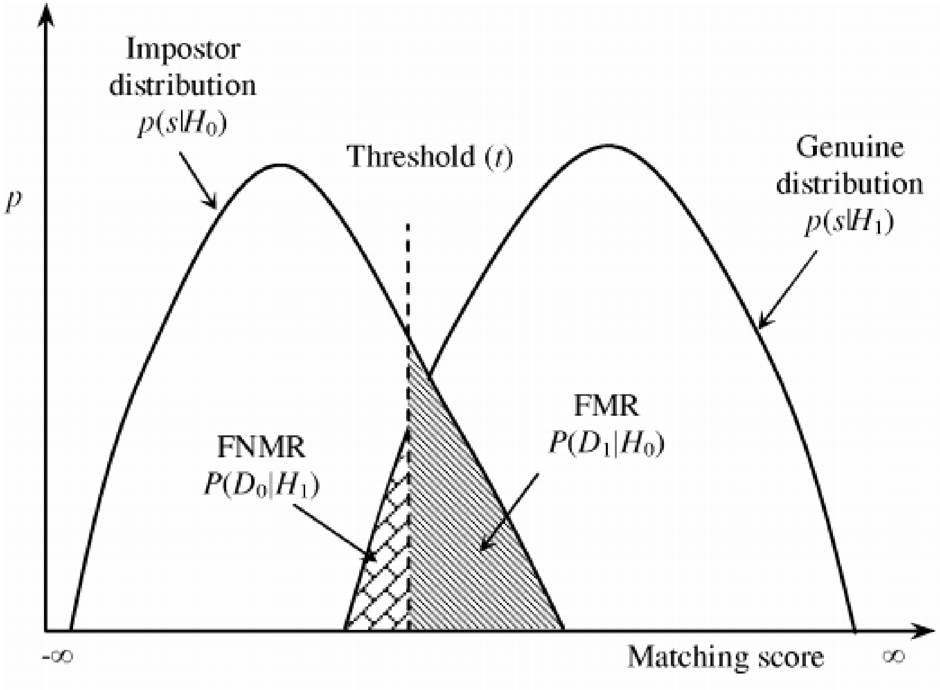
Biometric Systems (11)

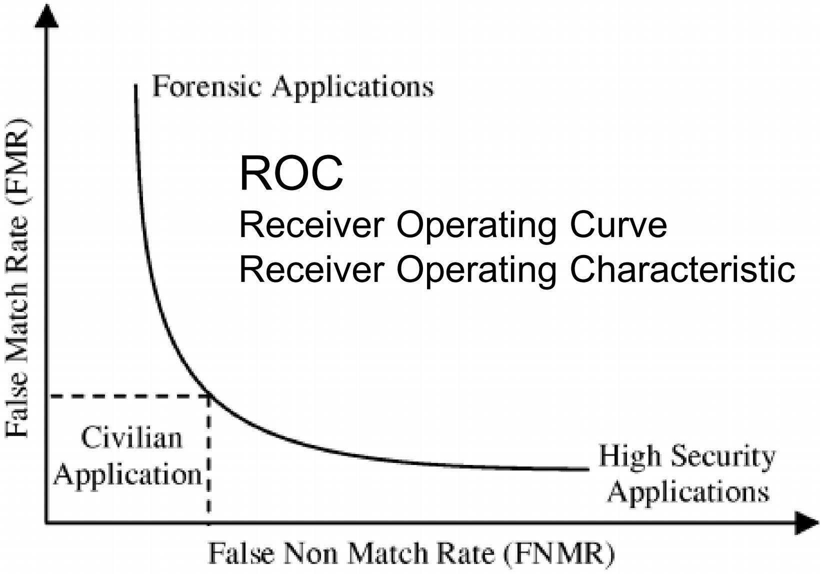
- Some common metrics
  - FTE – Failure to Enroll (on the enroll phase)
  - FMR – False Match Rate
  - FNMR – False Non-Match Rate

Biometric Systems (12)

- FMR – False Match Rate
  - FPR – False Positive Rate or FAR – False Accept Rate

- FNMR – False Non-Match Rate
  - FNR – False Negative Rate or FRR – False Reject Rate





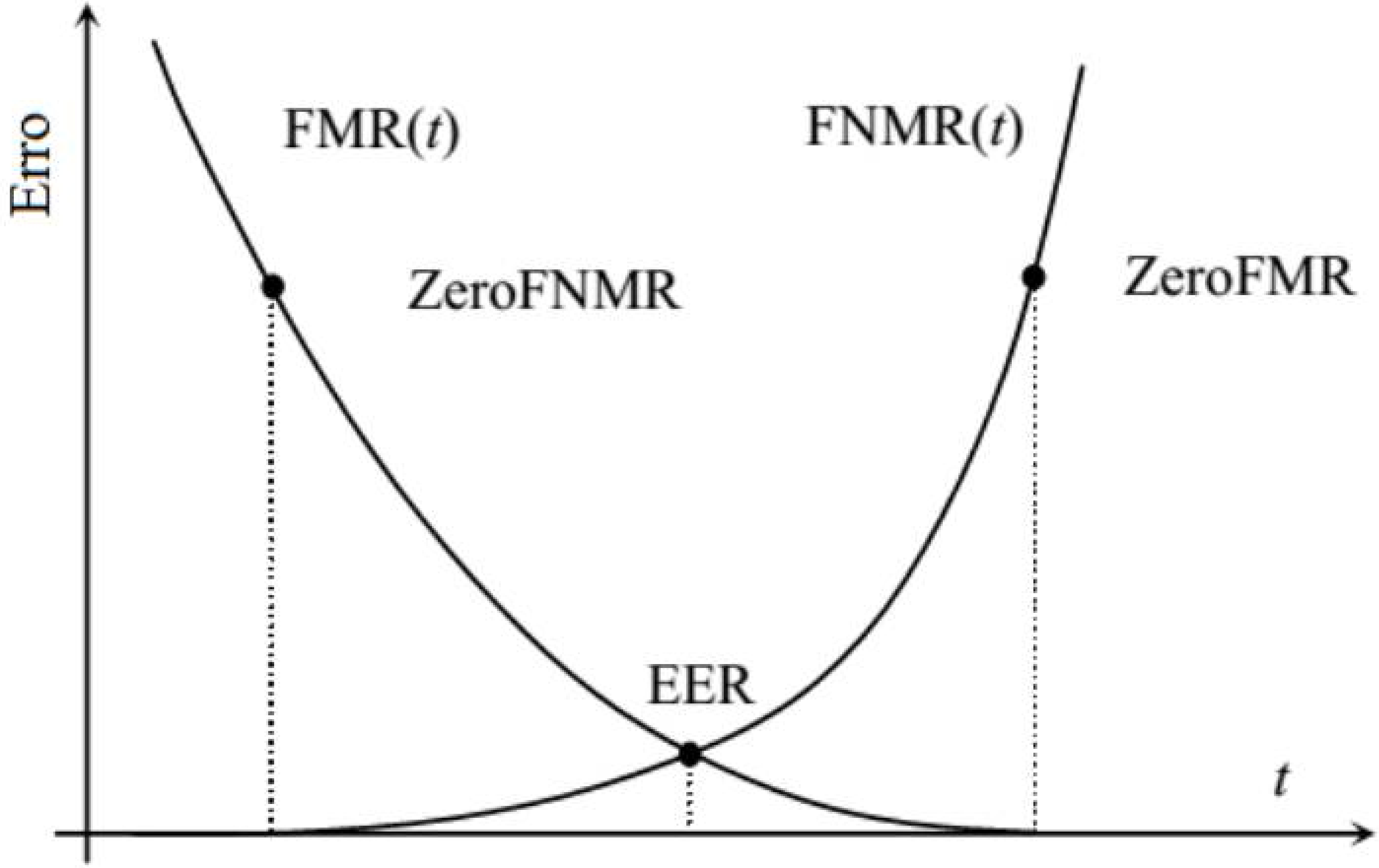
ROC

Receiver Operating Curve

Receiver Operating Characteristic

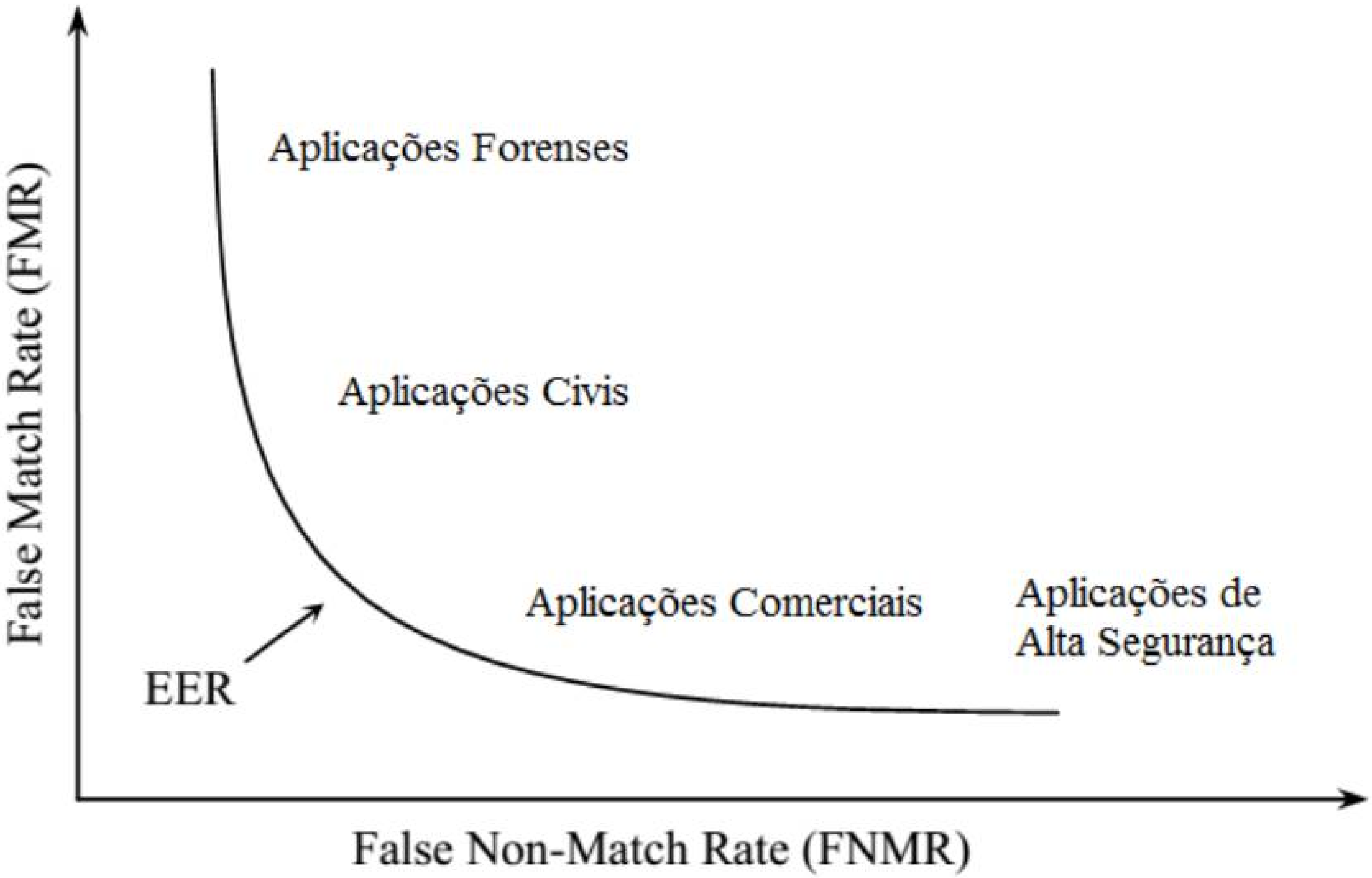
Biometric Systems (13)

- EER – Equal Error Rate



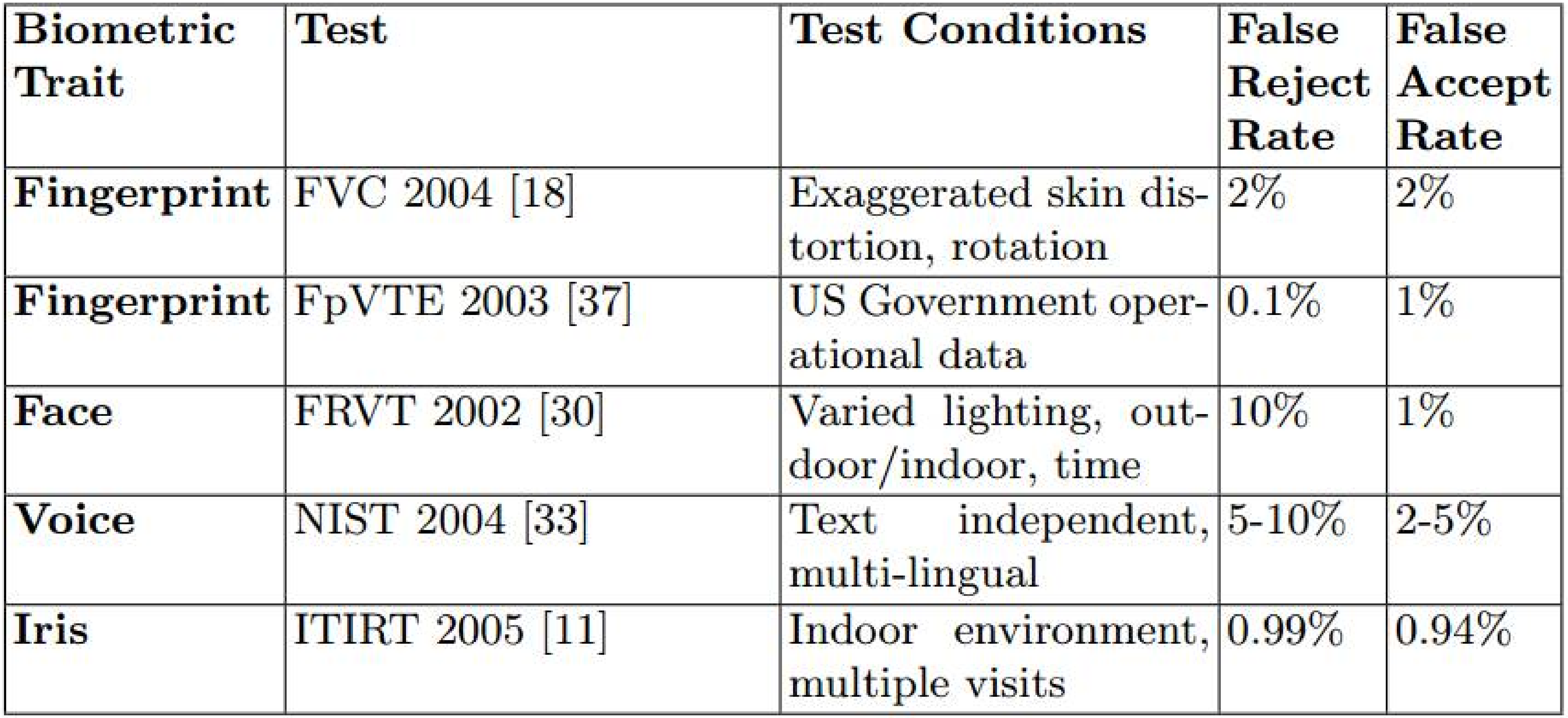
Biometric Systems (14)

- ROC



Biometric Systems (15)

- FAR and FRR for common modalities



Biometric Trait	Test	Test Conditions	False Reject Rate	False Accept Rate
Fingerprint	FVC 2004 [18]	Exaggerated skin distortion, rotation	2%	2%
Fingerprint	FpVTE 2003 [37]	US Government operational data	0.1%	1%
Face	FRVT 2002 [30]	Varied lighting, outdoor/indoor, time	10%	1%
Voice	NIST 2004 [33]	Text independent, multi-lingual	5-10%	2-5%
Iris	ITIRT 2005 [11]	Indoor environment, multiple visits	0.99%	0.94%