Biometrics Introduction

By

Hafez Barghouthi

Definition

”Biometric Technologies” are

automated methods

of verifying or recognizing the identity of a **living person** based on

a **physiological**

or **behavioural** characteristic

Definition Explaining

- Automated
  - Different from human identification

- Living person
  - Single persons, no groups
  - Alive not dead (just JOKING)☺

Definition Explaining

- Physiological biometrics
  - Fingerprint, Iris, Face, Hand

- Behavioural biometrics
  - Signature, Gait, Voice

History - 1

- Dates back to ancient Egypt
- Anthropometry (bodily measurements):
  - Adolphe Quetelet (1871), Belgian mathematician
  - Alphonse Bertillon (1880’s), French policeman
- Fingerprints and palmprints
  - Used already by Babylonian kings
  - Jan Evangelista Purkinje, Czech studying sweat glands
  - Juan Vucetich, Argentinian policeman, first to take fingerprints in ink
  - Francis Galton, Edward Henry: Galton-Henry system for classification

History - 2

- Fingerprints and facials, 1880’s, Henry Faulds, William Herschel and Francis Galton
- fingerprint recognition on current form, 1960’s
- Hand geometry, 1970’s
- Retinal, signature and face verification, 1980’s
- Iris recognition, 1990’s
- Newer and newer: gait, keystroke dynamics, mouse movement, cardiac sounds, brain waves

Positive / Negative

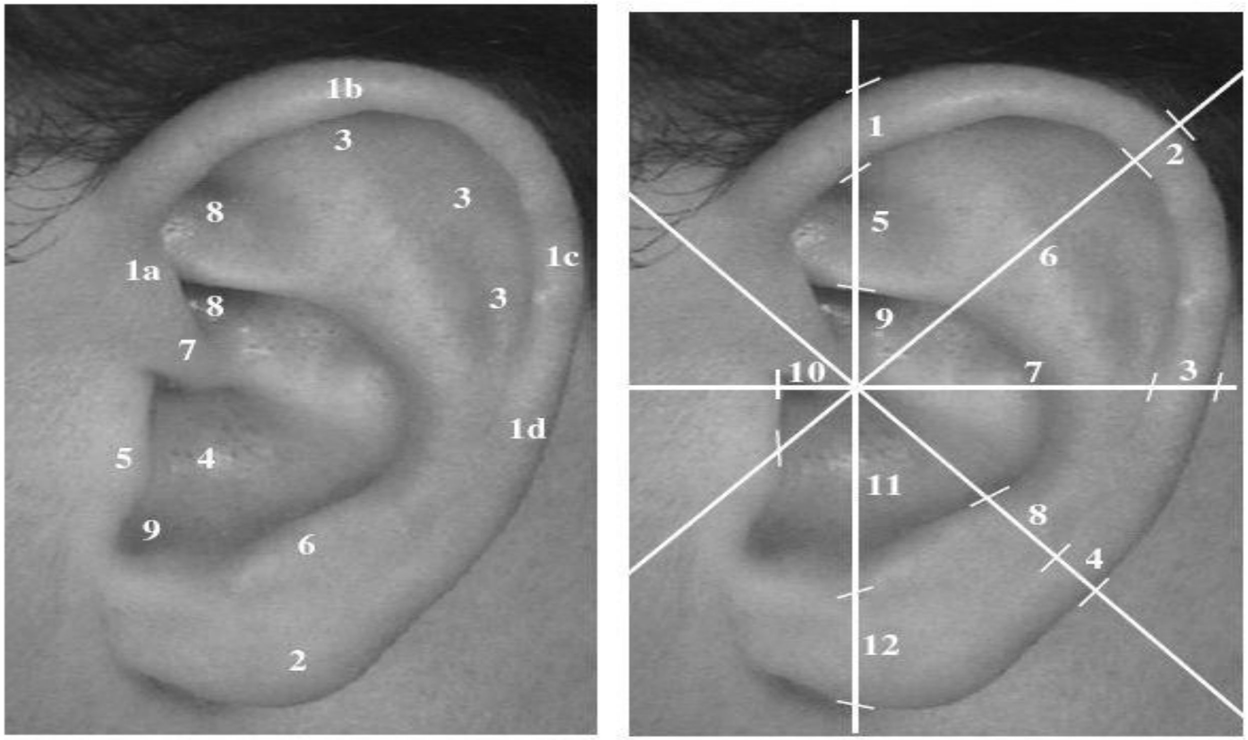
- Positive recognition
  - To prevent multiple people from using the same identity
- Negative recognition
  - To prevent one person from using multiple identities

Physiological / Behavioural

- Physiological:
  - Physical features ”unchangeably” attached to a person
  - E.g. fingerprint, DNA, and face
- Behavioural:
  - Behaviour that is very specific to a person
  - E.g. signature, gait, and voice

Examples - Ear

- Shape of ear can be used for authentication



(a) Anatomy.

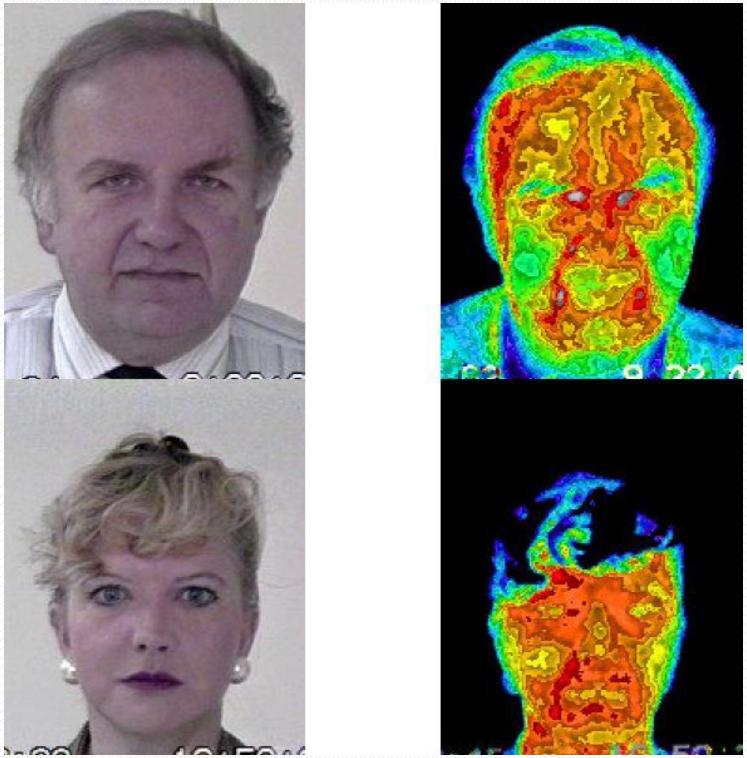
(b) Measurements.

Examples - Face

- Used by humans
- Many different techniques available

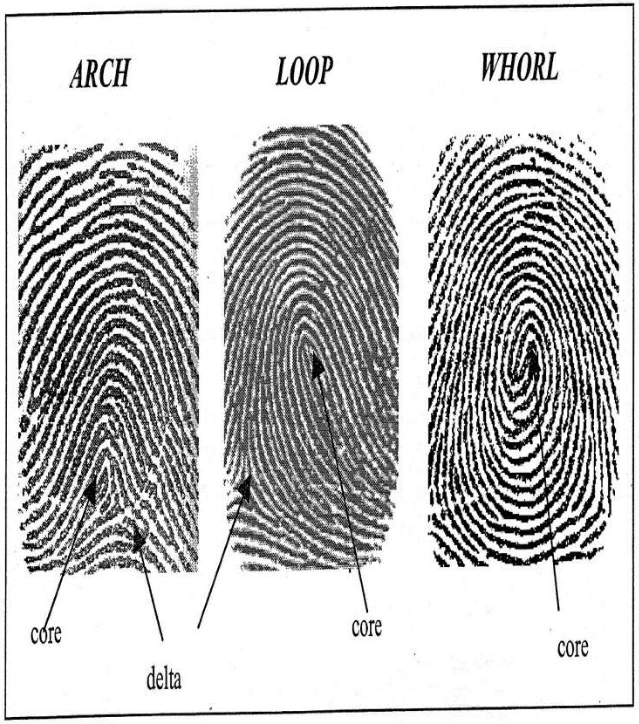
Examples - Thermograms

- Facial, hand, hand vein

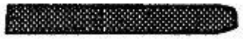
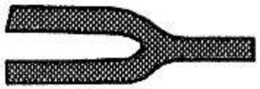
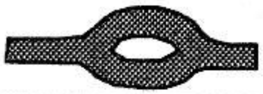
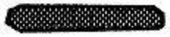
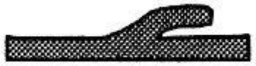
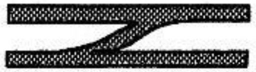


Examples - Fingerprint

- Global features

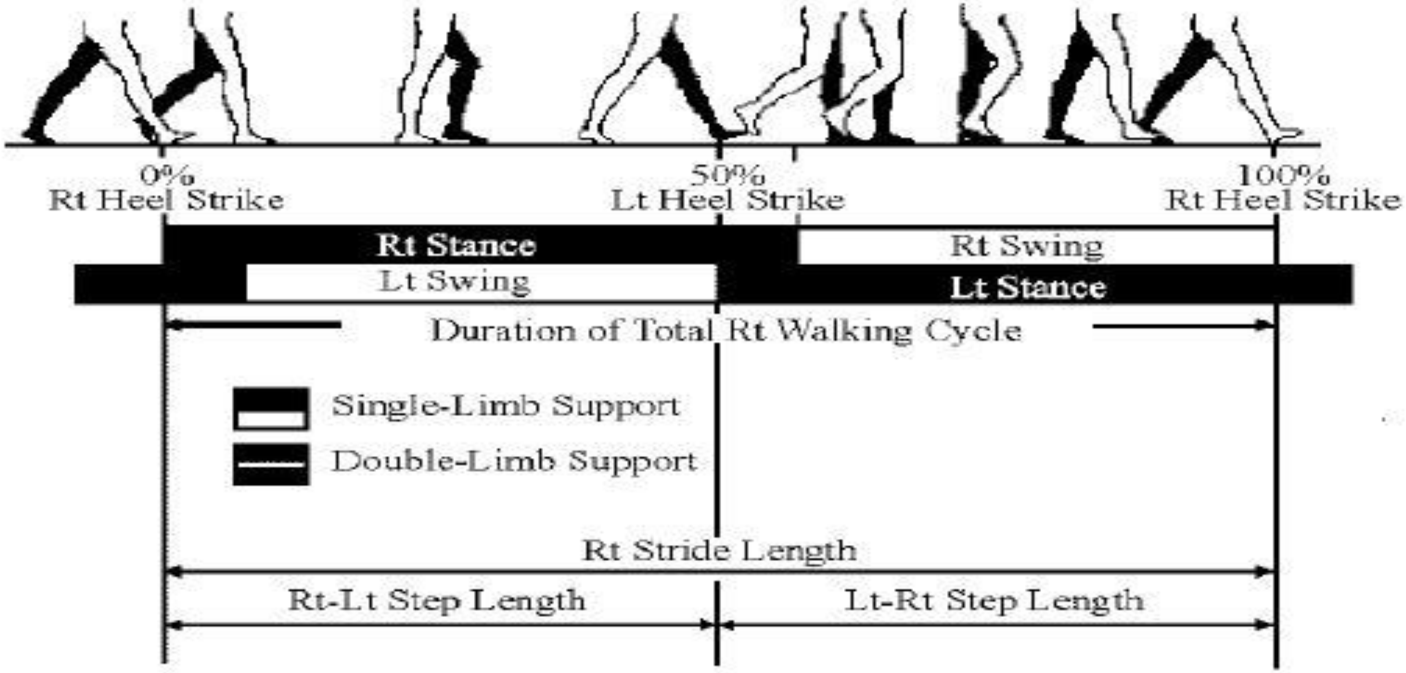


Local features

	Termination
	Bifurcation
	Lake
	Independent ridge
	Point or island
	Spur
	Crossover

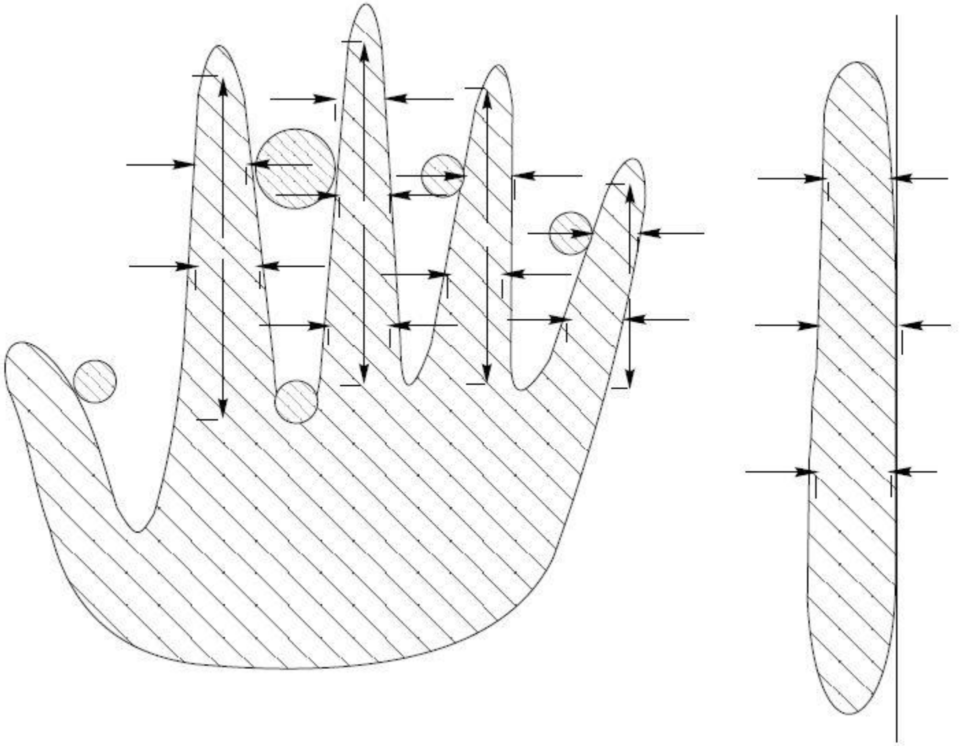
Examples - Gait

- "Great Juno comes; I know her by her gait" from "The Tempest“ by Shakespeare



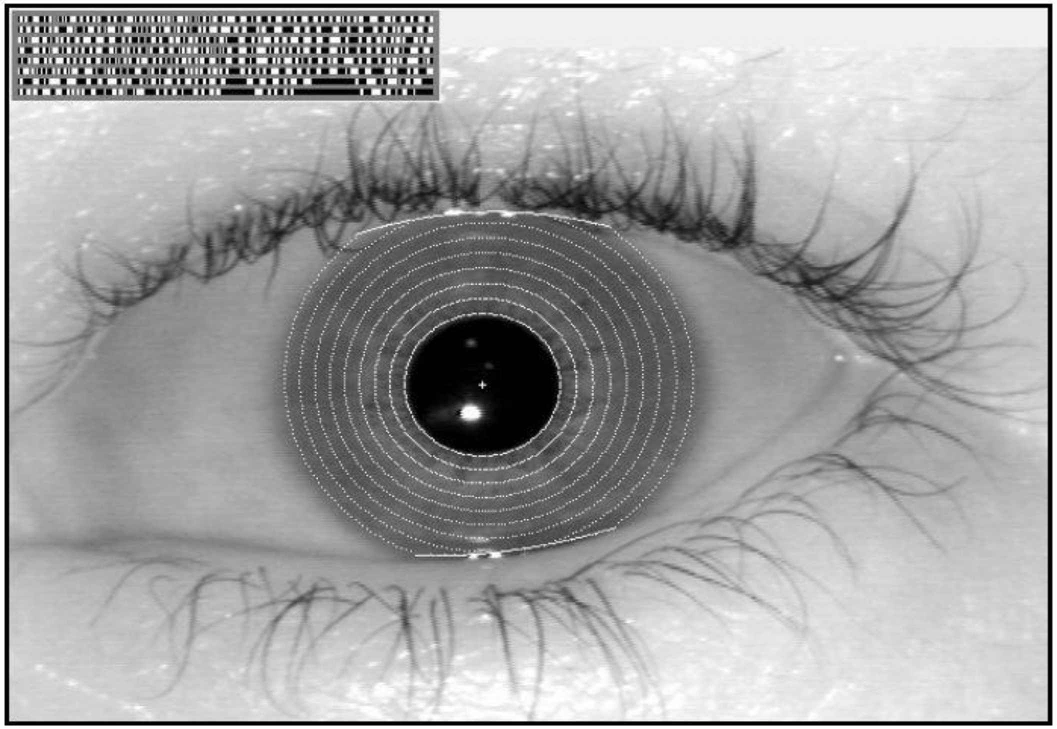
Examples - Geometry

- Hand and finger geometry



Examples - Iris

- Remains unchanged after 2 years
- Iris code.



Examples - Keystroke

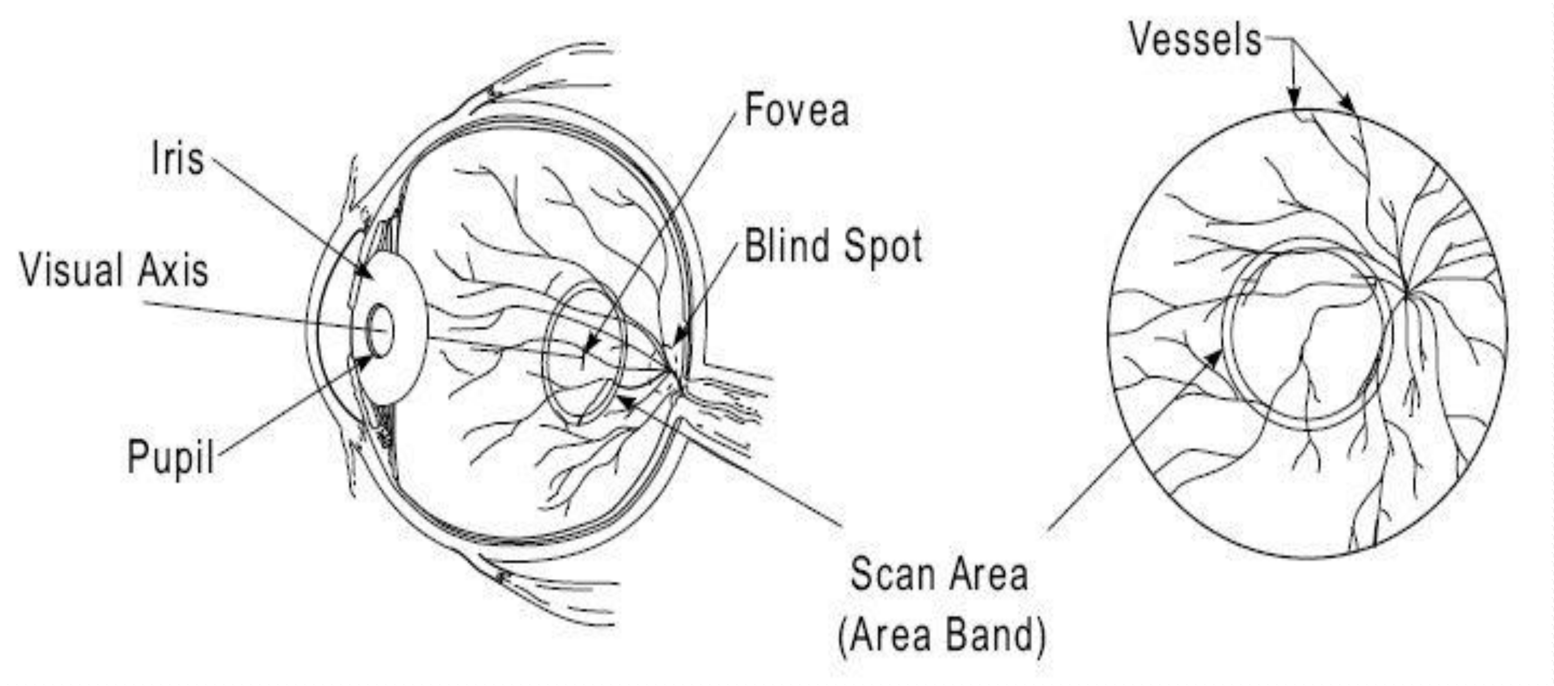
- Typical way of typing
- Combinations of keys
- Speed, force and press-down

Examples - Odor

- Used by humans
- Many problems

Examples – Retinal Scan

- Supposed to be the most secure biometric
- Not user friendly



Characteristics - overview

- Universality
- Distinctiveness
- Permanence
- Collectability
- Performance
- Acceptability
- Circumvention

Characteristic - Universality

- Each person should have the characteristic
  - Failure to Enroll Rate (FER)

Distinctiveness

- Different persons should have different biometric properties
  - False Match Rate (FMR)

Characteristic – Permanence

- The characteristic should be sufficiently invariant over a period of time
  - False Non-Match Rate (FNMR)

Characteristic – Collectability

- The biometric property should be easy to collect (electronically) and to quantify

Characteristic – Performance

- This refers to the achievable recognition accuracy and speed
  - False Non Match Rate (FNMR)
  - Failure to Capture Rate (FCR)

Characteristic – Acceptability

- To which extent are people willing to accept the use of a specific biometric

Characteristic – Circumvention

- Reflects how easy it is to fool the system
  - False Match Rate (FMR)

Application Environments

- Overt vs. covert
- Habituated vs. non-habituated
- Attended vs. non-attended
- Standard vs. non-standard
- Public vs. private
- Open vs. closed

Overt vs. covert

- Overt:
  - User is aware that the biometric feature is being measured (e.g. finger on a fingerprint reader)
- Covert:
  - User is unaware that the biometric feature is being measured (e.g. face recognition)

Habituated vs. non-habituated

- Habituated:
  - System is used on a daily basis (e.g. to have access to the PC at work)
- Non-habituated:
  - System is used irregularly (e.g. to access a personal safe in a bank)

Attended vs. non-attended

- Attended:
  - Use is observed and guided by system management (e.g. access to a building)
- Non-attended:
  - No observation or (regular) help is provided (e.g. access to PC)

Standard vs. non-standard

- Standard:
  - System is in a static environment with controlled conditions (e.g. fixed lightning and background for face recognition)
- Non-standard:
  - System in a dynamic environment (e.g. background noise for voice recognition)

Public vs. private

- Public:
  - “Anybody” can use the system (e.g. voice recognition for bank transfers via phone)
- Private:
  - Only employees can use the system (e.g. access to a factory or office building)

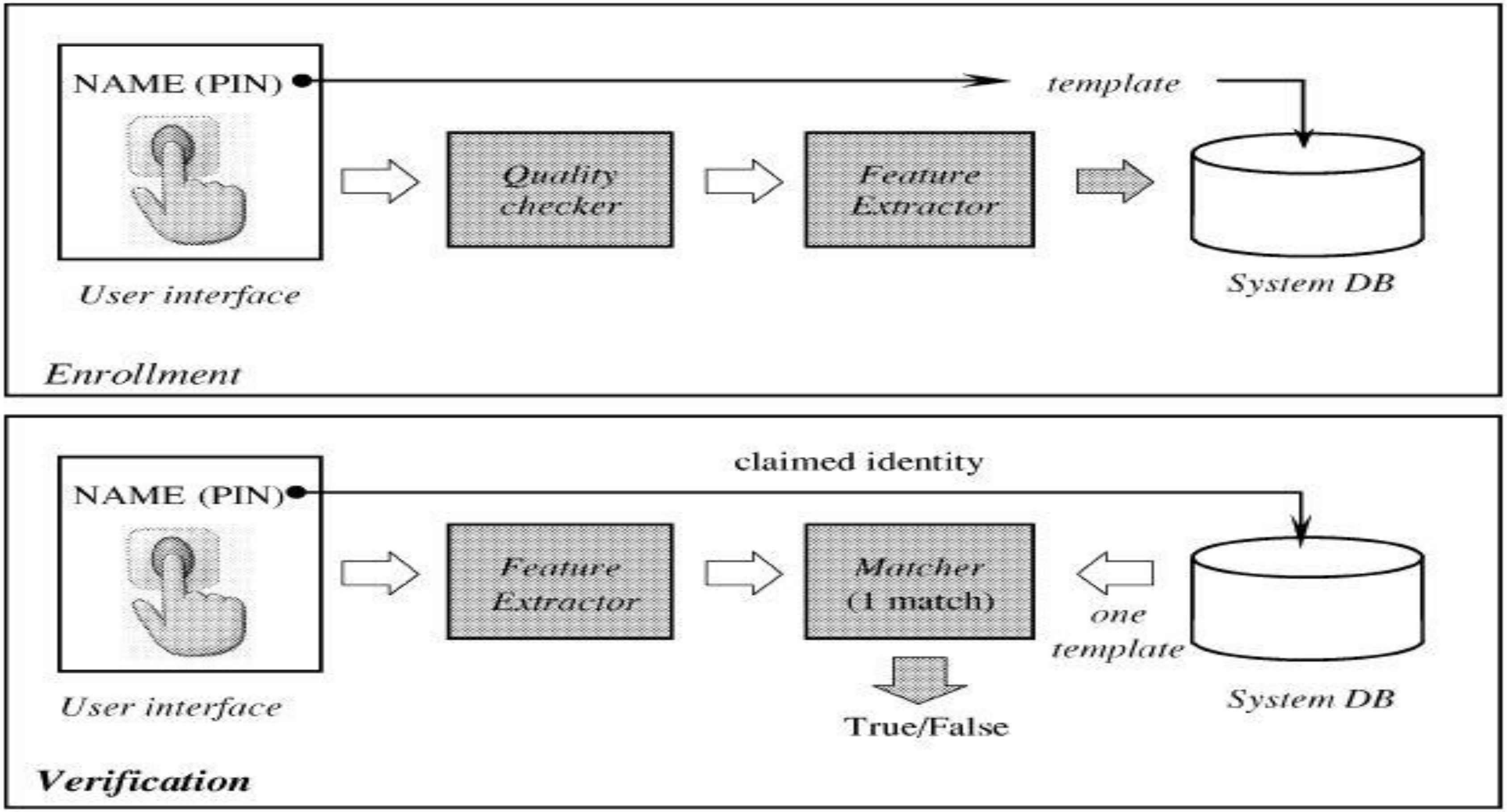
Open vs. closed

- Open:
  - System can interact with other (biometric) system (e.g. biometric passport)
- Closed:
  - System is stand-alone and no information is shared (e.g. systems to access classified information)

Biometrical Systems

- A biometrical systems consists of 2 modules:
  - Enrollment module
    - Template created and stored in database
  - Authentication module
    - Checked against stored template

Biometrical Systems



Errors

- False Non-Match Rate (FNMR)
- False Match Rate (FMR)
- False Rejection Rate (FRR) (used wrongly in literature). USE (FNMR) instead
- False Acceptance Rate (FAR) used wrongly in literature. USE (FMR) instead
- Failure to Enroll Rate (FER)
- Failure to Capture Rate (FCR)

Hypotheses and decisions

- H_0 : input biometric does **not** belong to the same person as the template biometric
- H_1 : input biometric does belong to the same person as the template biometric
- D_0 : Person is **not** who he claims to be
- D_1 : Person is who he claims to be

False Match Rate (FMR)

- Probability that a false claimed identity is not recognized as false
- Also called *Type I Error*
- Probability that D_1 is decided, given that H_0 is true:
  - Prob(D_1 | H_0)
- Depends on a threshold t

False Non-Match Rate (FNMR)

- Probability that a correctly claimed identity is not recognized as true
- Also called *Type II Error*
- Probability that D_0 is decided, given that H_1 is true:
  - Prob(D_0 | H_1)
- Depends on a threshold t

Failure to Enroll Rate (FER)

- Probability that a person cannot enroll in the biometric system
- Person doesn’t have biometric feature
- Person has poor quality biometric feature
- Trade-off between FMR/FNMR and FER

Failure to Capture Rate (FCR)

- Probability of failure to capture the biometric feature when trying to authenticate
- Bad capturing conditions
  - Too dark for face recognition
  - Dirty fingerprint reader
  - Background noise for voice recognition

Equal Error Rate (EER)

- EER is the point where FMR and FNMR are equal

Distance metrics - 1

- In biometrics we need to compare extracted features that will differ a bit every time they are measured
- Need a way to compare extracted features
- ”Inter person” distance must be large
- ”Intra person” distance must be small

Distance metrics - 2

- We want to know how far 2 sequences **x** and **y** are apart or how close together they are.
- Let **x** = $(x_1,x_2,\ldots,x_n)$
- Let **y** = $(y_1,y_2,\ldots,y_n)$
- Assume **x** can be compared to **y**

Absolute Distance

- Sum the absolute differences between each of the components of **x** and **y**
- $d_1(\mathbf{x},\mathbf{y}) = \Sigma \mid x_i - y_i \mid$
- Extremely easy to calculate

Euclidean Distance

- Sum the squares of the differences between each of the components of **x** and **y**

- $d_2(\mathbf{x},\mathbf{y}) = \sqrt{\ } [\Sigma (x_i - y_i)^2]$

- Also easy to calculate

Maximum Difference Distance

- The distance between **x** and **y** is defined as the maximum absolute difference of its components

- $d_3(\mathbf{x},\mathbf{y}) = \max | x_i - y_i |$

- Extremely easy to calculate

More distance metrics?

- Many more distance metrics possible
- Sometimes first a mathematical transformation of the data is needed
- Not all parts of the data need to be taken into account

Threshold

- Features are extracted from biometric characteristic
- Features are compared to template
- Distance metric gives distance d
- Use of threshold t
- $d \leq t$: authentication OK
- $d > t$: authentication NOT OK

Example - Distance scores

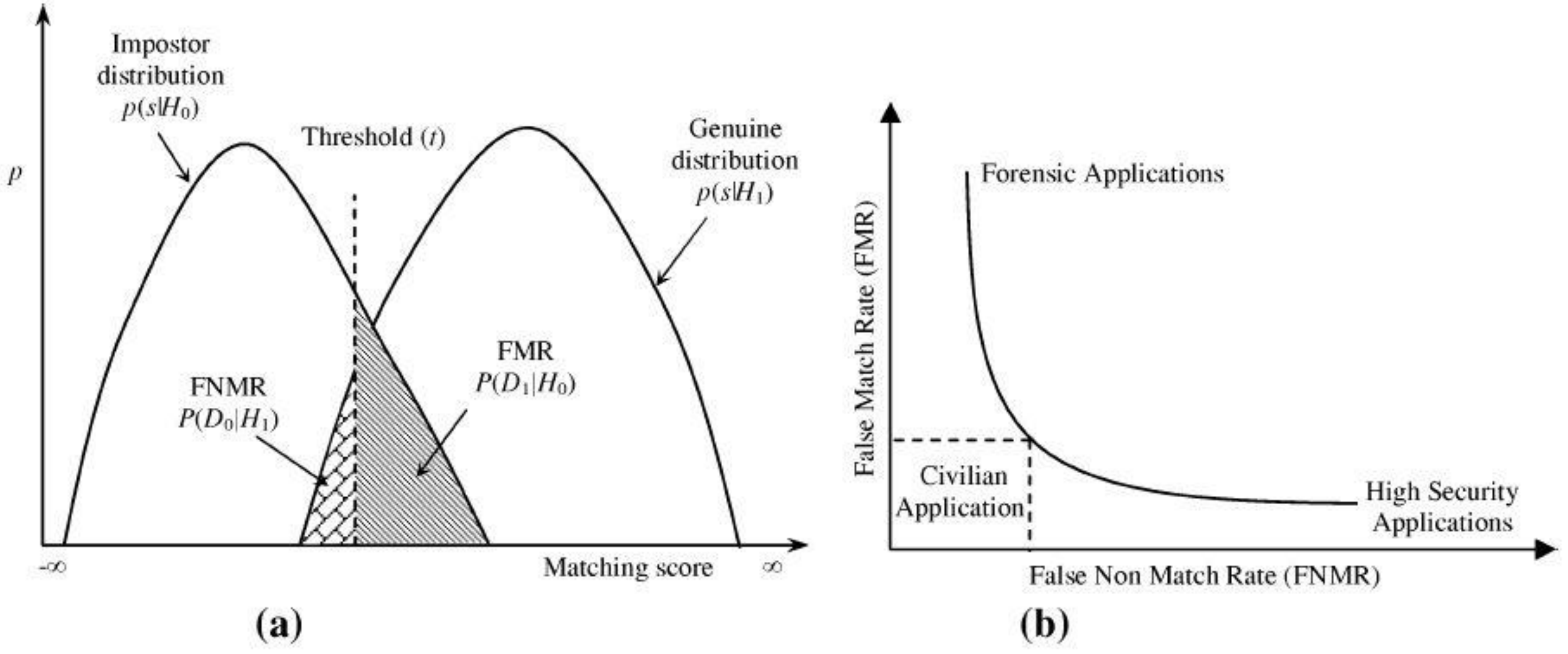
	Templ 1	Templ 2	Templ 3	Templ 4	Templ 5
Test 1	**0,182**	0,588	0,435	0,208	0,909
Test 2	0,323	**0,213**	0,286	0,476	0,244
Test 3	0,909	0,625	**0,147**	0,476	1,111
Test 4	0,238	0,294	0,476	**0,256**	0,526
Test 5	0,588	0,454	1,250	0,526	**0,130**

Example – FNMR/FMR

- If t=0.256 we see that
  - (FNMR,FMR) = (0/5 , 3/20)
- If t=0.213 we see that
  - (FNMR,FMR) = (1/5 , 1/20)
- If t=0.212 we see that
  - (FNMR,FMR) = (2/5 , 1/20)
- If t=0.207 we see that
  - (FNMR,FMR) = (2/5 , 0/20)

ROC Curve

- ROC: Receiver Operating Characteristic



Impostor distribution $p(s|H_0)$
p
Threshold (t)
Genuine distribution $p(s|H_1)$
FNMR $P(D_0|H_1)$
FMR $P(D_1|H_0)$
$-\infty$
Matching score
∞
(a)
Forensic Applications
False Match Rate (FMR)
Civilian Application
High Security Applications
False Non Match Rate (FNMR)
(b)