Biometric Systems
Lesson 1 - Introduction

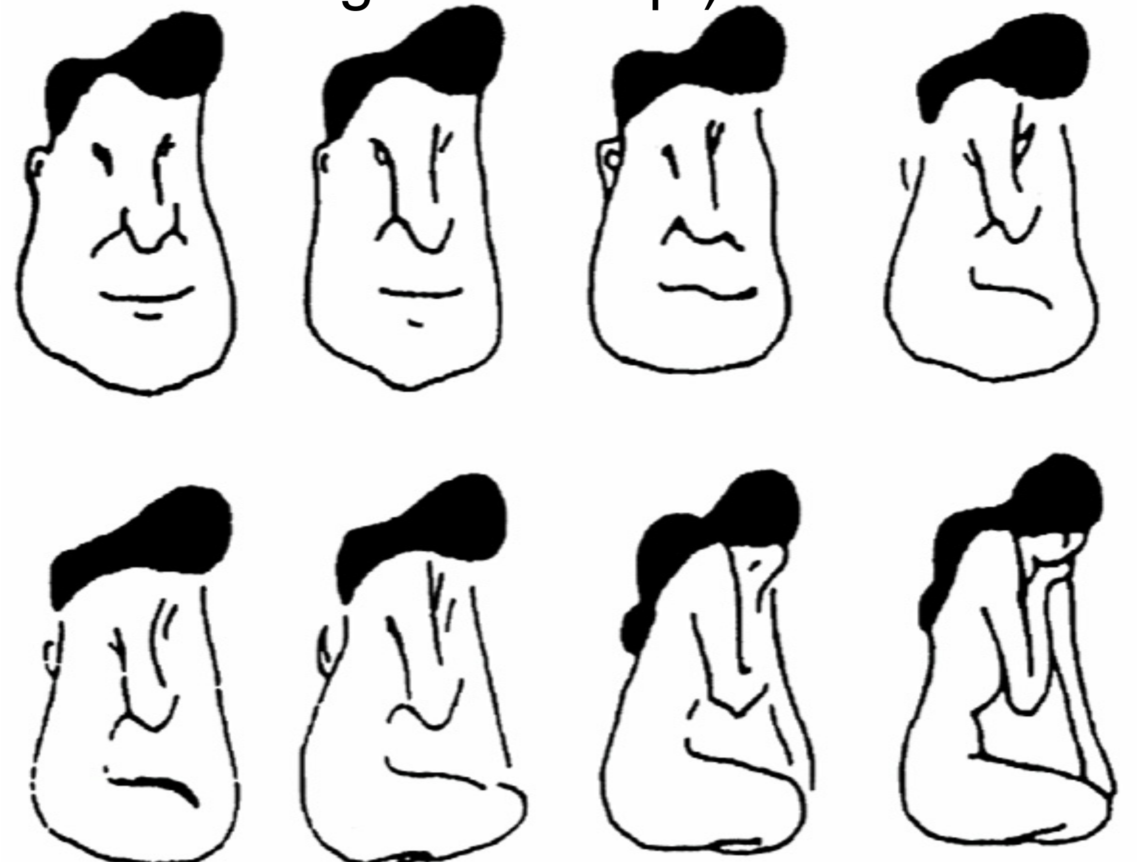
Maria De Marsico
demarsico@di.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Dipartimento di
Informatica

Biometric System – System for a kind of Pattern Recognition

Two patterns are similar if the measure of the **distance** between their **feature** vectors is **small** (three basic issues: what is a good distance measure, which are the best features, what is the difference margin to accept)



Pattern recognition in different kinds of ways

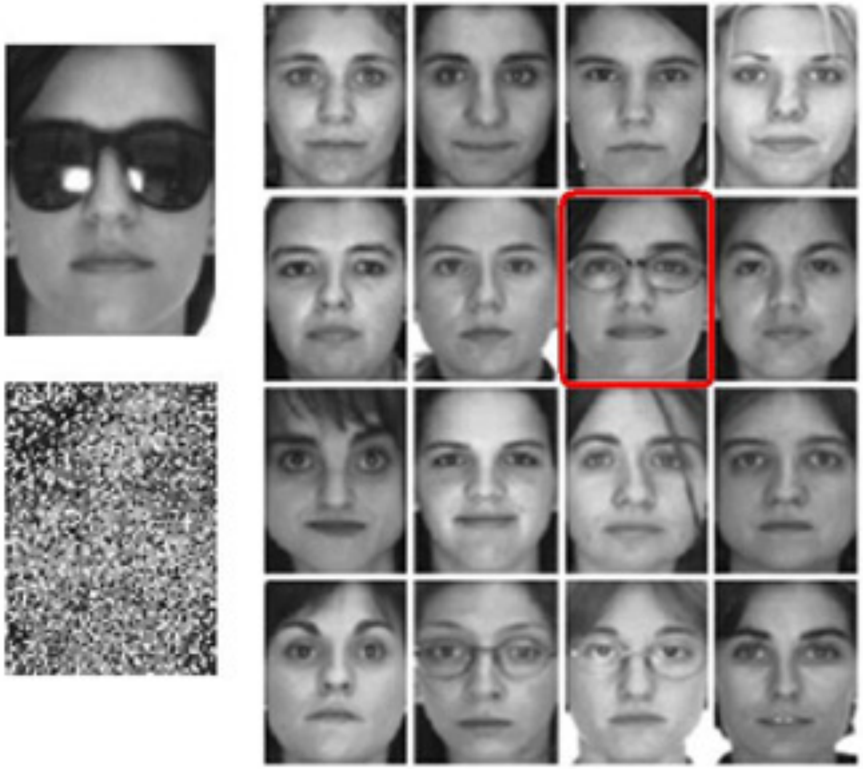
- Content based image retrieval
  - Classes= types of objects
  - Pattern = allows to distinguish a face from a flower

Pattern recognition in different kinds of ways

- Recognition
  - – Classes = subclasses of a same type (.e., dogs)
  - – Pattern = allows to distinguish a subclass

Pattern recognition in different kinds of ways

- Biometrics
  - Classes = individuals
  - Pattern = allows to disttinguish among individuals



What is biometrics?

- From Greek *bios* (= life) and *métron* (= measure)
- In general = Measure and statistical analysis of biological data
- In technological sense = measure and analysis of physical and/or behavioral characteristics to authenticate /recognize a person
- Definition by Biometric Consortium = “automatic recognition of a person according to discriminative characteristics”

What is biometrics?

- Basic assumption: each person is unique
- Main issues:
  - Determine the unique features able to identify a person
  - Find reliable techniques to measure such features
  - Devise reliable algorithms to recognize/classify a person according to the measured features

Access Types

- Physical Access
  - Room
  - Building
  - Area

- Logical Access
  - Electronic resources
  - Critical data

Why biometric systems

At present, recognition (often for authentication purposes) is performed according to two modalities:

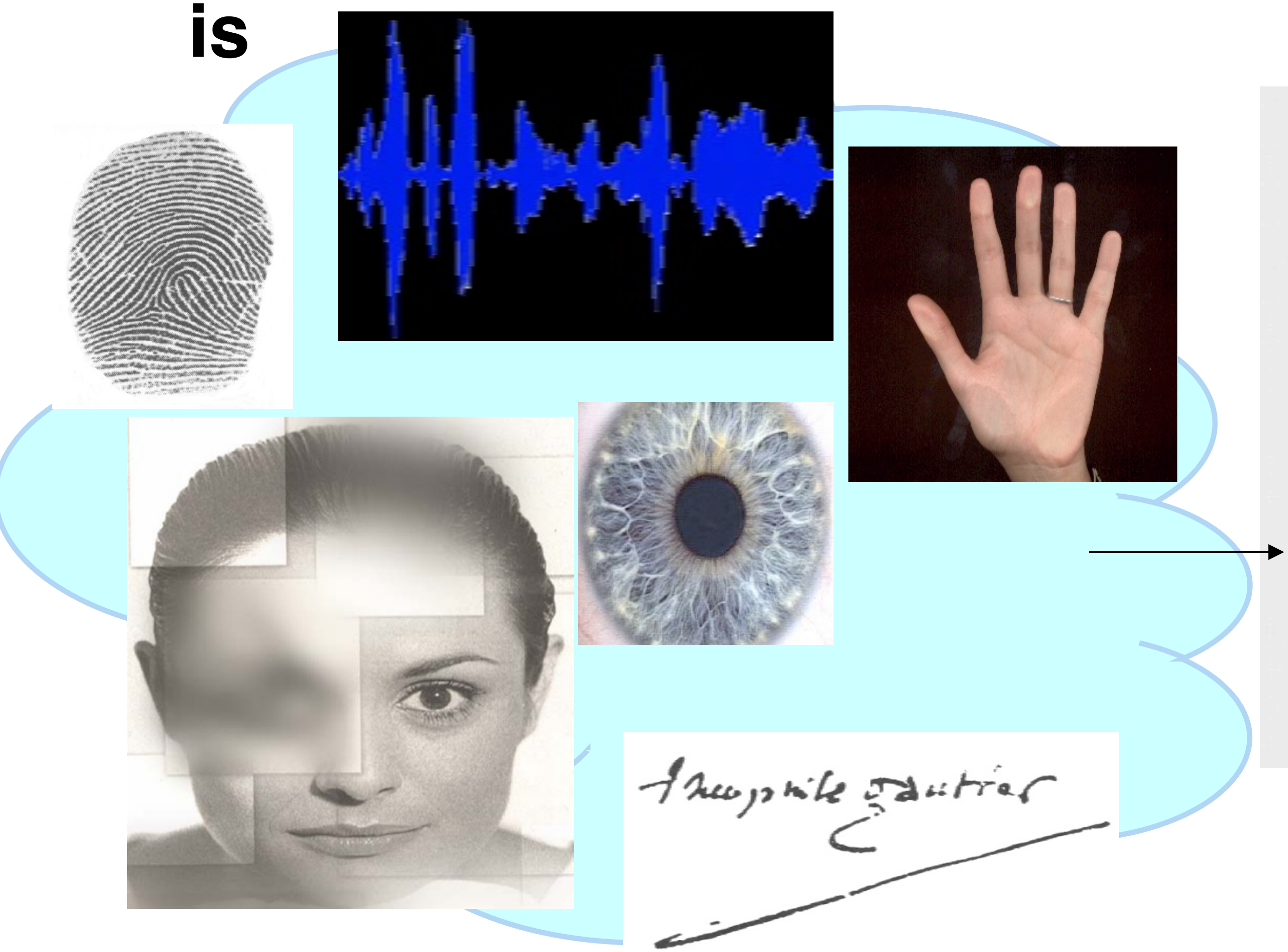
- Something one **owns**: a card or a document … but … it can be lost, or stolen, or copied … Actually the system authenticates the object, not its owner ☾

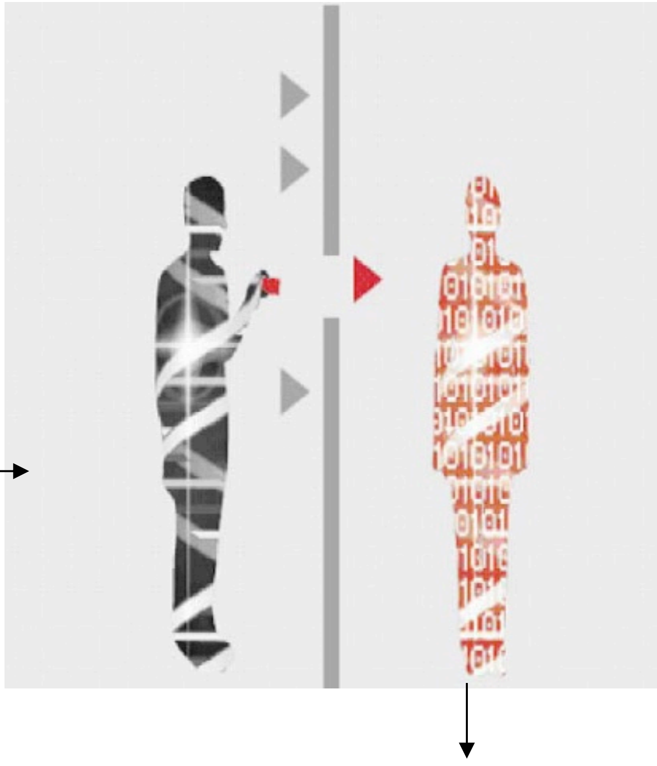
- Something one **knows**: an individual or community password … but … it can be guessed, wo forgotten (but easy to remember = easy to guess!)

"Your logon password is XB#2D940. Write it down and don't lose it again."

Why biometric systems

- Based upon what **one is**





Some history: Bertillon

- In1882 Alphonse Bertillon (1853-1914), chief of the identification service of Paris police, introduced a new system of bodily measure expressely devised to identify criminals.
- In theory , those measures should have identified univocally an individual and should have been persisent along time (in adult life at least).
- The procedure was called *Bertillonage*.

Some history: Bertillon

Hand shape

Head shape

Bust measure

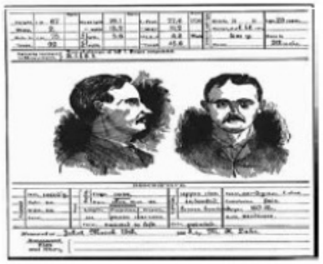
Limbs measures

Caliper compass

Sliding compass

...

Face details



Identification card recording the relevant measures

Slide produced by da J.L. Dugelay (Eurecom-France)

Some history: Bertillon

By dividing each of the measurements into small, medium and large groupings,

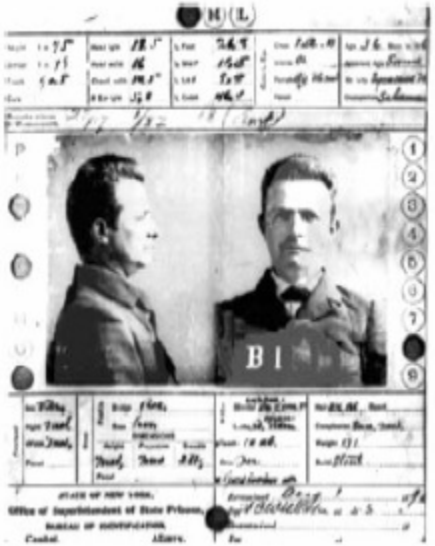
Bertillon could place the dimensions of any single person into one the 243 distinct categories.

Further subdivisions by eye (7) and hair color provide 1,701 separate groupings.

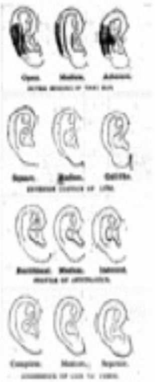
For example, in a file a 5,000 records, each of the primary categories would hold about 20 cards.

Therefore, it was not difficult to compare the new record to each of the other cards in the same category.

Scale of Pigmentation.
Divisions Nos 1 2 3 4 5 6 7 of the Classification
Frank
Frank
Frank
Frank
Frank
Frank


H
L
B I
STATE OF NEW YORK.

The first criminal identification card filed by the New York State Bertillon Bureau



Slide produced by da J.L. Dugelay (Eurecom-France)

Some history: Bertillon

Origins of the New York State Bureau of Identification

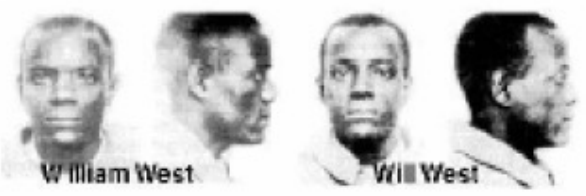
- **Bertillonage was officially adopted in France in 1882 and soon after in some other countries.**
- **Anthropometry was first introduced in the United States by Major McClaughry, the translator of Bertillon's book (*Spoken portrait*), in 1887 when he was the warden of the Illinois State Penitentiary at Joliet.**
  - ✓ **1896: Establishment of the National Bureau of Identification; forerunner of the FBI (Federal Bureau of Investigation), Chicago, 1897.**
  - ✓ **After 1 year: 16,000 Bertillon cards; and 24,000 after 2 years;**

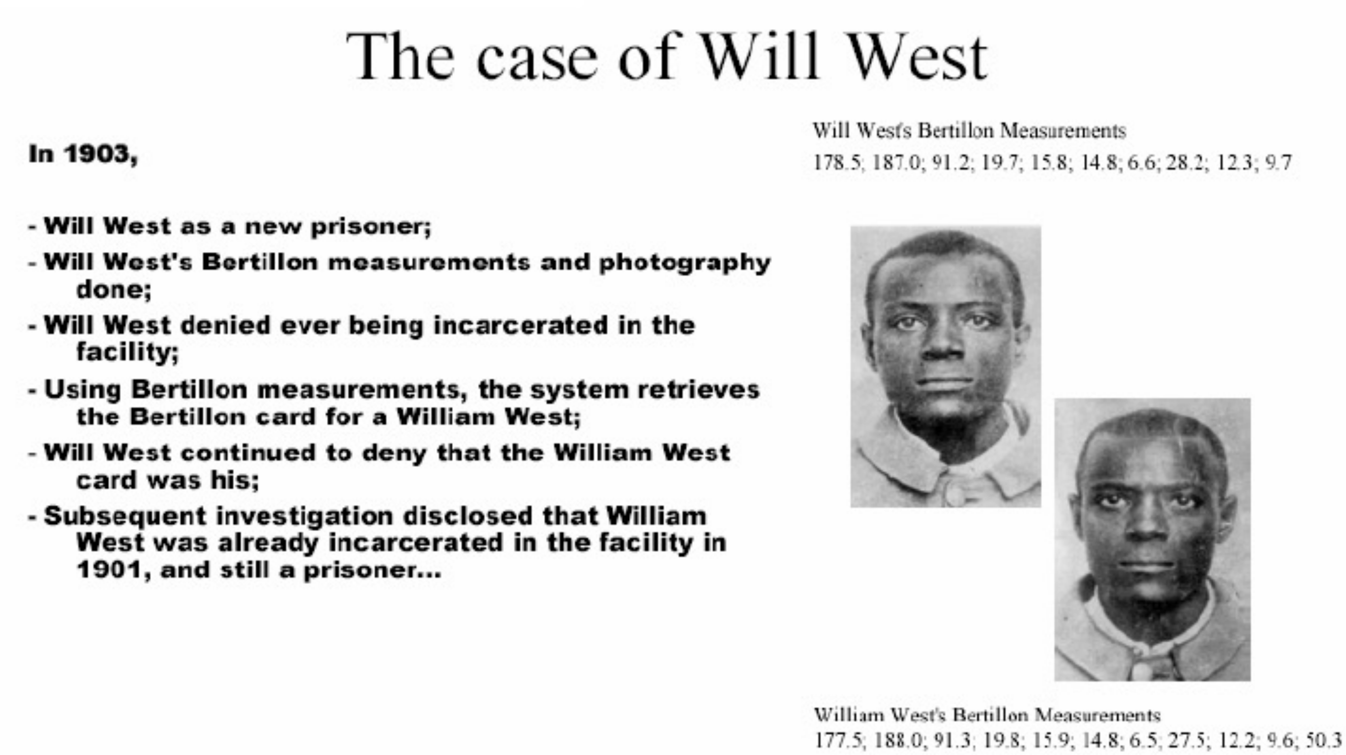
  … and 131 criminals received at State Prisons as « first offenders » were found to have prior records.
  - ✓ **1900: A law allows the Prison Department to accept Bertillon cards.**

The NY State Bertillon Bureau in 1902

Slide produced by da J.L. Dugelay (Eurecom-France)

Some history: Bertillon





The case of Will West

In 1903,

- **Will West as a new prisoner;**
- **Will West's Bertillon measurements and photography done;**
- **Will West denied ever being incarcerated in the facility;**
- **Using Bertillon measurements, the system retrieves the Bertillon card for a William West;**
- **Will West continued to deny that the William West card was his;**
- **Subsequent investigation disclosed that William West was already incarcerated in the facility in 1901, and still a prisoner...**

Will West's Bertillon Measurements
178.5; 187.0; 91.2; 19.7; 15.8; 14.8; 6.6; 28.2; 12.3; 9.7

William West's Bertillon Measurements
177.5; 188.0; 91.3; 19.8; 15.9; 14.8; 6.5; 27.5; 12.2; 9.6; 50.3

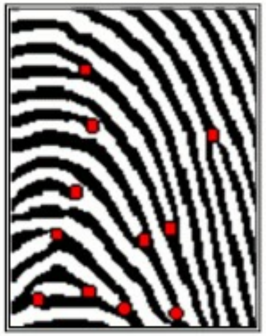
Slide produced by da J.L. Dugelay (Eurecom-France)

Some history: Galton

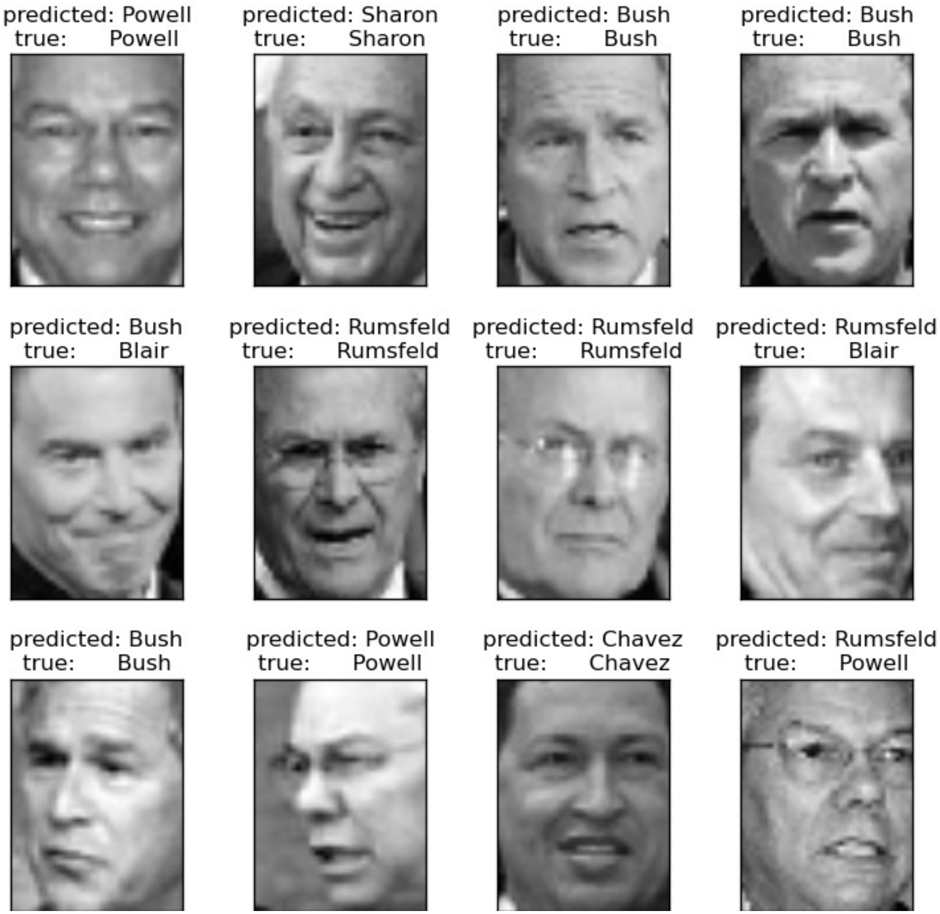
- At the end of XIX century Galton criticized the system of Bertillon from a statistical point of view.
- In 1892 he introduced the notion of *minutia* and devised a first very simple system to classify fingerprints.
- In 1893, the Home Ministry Office, UK, recognized

that no pair of individuals has the same fingerprints.

- Many police department started acquiring and storing fingerprints of criminals and scientific methods were developed to visually compare them.
- The classification system by Galton-Henry (1900) is the base for the fingerprint recognition systems in many police departments in many countries



It does not always work …



predicted: Powell
true: Powell

predicted: Sharon
true: Sharon

predicted: Bush
true: Bush

predicted: Bush
true: Bush

predicted: Bush
true: Blair

predicted: Rumsfeld
true: Rumsfeld

predicted: Rumsfeld
true: Rumsfeld

predicted: Rumsfeld
true: Blair

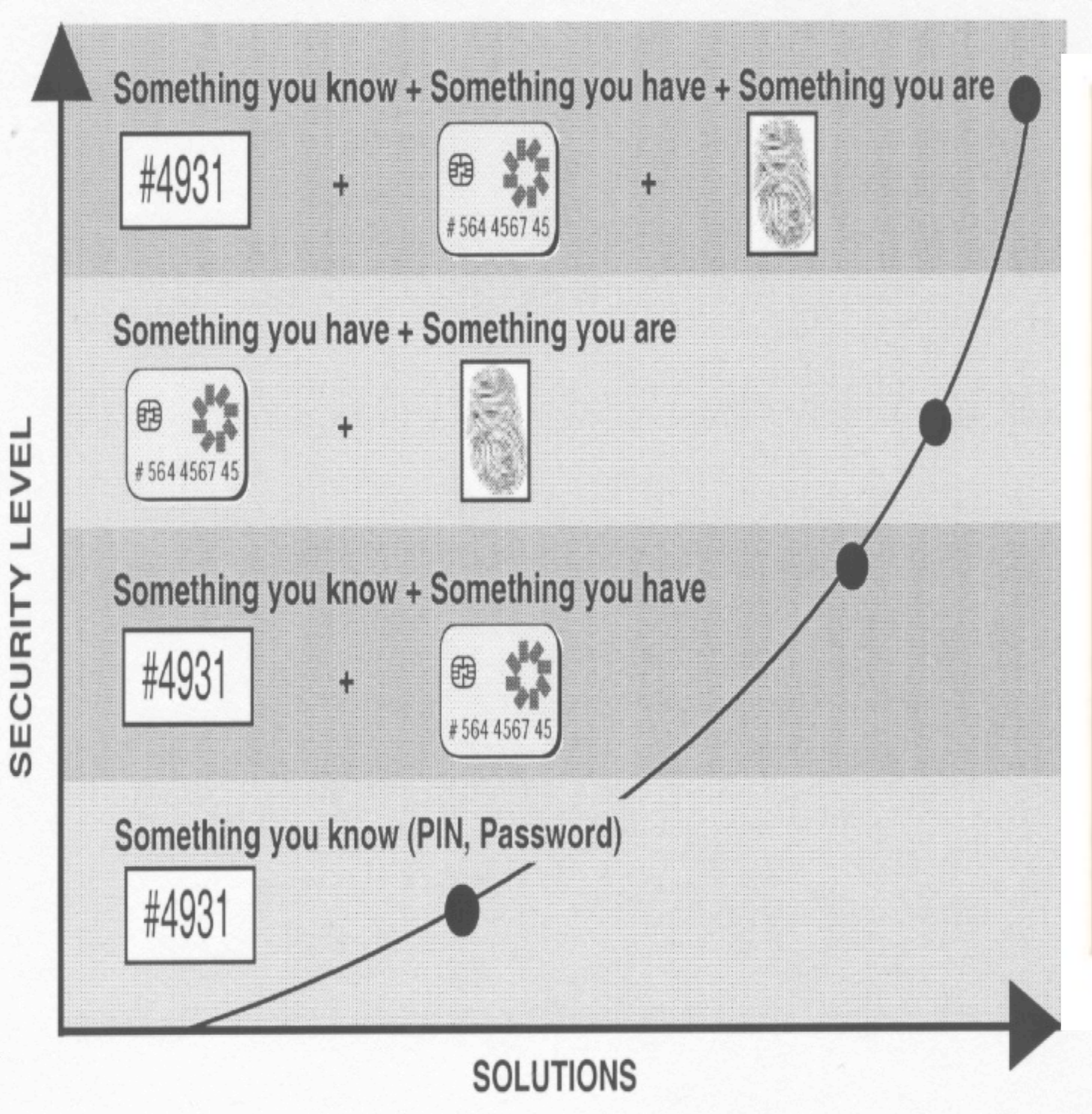
predicted: Bush
true: Bush

predicted: Powell
true: Powell

predicted: Chavez
true: Chavez

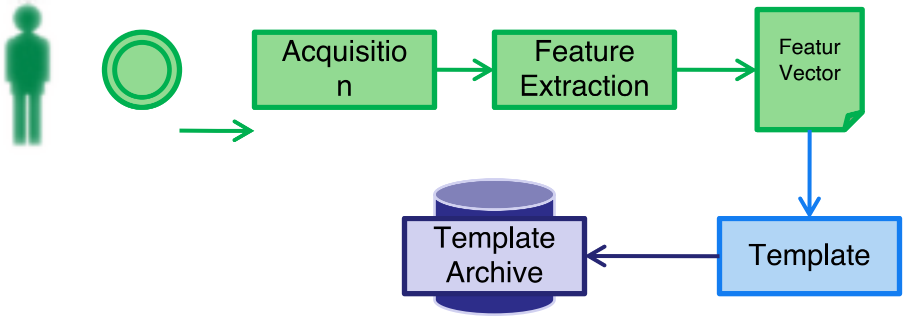
predicted: Rumsfeld
true: Powell

… but integration with traditional systems …

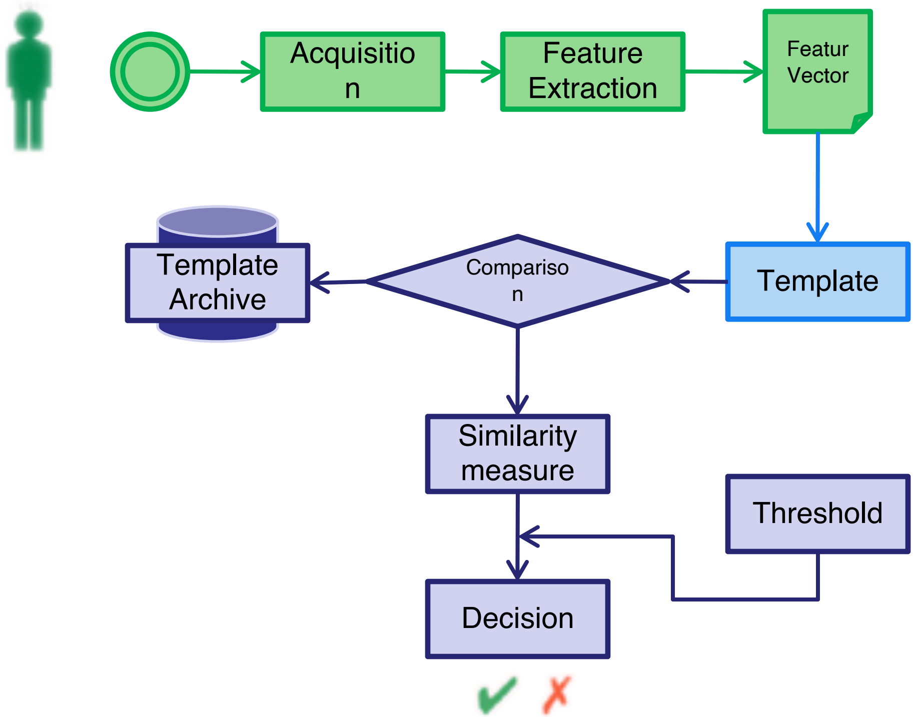


Architecture of a Biometric System

Enrollment:
*C*apture and processing of user biometric data for use by system in subsequent authentication operations (gallery).



Recognition:
Capture and processing of user biometric data in order to render an authentication decision based on the outcome of a matching process of the stored to current template (verification 1:1 identification 1:N)



Probe: each template which is submitted for recognition.

Gallery: the set of templates pertaining to enrolled subjects

Modules of a biometric system

A biometric system is generally designed to operate with four modules.

- Sensor Module : where biometric data are caught.
- Feature extraction module : where a set of main characteristics is extracted from acquired data. During enrollment it produces the templates to be stored in the system.
- Matching module: where extracted features are matched with stored templates to return one or more matsching scores.
- Decision module: where a decision is made according to matching results.

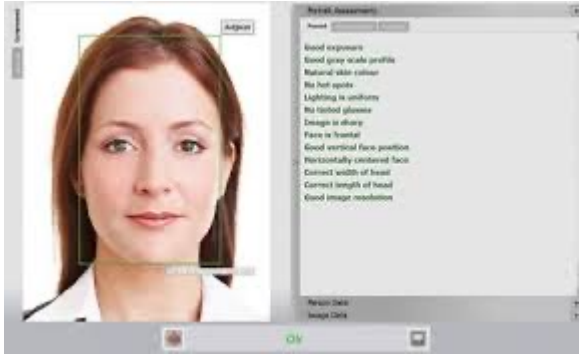
Types of users

- ***Cooperative***: the user is interested in recognition (an impostor might try to be recognized as a legal user).
- ***Non-cooperative***: the user is indifferent or even adverse to recognition (an impostor might try to avoid being recognized)
- ***Public/Private***: users of the system are customers or employees of the entity installing the system

- ***Used/Non used***: frequency of use of the biometric system (more times a day, daily, weekly, monthly, occasionally …).
- ***Aware/Not aware***: the user is aware or not of the recognition process

Types of settings

- ***Controlled***: capture settings can be controlled, distortions mostly avoided (e.g., for face, pose, illumination, and expression), defective templates can be rejected, and capture repeated

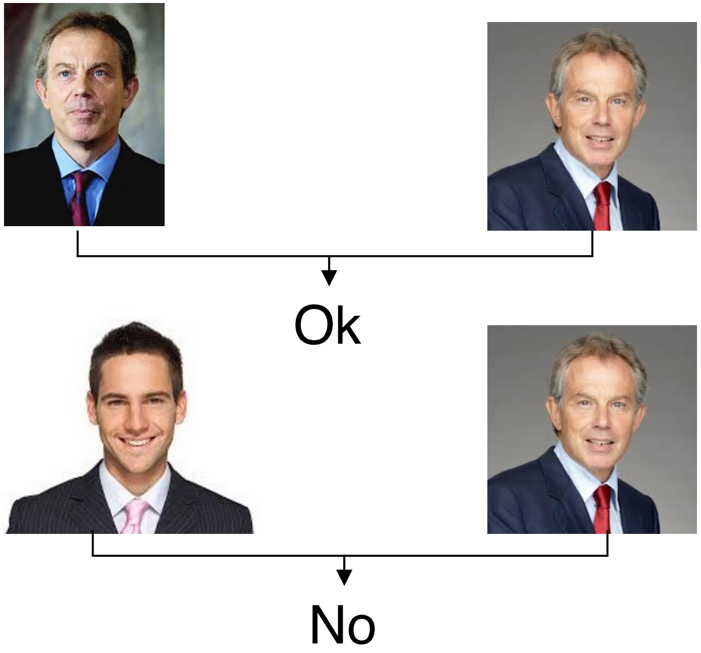


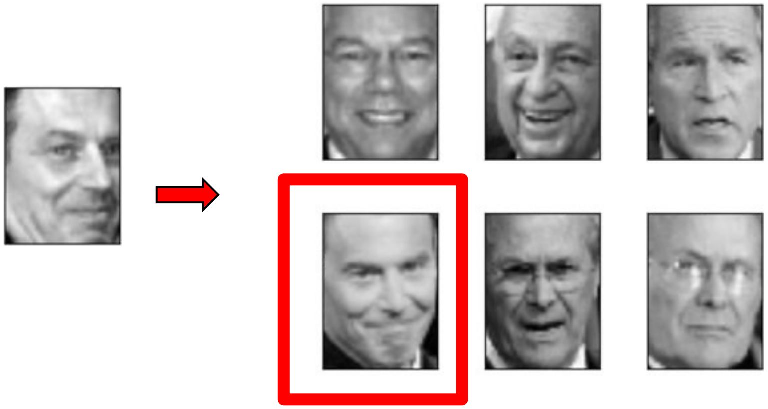
Good exposure
Good gray scale profile
Natural skin colour
No hot spots
Lighting is uniform
No tinted glasses
Image is sharp
Face is frontal
Good vertical face position
Horizontally centered face
Correct width of head
Correct length of head
Good image resolution

- ***Uncontrolled/undercontrolled***: capture settings cannot be controlled, template can present various levels of distortion, defective templates can be rejected, but capture cannot be repeated

Types of recognition operation

- ***Verification***: the user claims an identity, possibly by presenting an ID card or other additional stuff → the system performs a 1:1 matching to verify the claimed identity → possible result = accept/deny

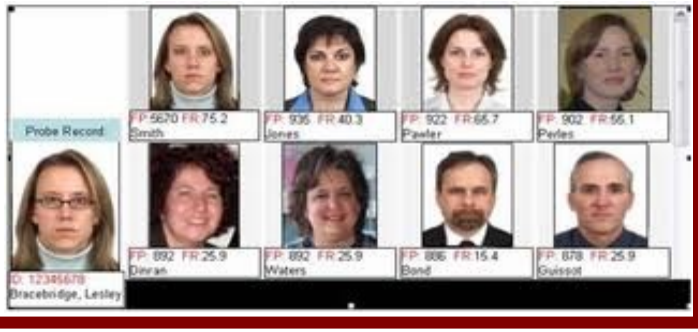




- ***Identification***: no claim by the user → the system has to determine the correspondence with one of the subjects in the system gallery by a 1:N matching operation → possible result = recognized identity

Types of identification

- ***Open set***: the system determines if probe p_i belongs to a subject in the gallery *G*.
- Some probe **might not** belong to any subject in *G* → the system has a ***reject*** option.
- **Possible errors**: reject a probe belonging to an enrolled subject **or** accept a probe non belonginhìg to an enìrolled subject **or** to return the wrong identity



FP 5670 FR 75.2
Smith

FP 936 FR 40.3
Jones

FP 922 FR 65.7
Pawler

FP 902 FR 56.1
Perles

Probe Record

ID: 12345678
Bracebridge, Lesley

FP 892 FR 25.9
Dinran

FP 892 FR 25.9
Waters

FP 886 FR 15.4
Bond

FP 878 FR 25.9
Guissot

- ***Closed set***: all probes belong to enrolled subjects.
- **Possible error**: return the wrong identity.

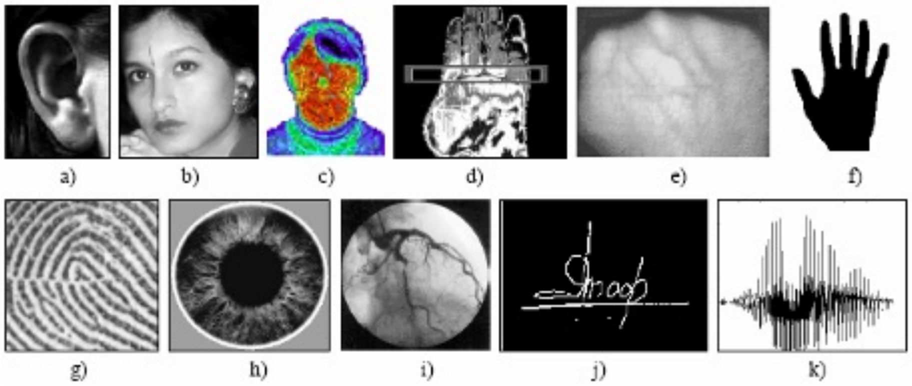
- ***Watch list***: the system has a list of subjects and checks if the probe belongs to the list.
  - **White list**: subjects in the list are granted access
  - **Black list**: subjects in the list are rejected (possible alarm)

Requirements for a biometric trait

- **Universality**
  – The trait must be owned by any person (except for rare exceptions …)
- **Uniqueness**
  – Any pair of people should be different according to the biometric trait
- **Permanence**
  – The biometric trait should not change in time
- **Collectability**
  – The biometric trait should be measurable by some sensor
- **Acceptability**
  – Involved people should not have any objection to allowing collection/measurement of the trait

Acknowledged techniques in X9.84 - 2003 Standard (minimum security requirements for an effective use of biometrics)

- **Fingerprints biometry** – fingerprint recognition
- **Eye biometry** – **iris** and **retina** recognition
- **Face biometry** – face recognition (**photo**, **infrared**)
- **Ear biometry** – ear recognition
- **Hand biometry** – finger **geometry**



Physiological Features

- **Signature biometry** – signature recognition (still and dynamic)
- **Keys typing**

Behavioural Features

- **Voice biometry** – vocal recognition

Mixed features miste

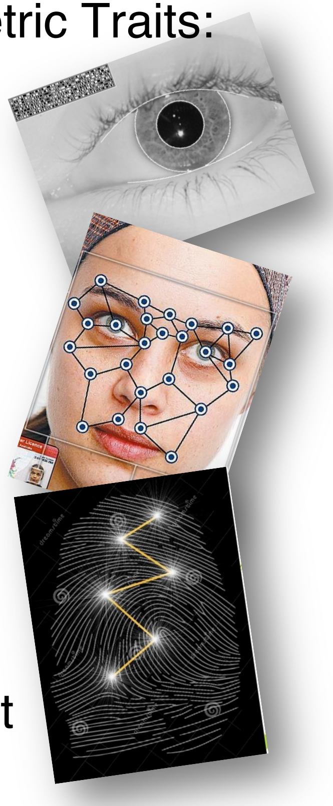
- **DNA**

Biological Traces

Biometrics

Strong Biometric Traits:

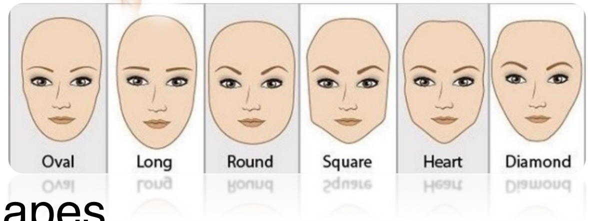
- Iris
- Face
- Fingerprint



Soft Biometric Traits:

- Hair Color

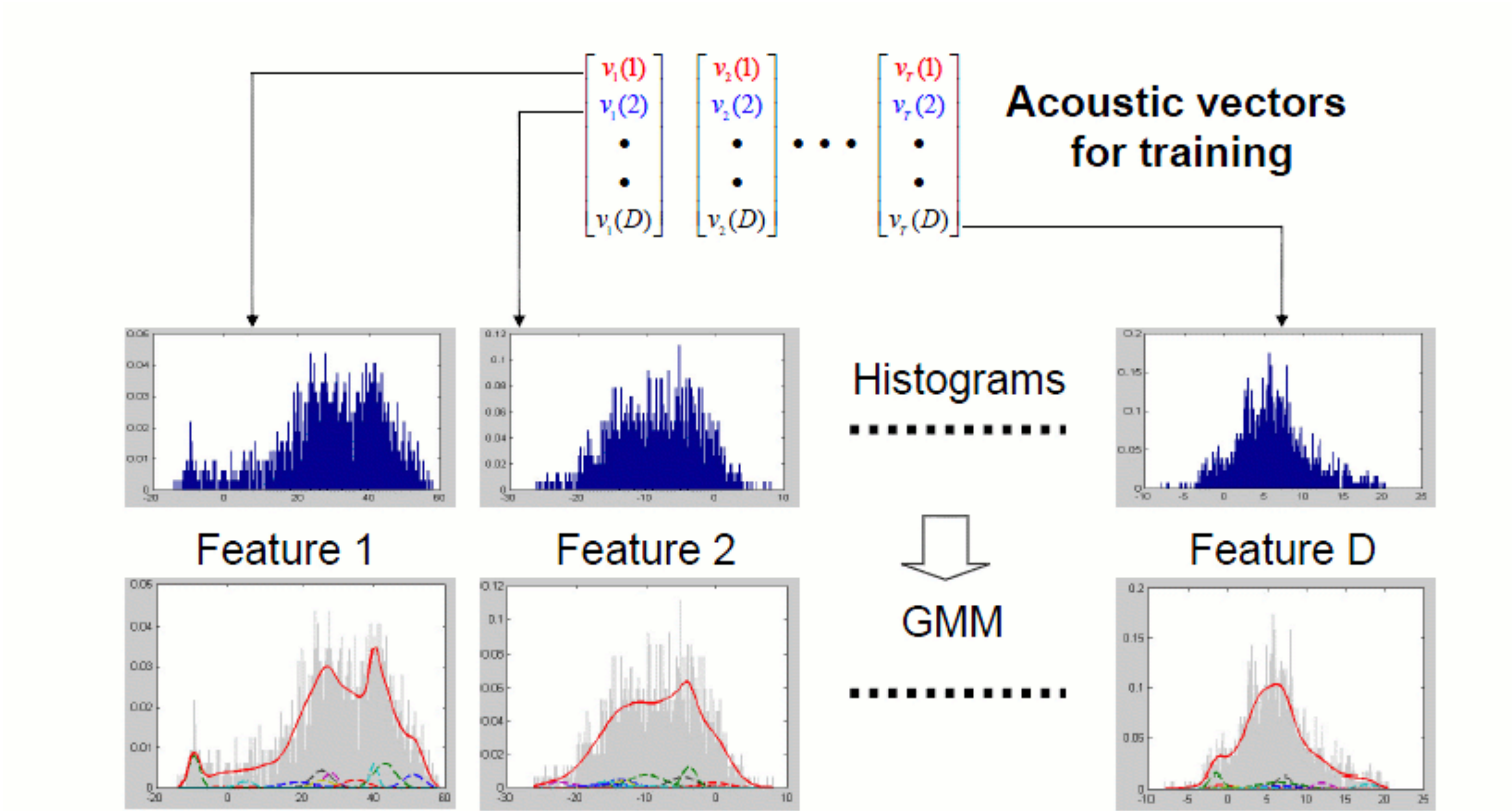
- Facial Shapes



- Gait

Either lack uniqueness (e.g., hair color) or persistance (e.g., behavioural that are affected by mood, health, etc.) but can be used to limit the search

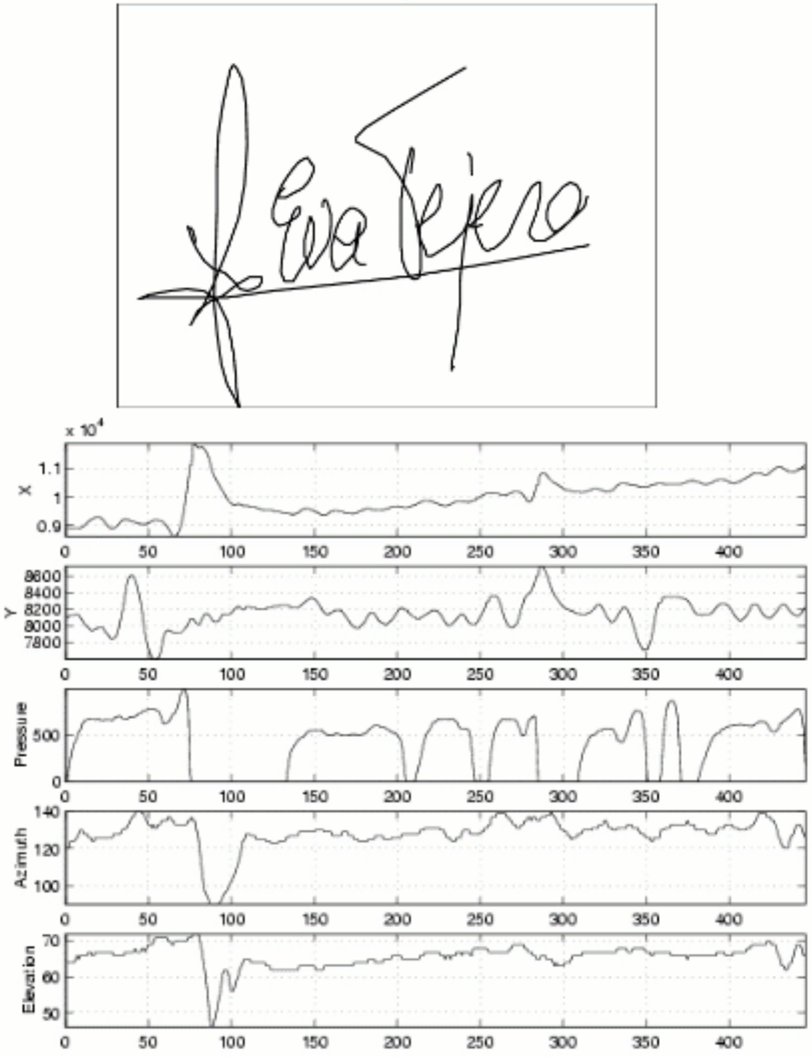
Voice: Gaussian Mixture Model (GMM)

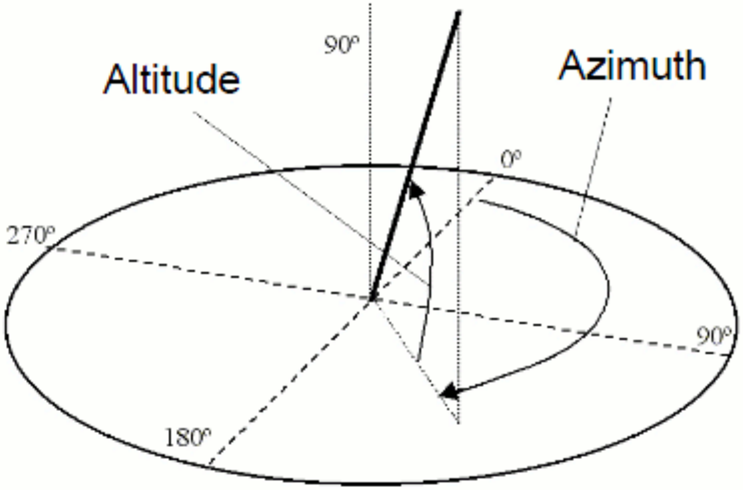


score = log-likelihood (speech | model)

From: Dr. Andrzej Drygajlo, Biometrics for Identity verification, 2007

Signature



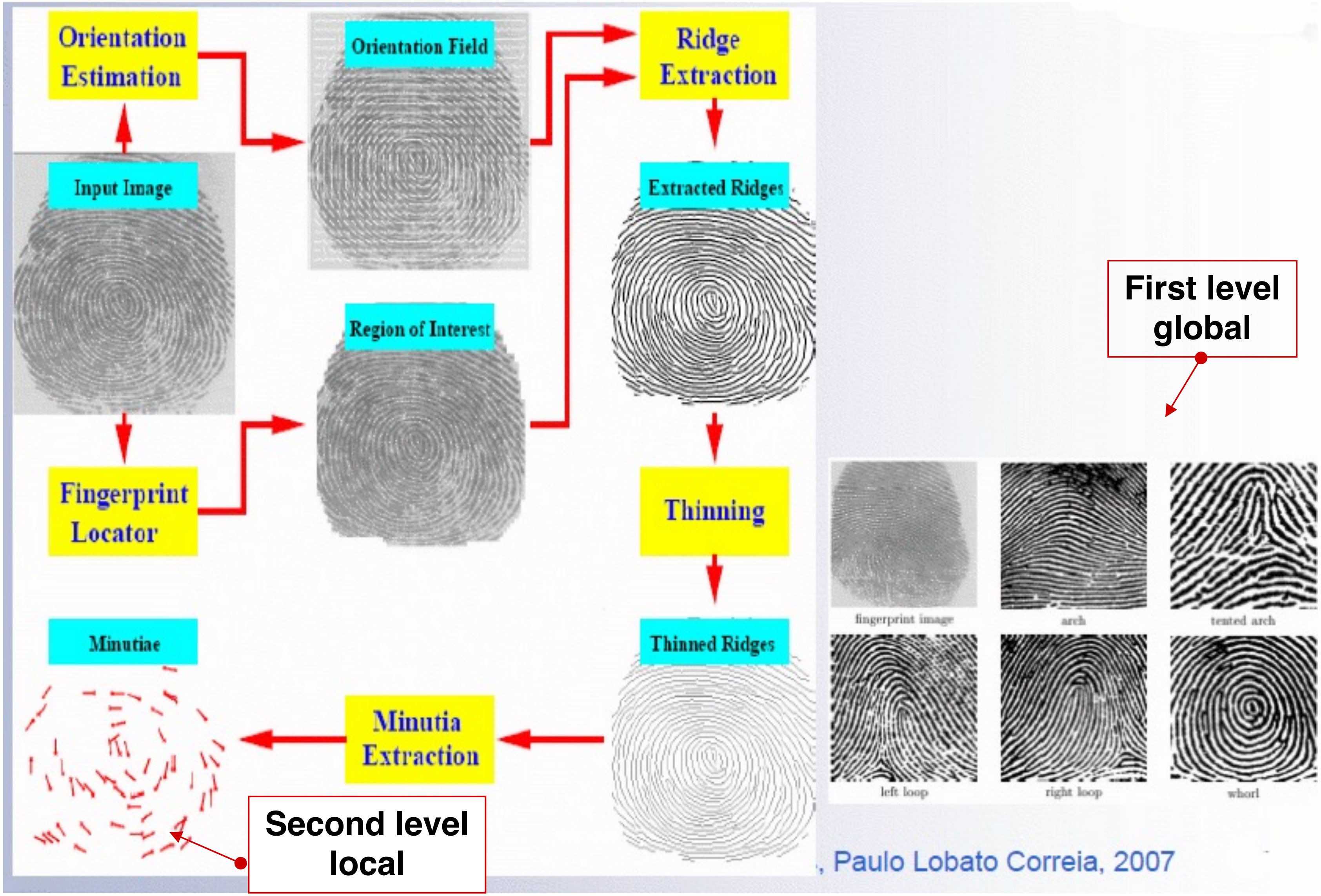


Features:

1. coordinate X
2. coordinate Y
3. pressure
4. pen azimuth (0° - 359°)
5. pen altitude (0° - 90°)

From: Dr. Andrzej Drygajlo, Biometrics for Identity verification, 2007

Fingerprint

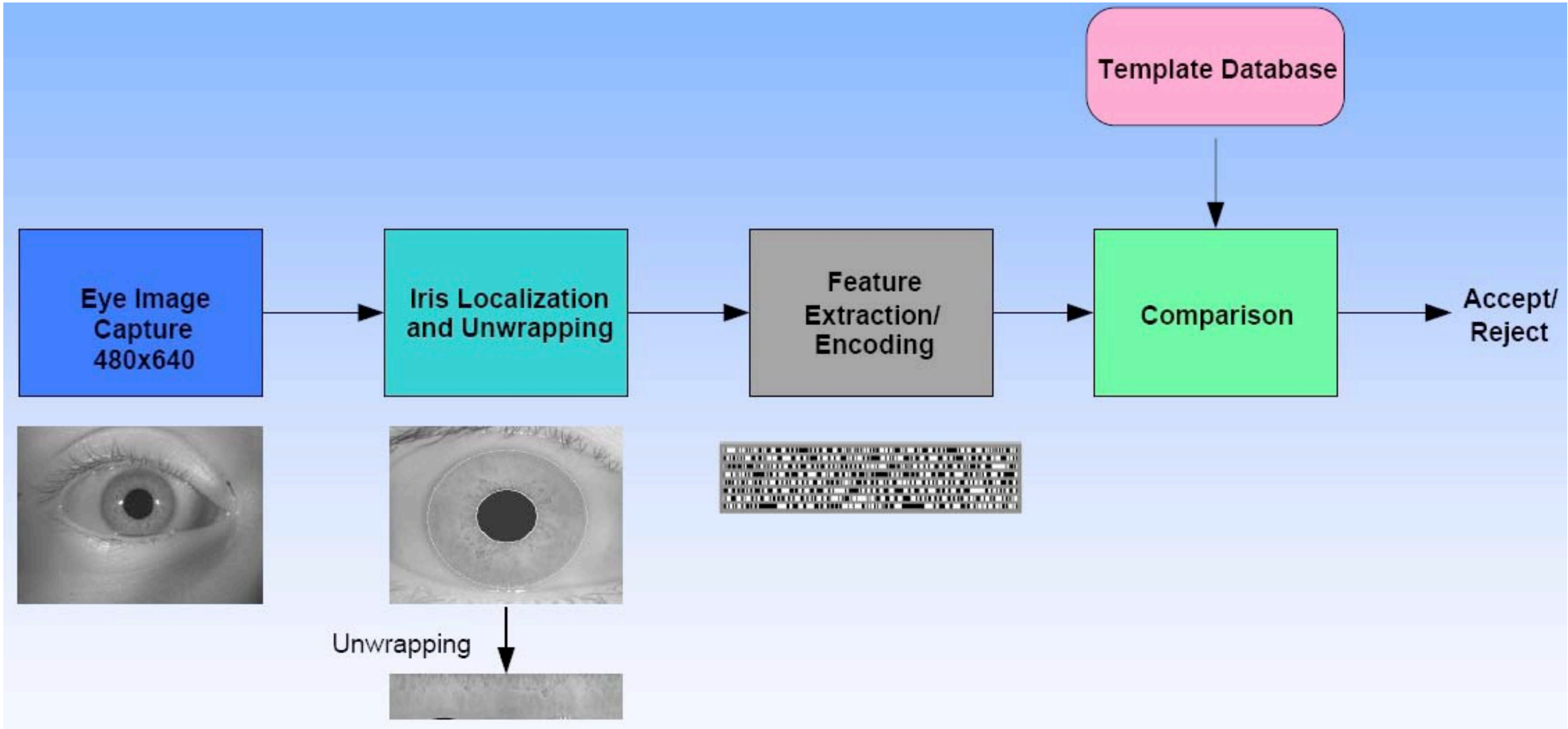


First level global

Second level local

, Paulo Lobato Correia, 2007

Iris


Template Database
Eye Image Capture 480x640
Iris Localization and Unwrapping
Feature Extraction/ Encoding
Comparison
Accept/ Reject
Unwrapping

J. Daugman,"Biometric Personal Identification System Based on Iris Analysis",
US Patent5291560, 1994

Retina

- **Retina scanning**
  - Mapping of capillary vessels on the eyeground

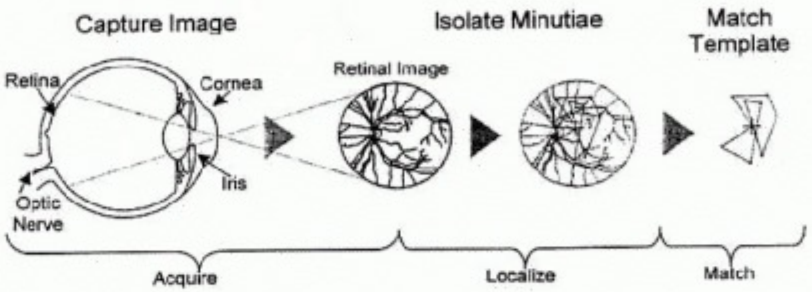
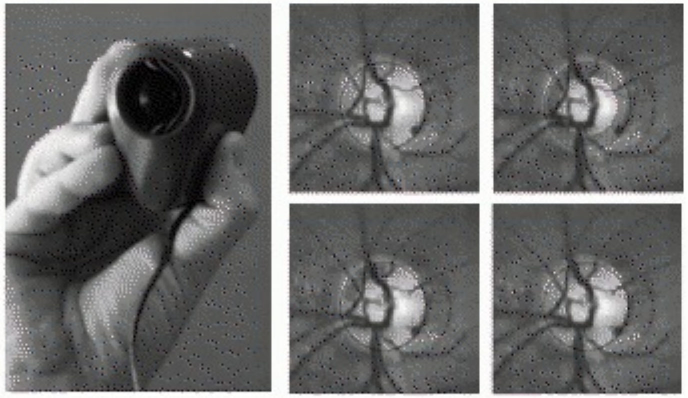
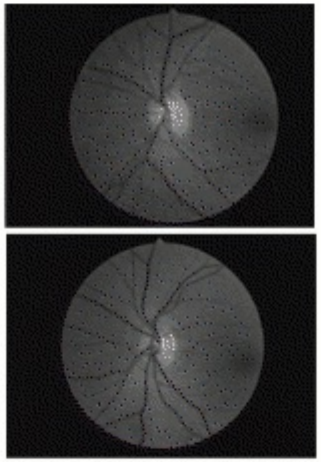


Exhibit 11-6. Retinal recognition process.



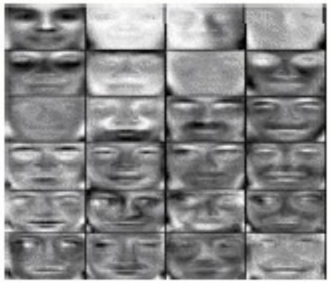


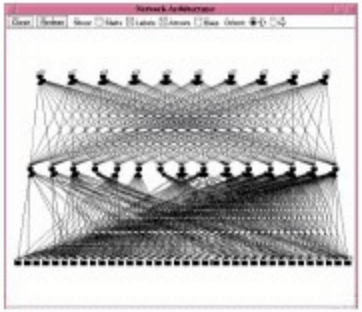
From: M. Nappi, Sistemi Biometrici, 2009

Face

Image Based

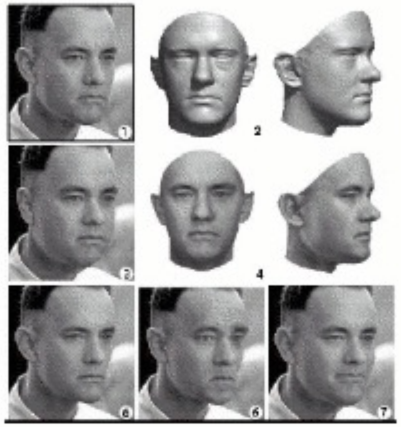
- ICA
- Neural Networks
- Eigenfaces





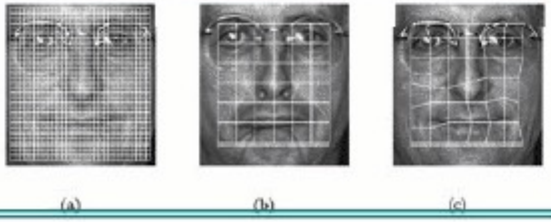
3D

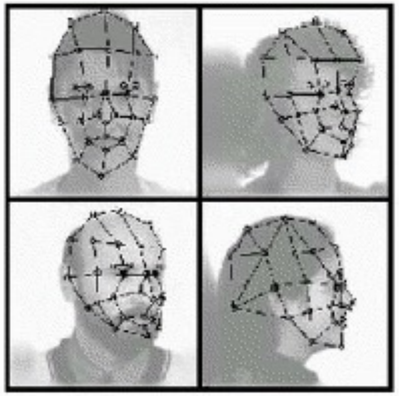
- 3D Morphable Models



Feature Based

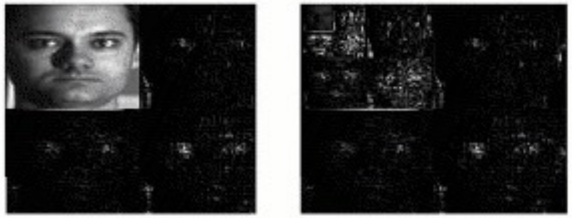
- Elastic Graph Matching





Hybrid

- Fractals
- Wavelets



From: D. Riccio, Face Recognition, 2007

The use of biometric traits

Biometric traits are a “natural” authentication methodology

- **Benefits**
  - Biometric traits cannot be lost, lent, stolen or forgotten (or changed either … see below)
  - The user must only appear in person

- **Drawbacks**
  - They do not ensure 100% accuracy
  - Some users cannot be recognized by some technologies (e.g. heavy workers show damaged fingerprints)
  - Some traits may change over time (e.g. face)
  - If a trait is “copied”, the user cannot change it, as it happens for usernames or passwords (plastic surgery ?)
  - Biometric devices may be unreliable under some circumstances.