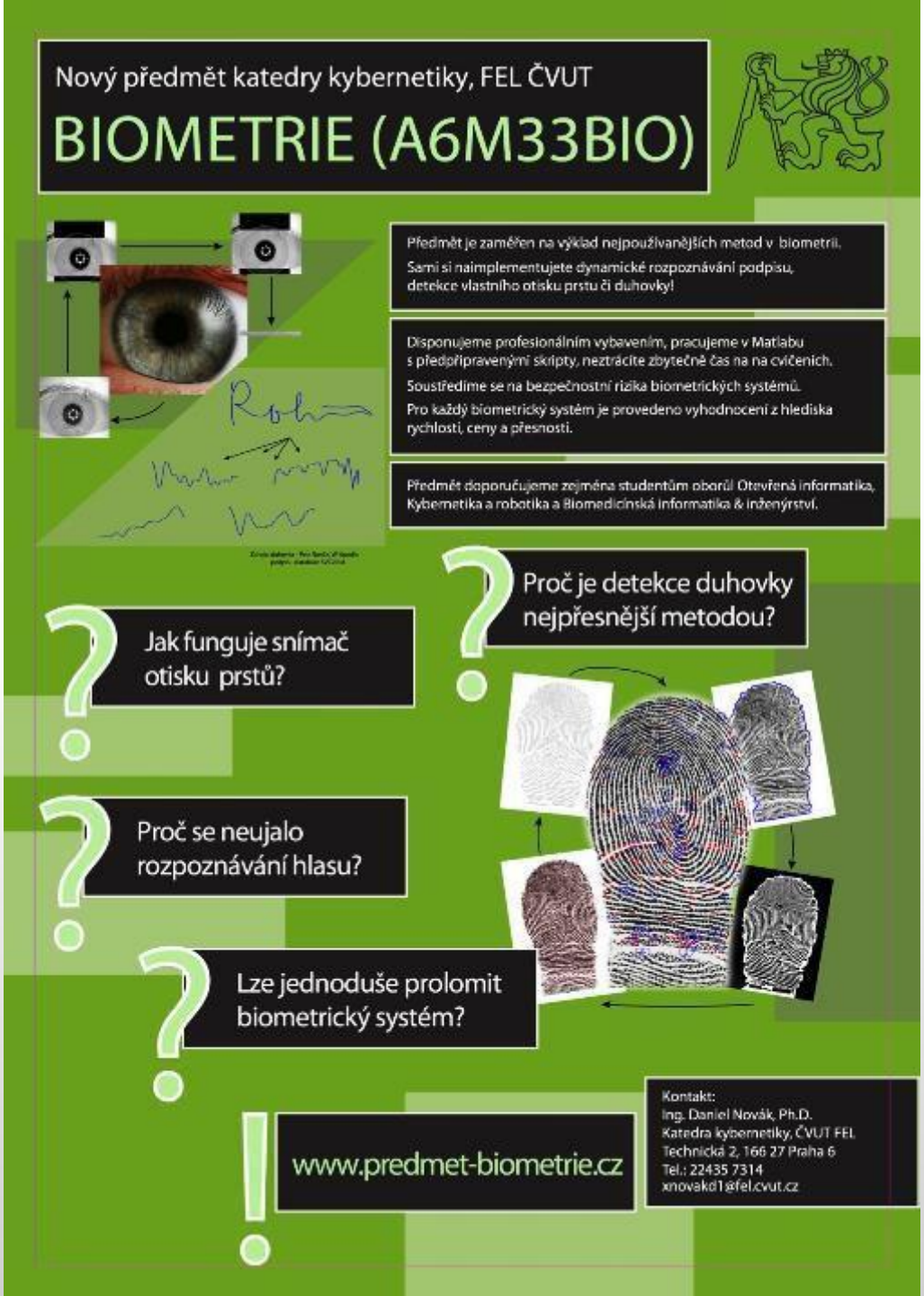


Biometrics Introduction

Daniel Novák
(+Eduard Bakštein)

4.10. 2018, Prague

Acknowledgments: Chang Jia, Andrzej Drygajlo

Outline

1. About the course
   - course logistics, contacts, syllabus, conditions
2. Biometrics: general introduction
   - Short history, what is biometrics
3. Basic statistical concepts in biometrics
   - Hypothesis testing, Type I and II error, FAR, FRR
4. Overview of biometric techniques
   - Fingerprint, signature, iris, face, pace…

1 About the course

Podmínky předmětu

- Garant předmětu: Daniel Novák, místnost E116, xnovakd1@labe.felk.cvut.cz
- Stránky předmětu
- https://cw.fel.cvut.cz/wiki/courses/a6m33bio/start
- 3. laboratorní úlohy – každá za 20 bodů, celkem 60 bodů
- Klasifikovaný zápočet – 20 otázek, každá za 2 body (celkem 40)
- Podmínky předmětu
- https://cw.felk.cvut.cz/doku.php/courses/a6m33bio/podminky

Body z předmětu	Stupeň ECTS	Známka
100–90	A	výborně
89–80	B	velmi dobře
79–70	C	dobře
69–60	D	uspokojivě
59–50	E	dostatečně
49 a méně	F	nedostatečně

Program přednášek

1. Úvod (Eduard Bakštein)
2. Podpis (Jakub Schneider)
3.-4. Duhovka (Eduard Bakštein)
5.-6. Otisk prstu (Daniel Novák)
7. Klasifikace a indexování v biometrických systémech (Daniel Novák)
8.-9. Tváře (Vojtěch Franc)
10.-11. Řeč (Petr Pollák)
12. Šifrování v biometrických systémech, padělky (Daniel Novák)
13. Závěrečný test, udělení klas. Zápočtu.

Program cvičení

Členění do třech bloků (+ úvod) – 3 úlohy

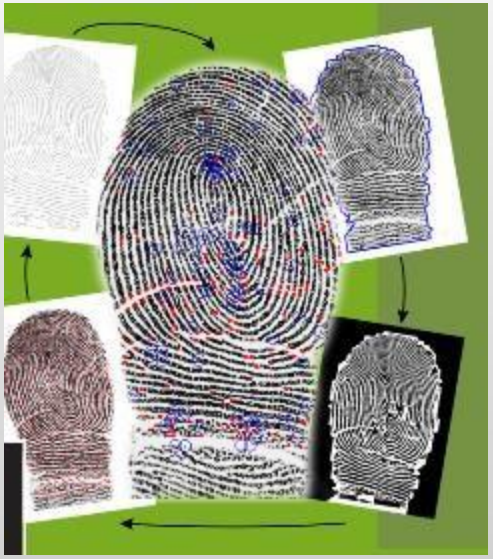
Práce na cvičení, popř. doma dokončit

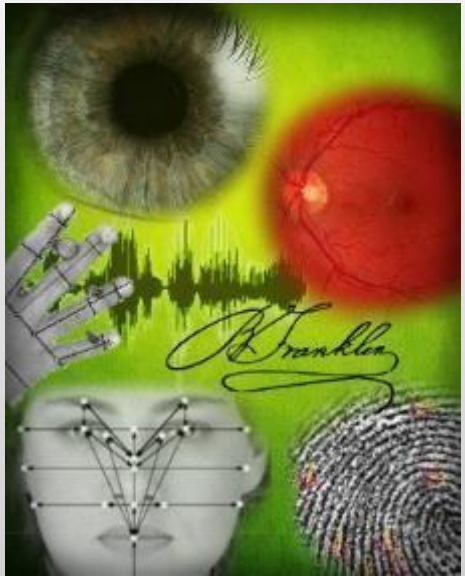
1	Základní biometrická statistika, latence úhozů
2.-4.	**Dynamický podpis** (Jakub Schneider)
5.-8.	**Duhovka** (Eduard Bakštein)
9.-13.	**Otisk prstu** (Jakub Schneider)

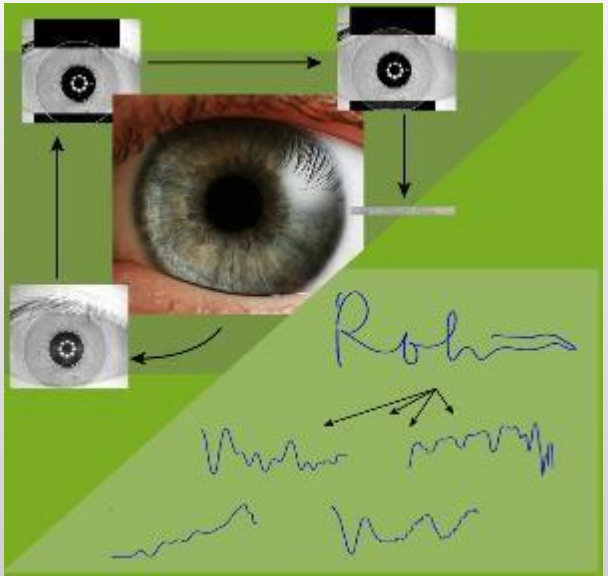
Facebook, Twitter, Web

- **Přispívejte zejména vy!!!!**
- Facebook (zalikujte, pokud se vám předmět bude líbit:)
- http://www.facebook.com/biometrieCVUT

- Webové stránky
- http://www.predmet-biometrie.cz/





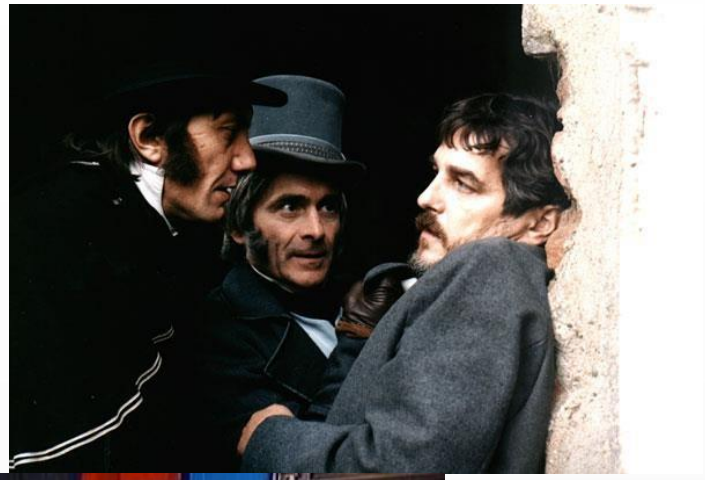


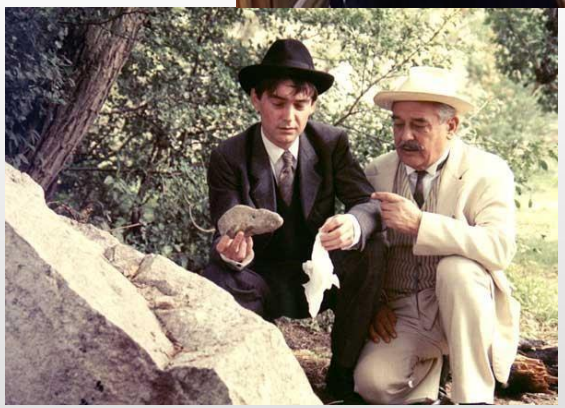
2 Biometrics: general introduction

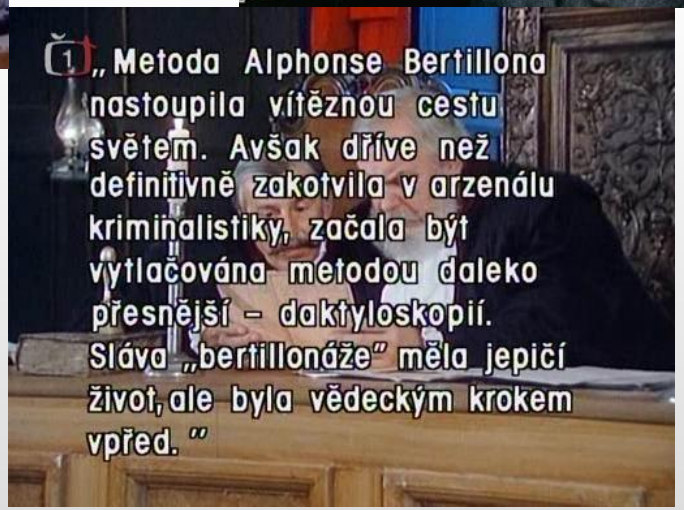
Biometrics: what for?

- Identification of individuals: ID is missing or can not be trusted
- Forensic applications
- Surveillance-free applications
- Humanitary applications

Alternative introduction

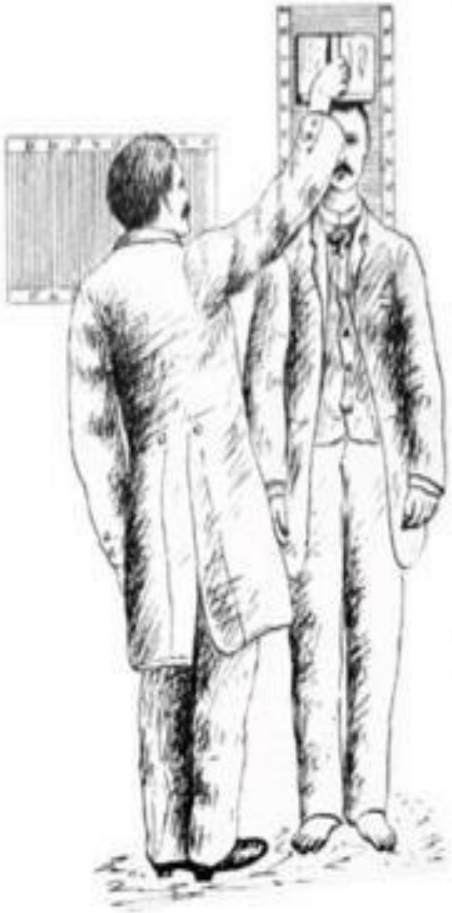


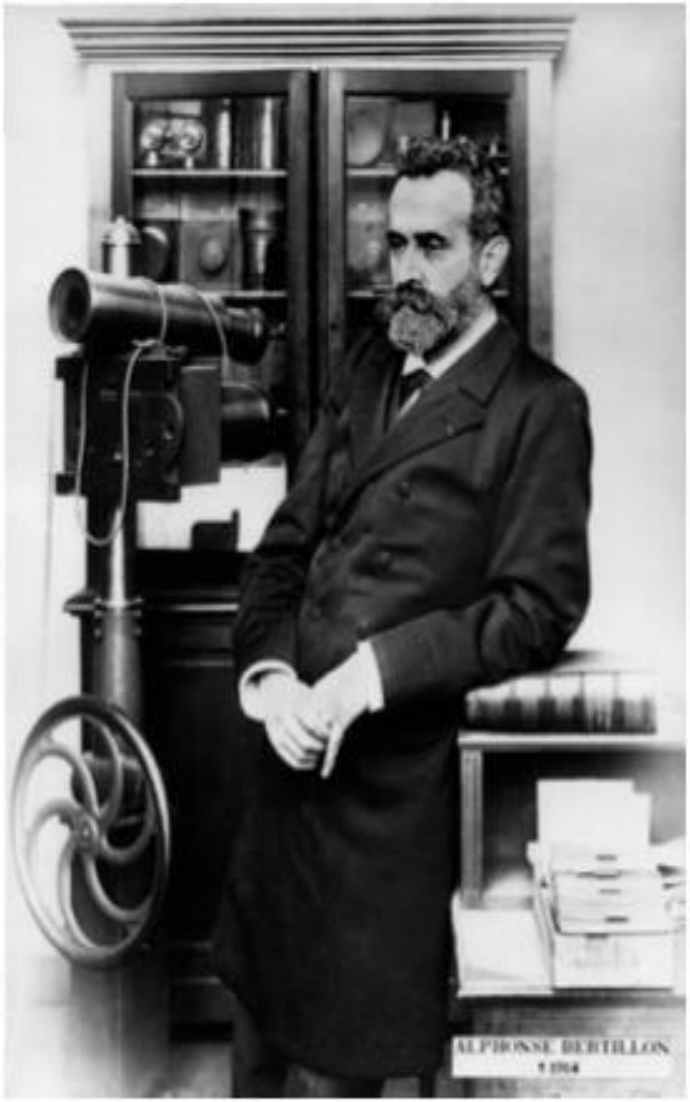




- Dobrodužství kriminalistiky na csfd
- Dobrodužství kriminalistiky na CT

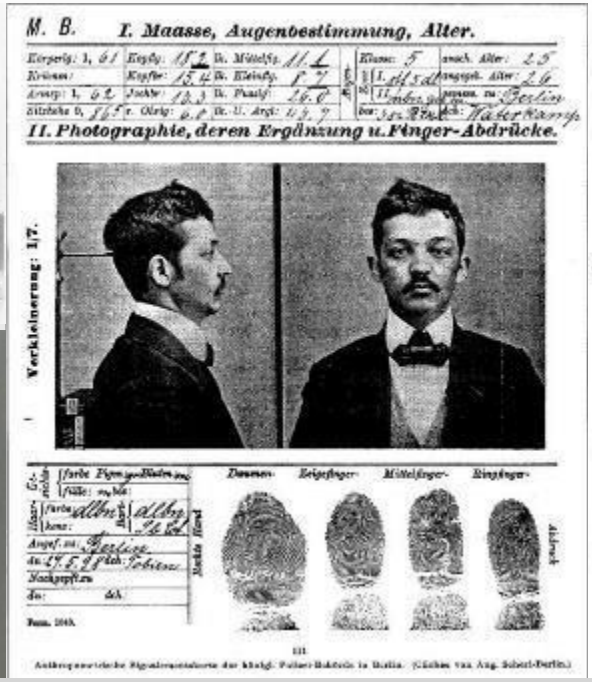
Alphonse Bertillon: Forensic Anthropometry





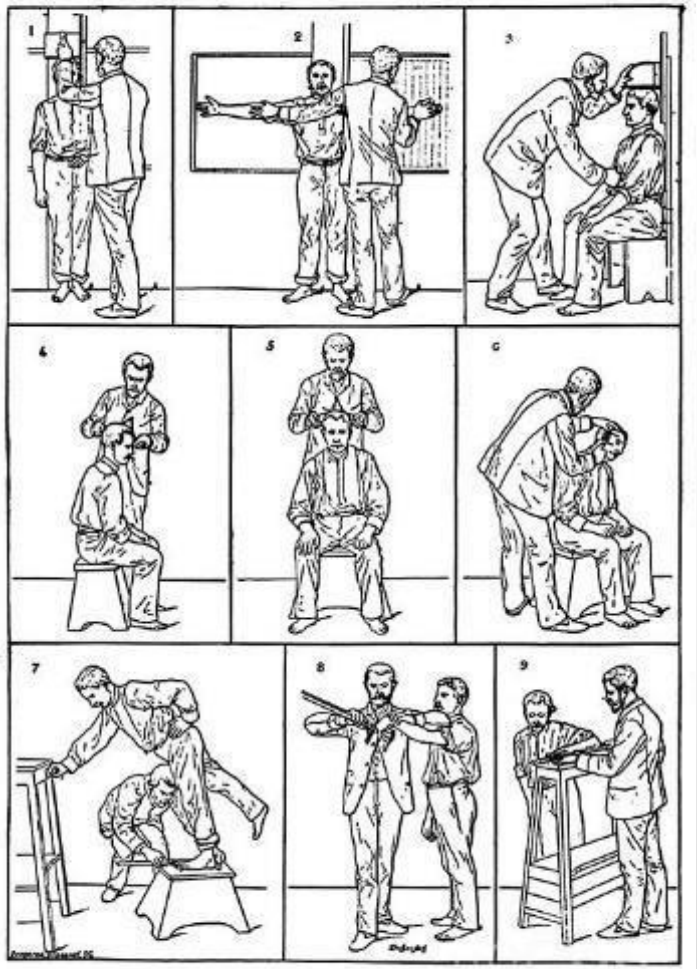
Alphonse Bertillon: antropometry

- System of physical measurements
- Invented **1879**, adopted by French police
- 1887 – adopted by US police
- Superseded by fingerprint identification in ca 1903
- „mug shot“ – still used



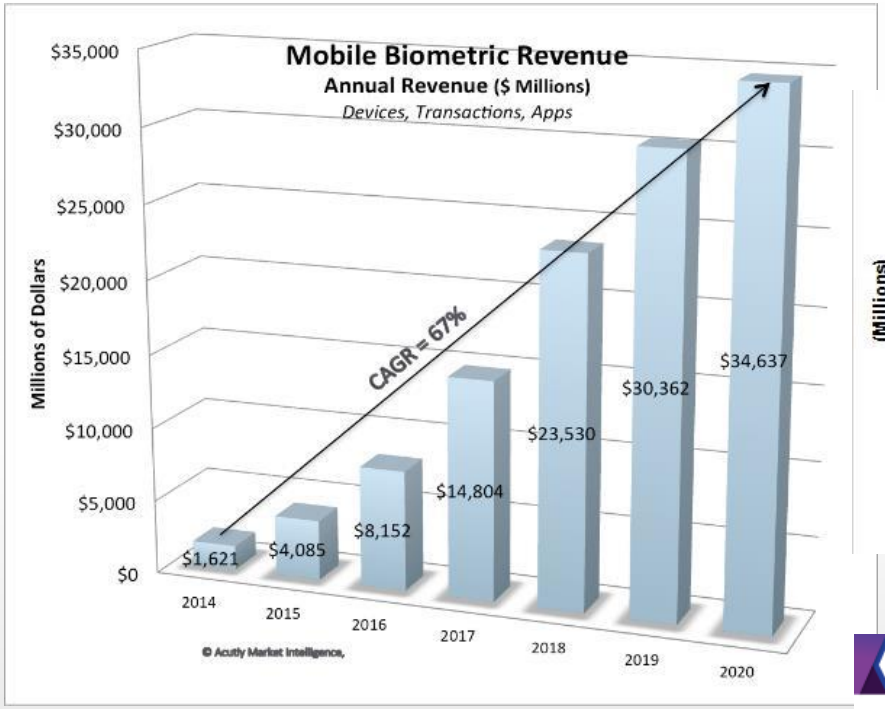
ABSTRACT OF

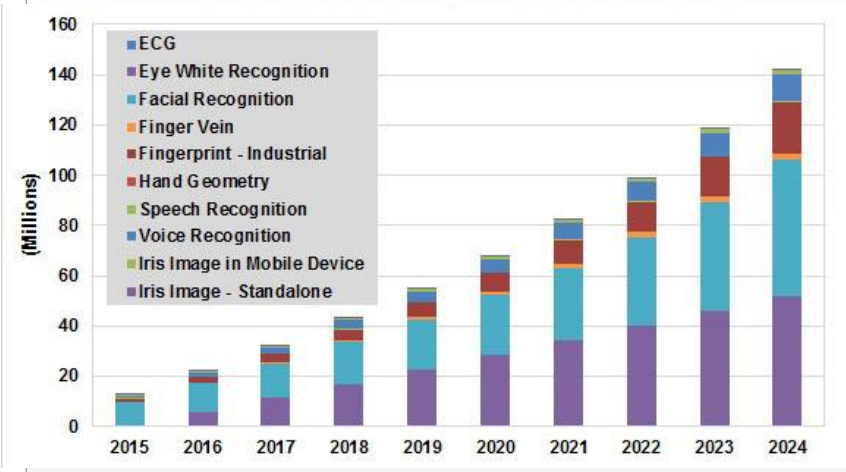
THE ANTHROPOMETRICAL SIGNALMENT



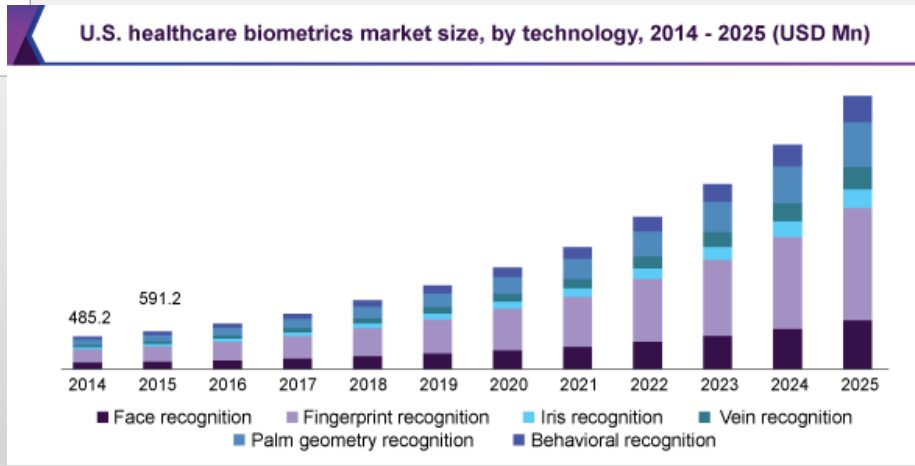
1. Height. 2. Reach. 3. Trunk.
4. Length of head. 5. Width of head. 6. Right ear.
7. Left foot. 8. Left middle finger. 9. Left forearm.

Trend: revenue of the field

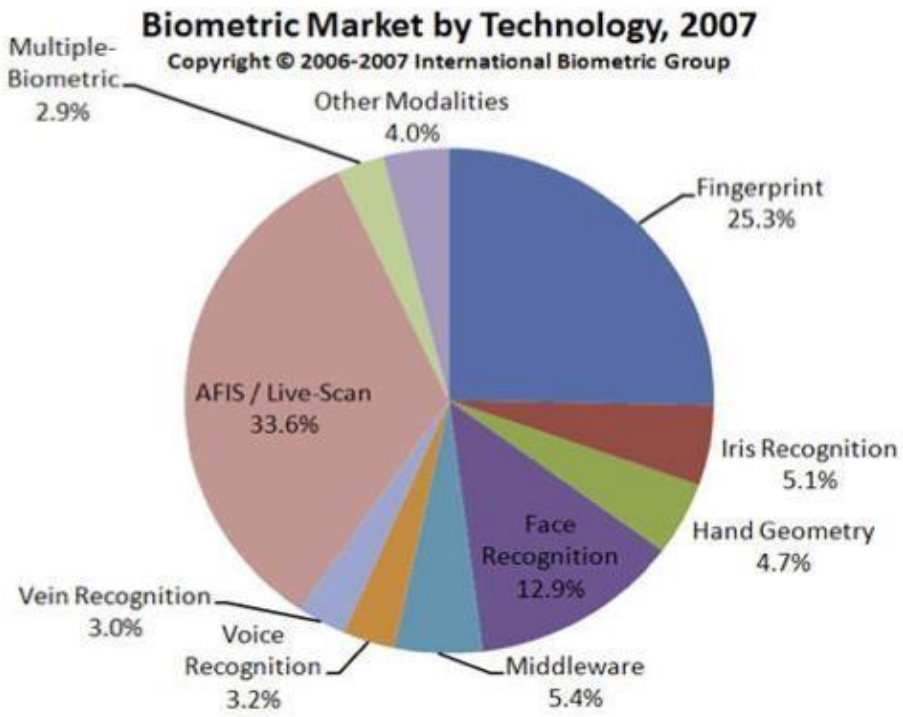




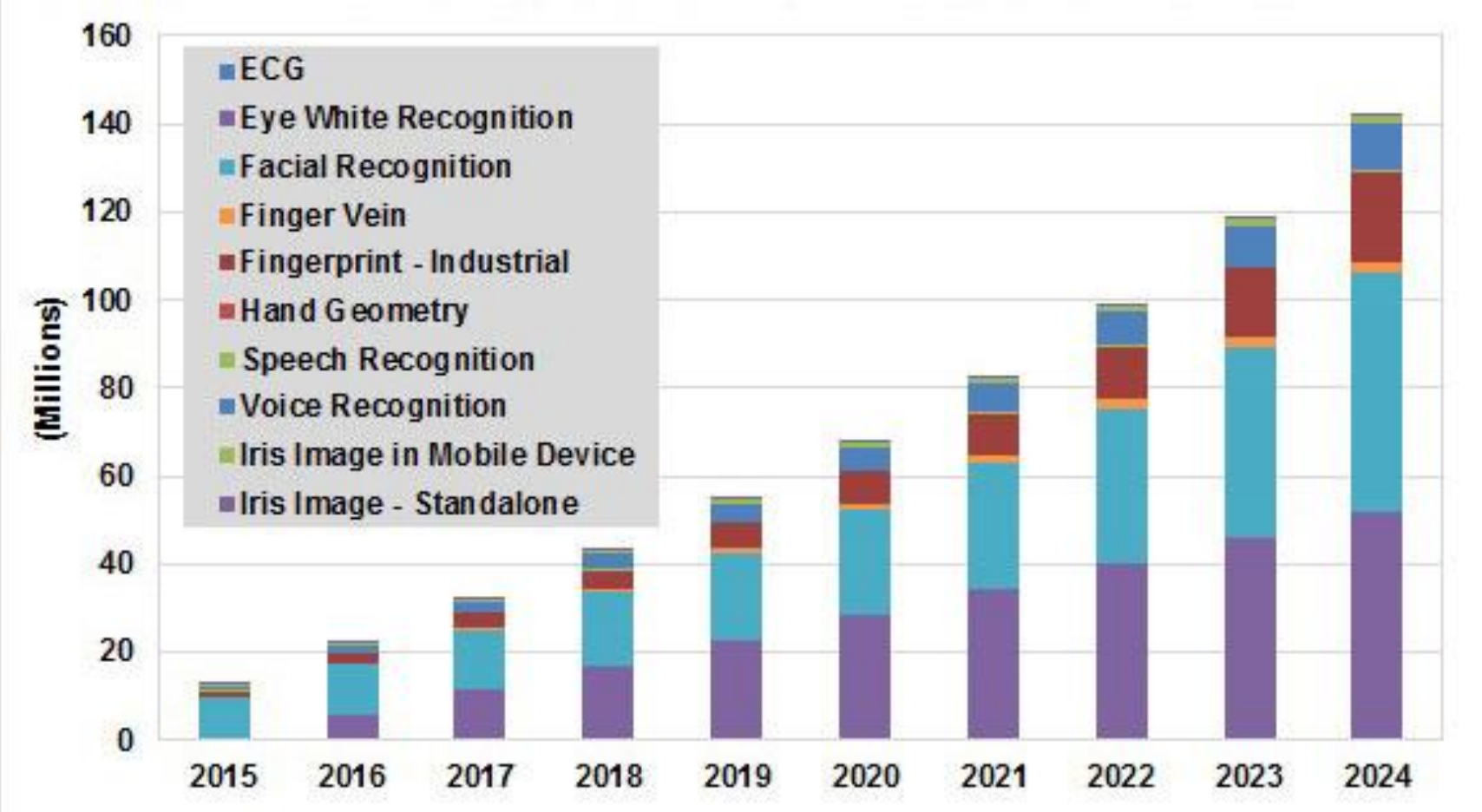
Analytics forecast steady rise
(historical data hard to find)



History: Market Share in 2007



Market share projection



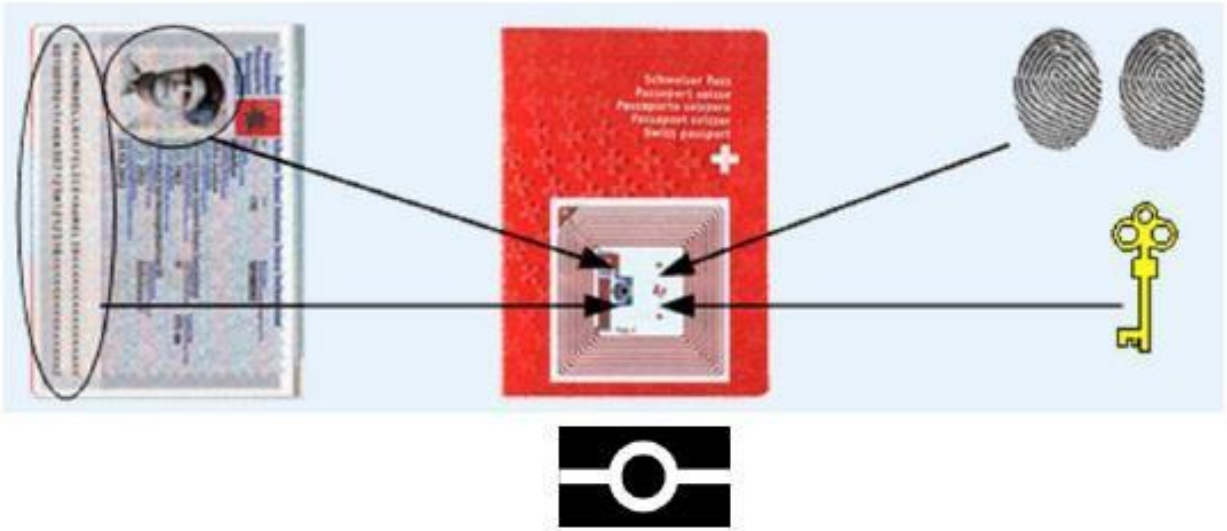
ePassport – Biometric passport

Necessary condition for travel to USA+ESTA. In ČR since 2006 (required by EU regulations), since April 2009 - 2 fingerprints included

http://czech.prague.usembassy.gov/biometricky_pas.html

http://www.youtube.com/watch?v=ptb_nxCpgYQ

In accordance with ICAO and EU specifications, the data of the machine readable zone, the facial image and two fingerprints plus electronic signatures will be stored in the chip.



Integration of Technologies: chip card (smart card), radio-frequency identification (RFID), electronic signatures and public key infrastructure (PKI), back-office systems (databases), biometrics

Since 2003: eBorders in the United Arab Emirates

- Iris recognition system
- Fully operational since April 2003
- 36 land, air and sea ports
- 12,000 passengers each day

- 1 central database
  - Watchlist application
  - Fully networked
  - Enrolment centres: prisons and deportation centres
  - More than 1 million enrolments (150+ nationalities)
  - Exhaustive search takes <2 seconds

- 12 billion comparisons each day (12,000 passengers against 1 million enrolments)
- About 50,000 persons caught since launch

400 000 caught (2015)

Replaced in 2015 bymultiple=biometric system

Stolen identity

Article in NY times and Telegraph, Hamas was responsible

- February 2010: Dubai Hamas murder: Fraudulent foreign passports were used by the alleged killers of a Hamas commander in Dubai

- One of the victims of the identity theft was British-Israeli Paul John Keeley (picture right). The passport used by one of the suspected assassins bore his name, but featured a photograph of another man (pictured left)

Another stolen identity

- HW – Unknown watch and rate at CSFD (71%)

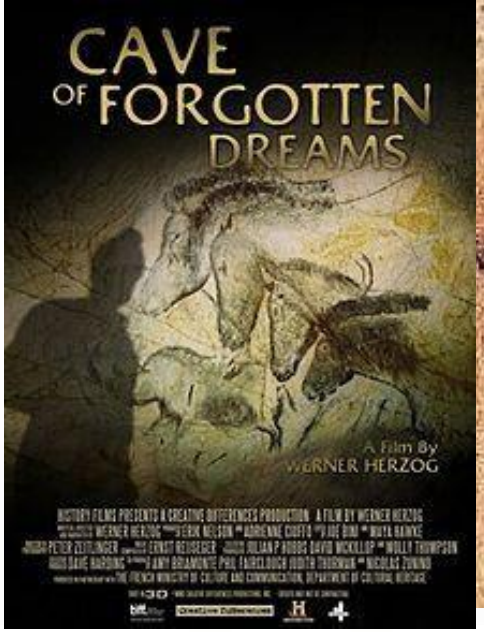
What is Biometrics?

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure)

- **Biometrics** – automated recognition of individuals based on their biological and behavioral characteristics
  - *Scientific follow-on to Bertillon's body measurements of the late 1800s*
- **Biometry** – statistical and mathematical methods applicable to data analysis problems in the biological sciences
- **Biometric system** – essentially an automatic pattern recognition system that recognizes a person by determining the authenticity of a specific biological and/or behavioral characteristic (biometric modality) possessed by that person
- **Anthropometry** – measurement techniques of human body and its specific parts
  - ***Forensic (judicial) anthropometry*** *– identification of criminals by these measurement techniques*

History of biometrics

- Well-done summary: http://www.biometrics.gov/documents/biohistory.pdf
- Oldest paintings in Chauvet cave, palm prints: I painted it! (documentary by Herzog)



- Ancient civilisations practised biometric techniques routinely.

Sumerians considered a hand print and outline of a hand on a clay tablet a good identifier.

- Egyptians brought the concept of biometric identity verification into the mainstream, in many various ways:
  - From discrete anatomical measurements, e.g., distance between the individuals outstretched thumb and the tip of the elbow
  - To more general notification of individual features, e.g., Nechutes, son of Asos, aged 40, of middle size, sallow complexion, cheerful countenance, long face with straight nose and a scar upon the middle of his forehead.

Identity Verification by Animals - Examples

- Penguins - by voice recognition to locate their offspring within a population sometimes numbering hundreds of thousands
- Frogs – discriminate between neighbours and strangers by voice recognition
- Hawks and other birds – by using visual information
- Wolves – by voice at a distance and corroborate this information by visual cues and scent at shorter distances
- Insects (bees, wasps, ants, etc.) – practice identity verification routinely

Traditional modes of authentication

- Possession-based schemes

  Based on ID cards, tokens, keys, etc.

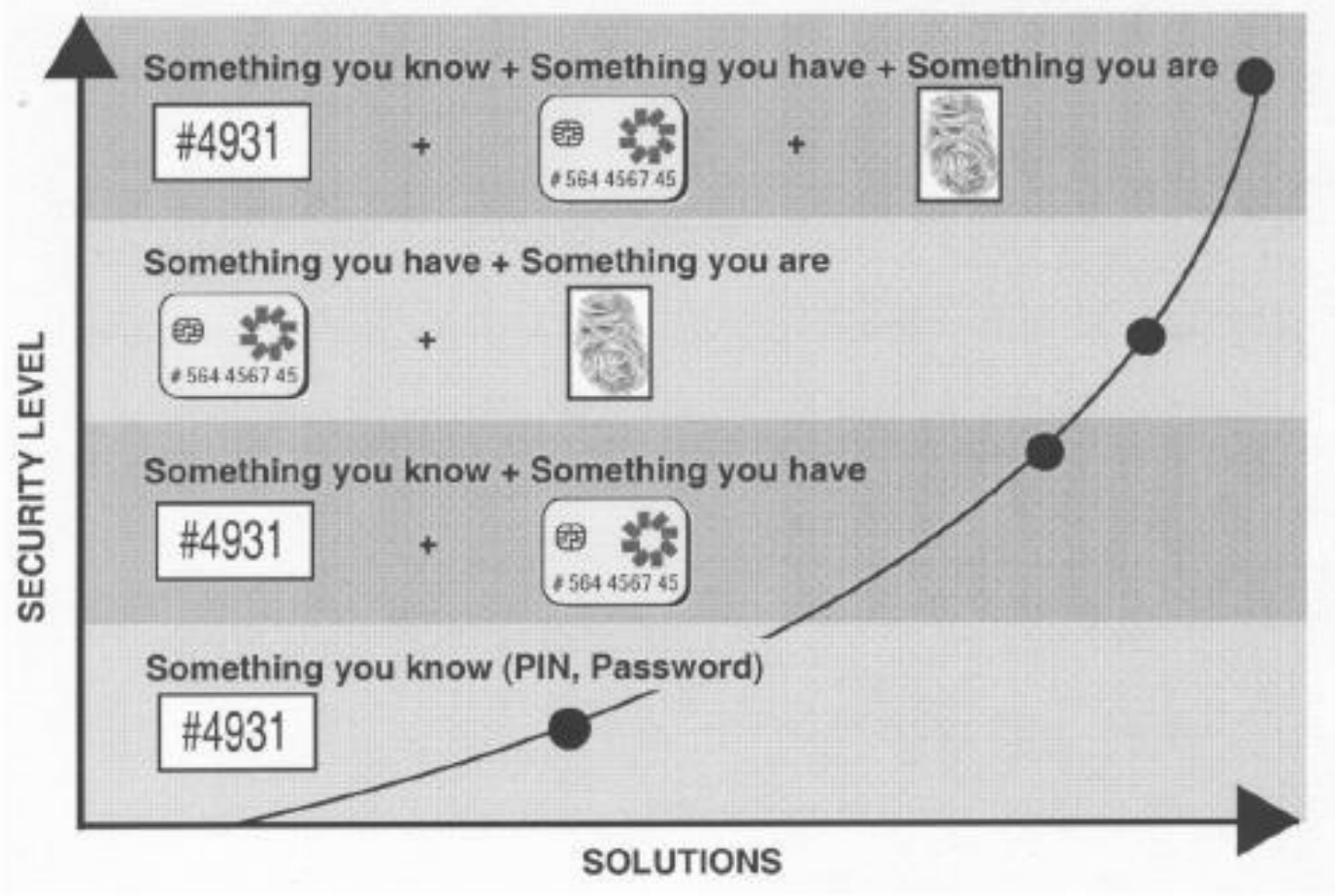
  WHAT YOU HAVE

- Knowledge-based schemes

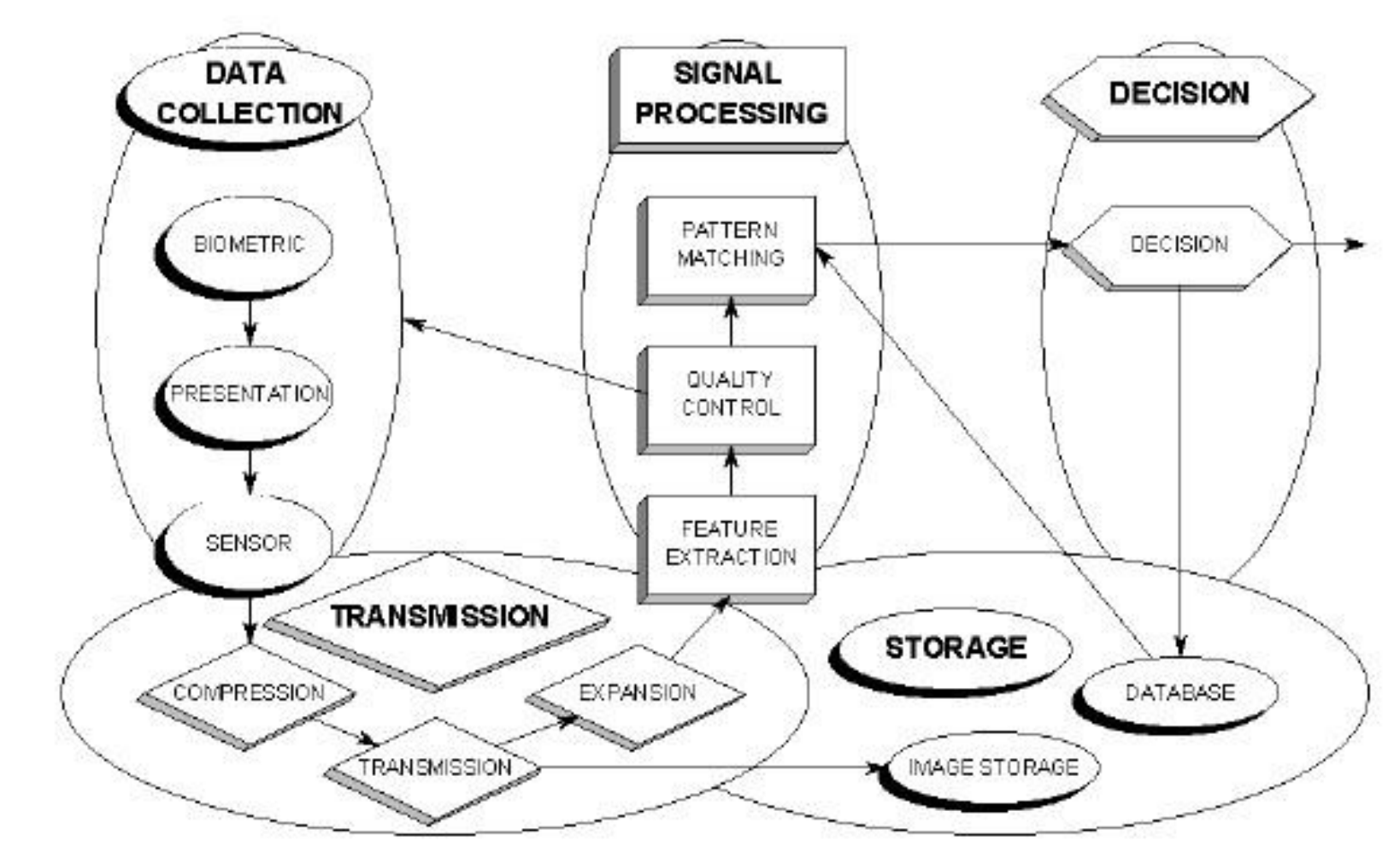
  Based on passwords, PINs, etc.

  WHAT YOU KNOW

Three basic means

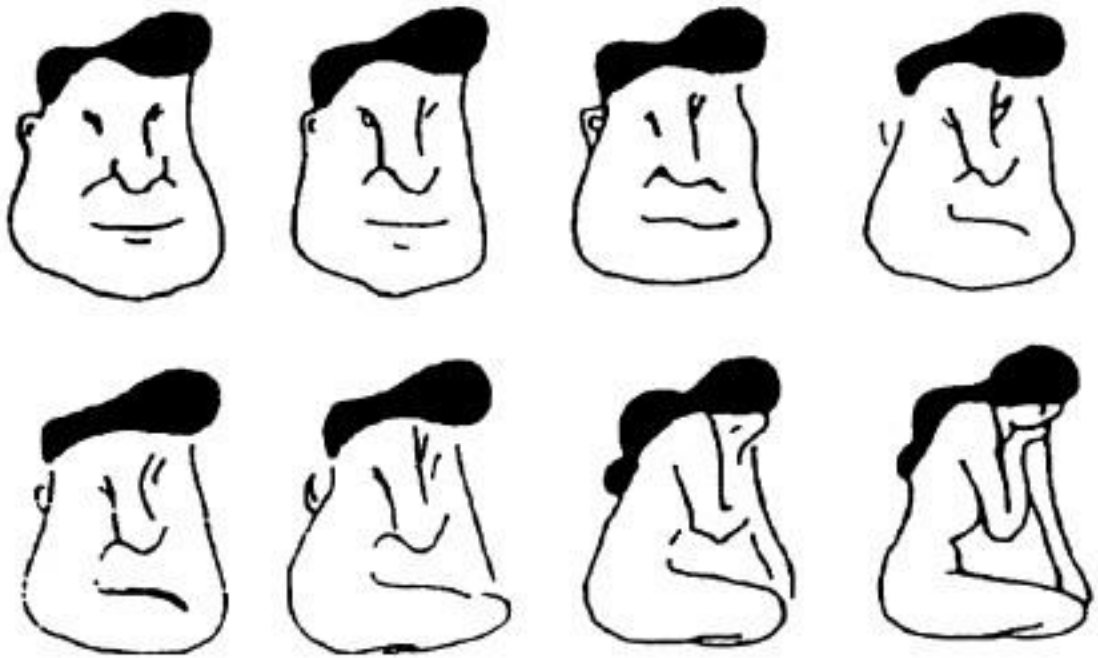


Generic Biometric System



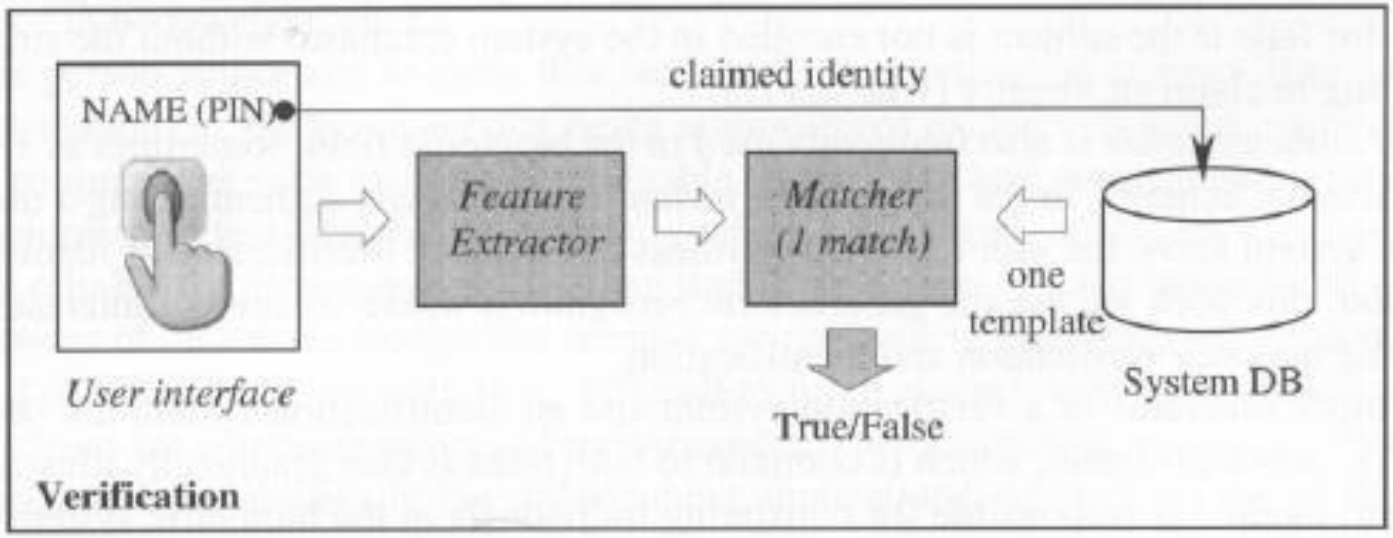
Pattern Recognition System

Two patterns are similar, if an appropriately defined distance measure between their feature vectors is small



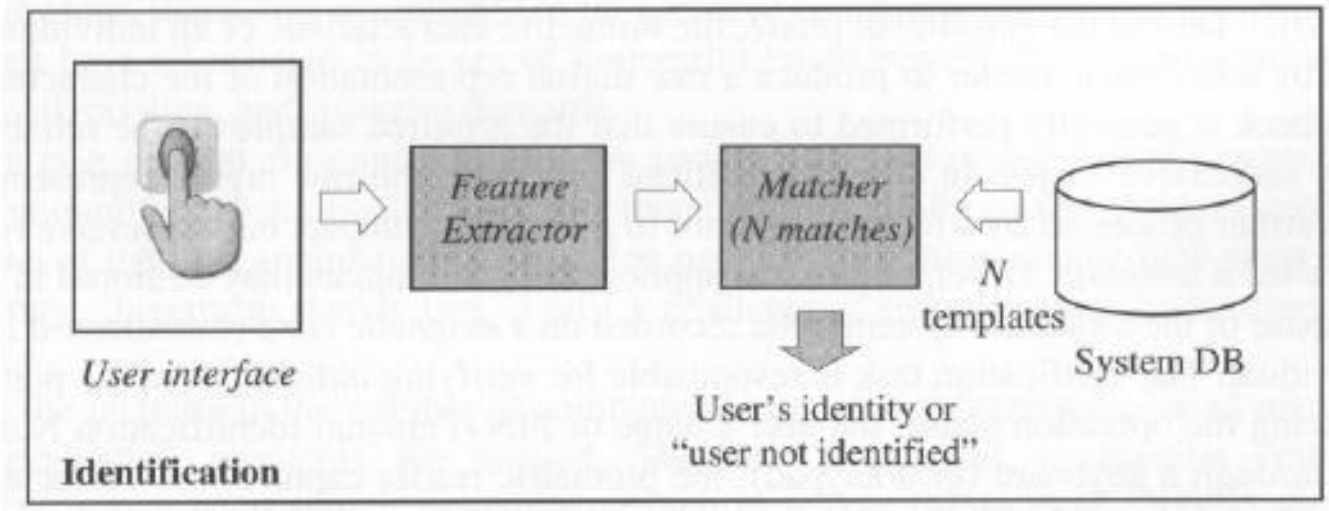
Person recognition

- Verification – biometric system function that performs a one-to-one comparison of a submitted biometric characteristic (sample) set against a specified stored biometric references, and returns the comparison score and decision.
- "Is this person who he claims to be?"

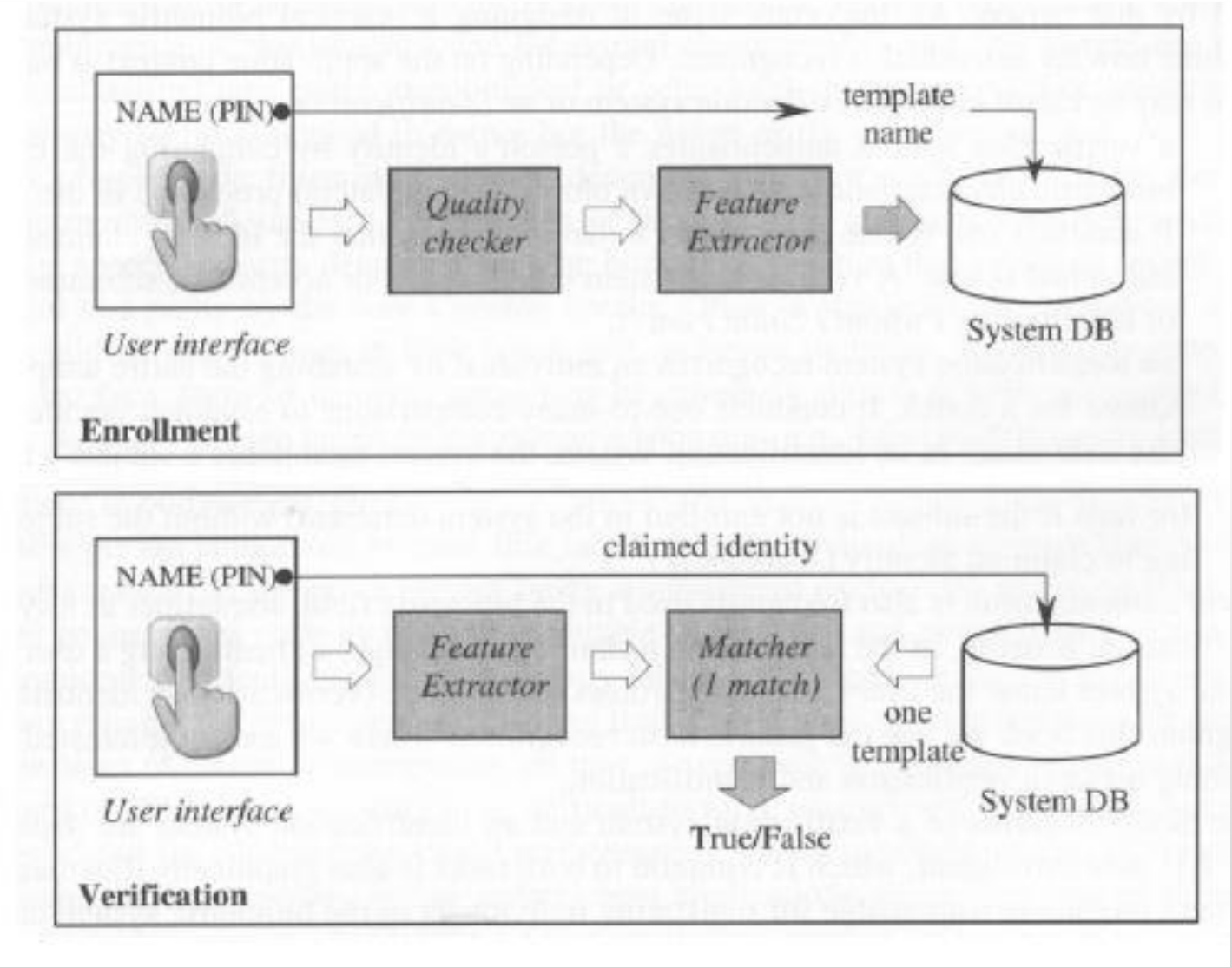


Identification

- Identification – biometric system function that performs a one-to-many comparison/search process in which a biometric characteristic set is compared against all or part of the database to find biometric references with a specified degree of similarity.
- "Who is this person?"

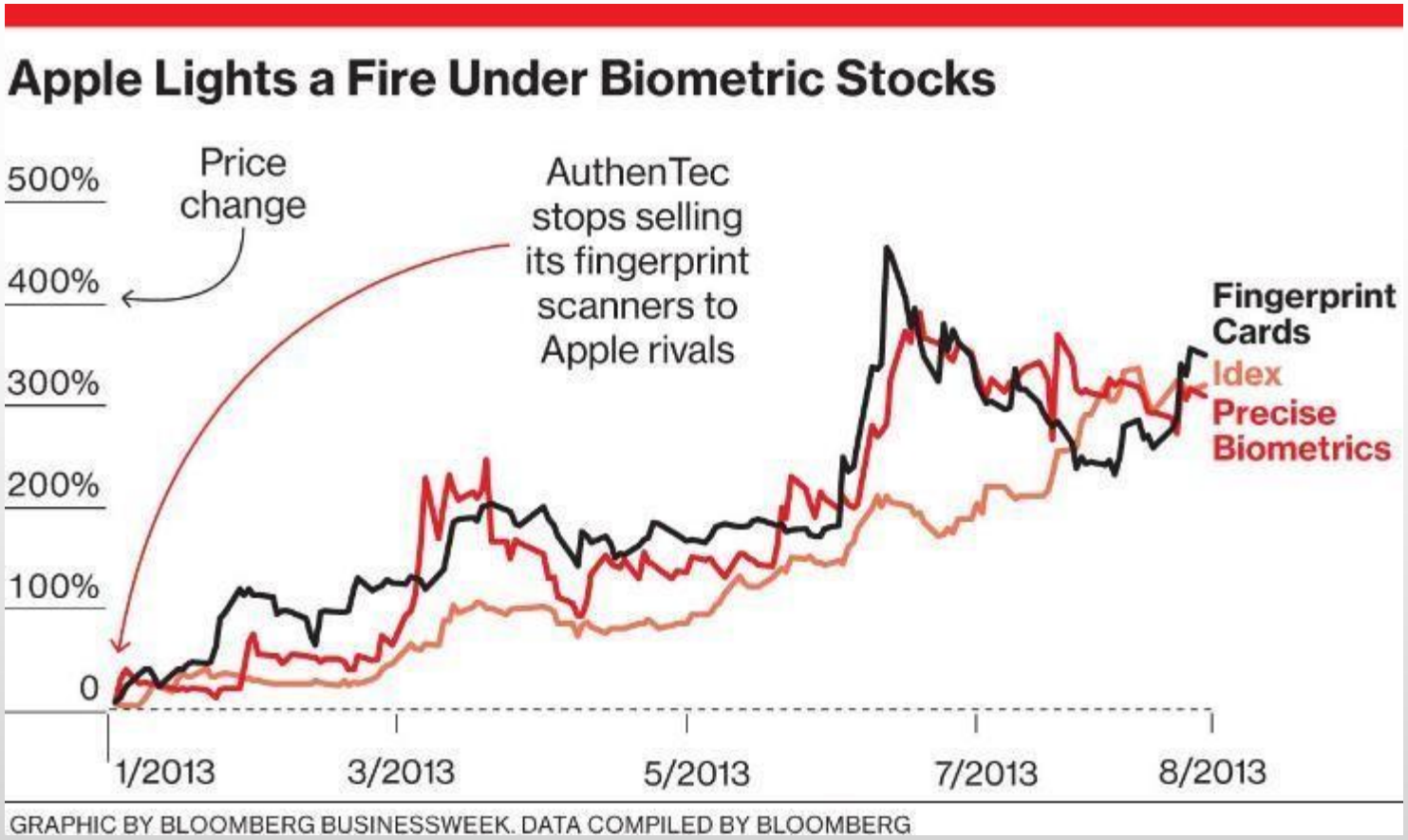


Enrollment


NAME (PIN)
template name
Quality checker
Feature Extractor
System DB
User interface
Enrollment
claimed identity
NAME (PIN)
Feature Extractor
Matcher (1 match)
one template
System DB
User interface
True/False
Verification

Some statistics of Mobile devices

Nice example – Motorola Atrix 4G using swipe fingerprint AuthenTec sensor
Company was bought by Apple in July 2012 for 356$ mil (8$ for share – cutrent value: 5$)

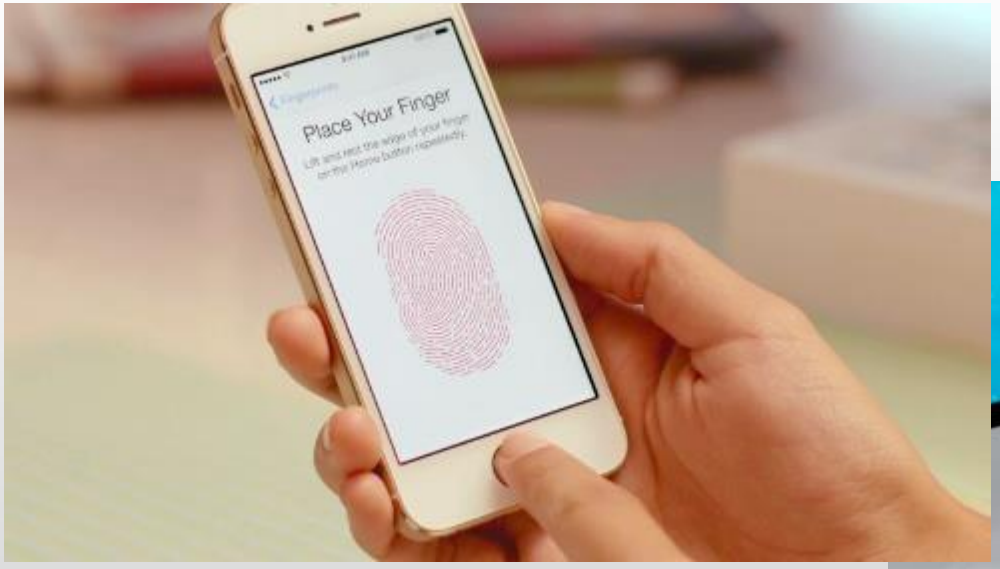


Mobile phone apps

- HW: try out and paste to fb or twitter
- BioLock, youtube video:

Mobile biometrics: future development?

- Iphone 5s (release 09/2013) has fingerprint sensor for authentication
- First mainstream smartphone with hw biometric sensor
- Iphone X (09/2017): 3D face scan



Biometrics in everyday technology

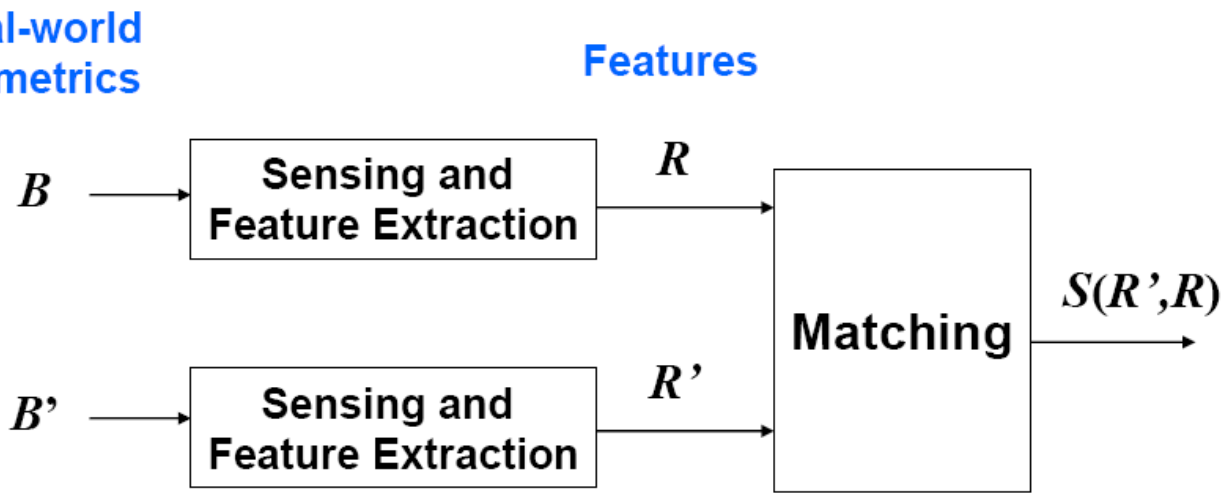
- **Face recognition**
- Android: first at Android 4.0 (2011) Android L (2014)
- **Fingerprint recognition:**
- iPhone since 5s (2013) „Touch ID“,
- Samsung since Galaxy S5 (2014) • Windows 10 („Hello“):
- **Face (IR 3D scan – intel realSense),** Fingerprint, iris (Lumia 940/950XL)
- Iris recognition: Microsoft Lumia 940/950 XL
- announced 10/15 ??

3 Basic statistics for biometrics

Example Iris & Speech

- Example
  - Assume 10'000 customers are signed up for biometric authentication and 1'000 transactions are done weekly
  - Assume best-case biometric verification error of 1 in 1 million (iris)
  - Assume best-case speaker verification error of 1 in 1 hundred
  - How often are customers falsely billed?
- Answer
  - On average 10 people are falsely billed each week
  - On average 100 000 people are falsely billed each week

Matching



$$s(R', R) = s(f_{t'}(B'(t')), f_t(B(t)))$$

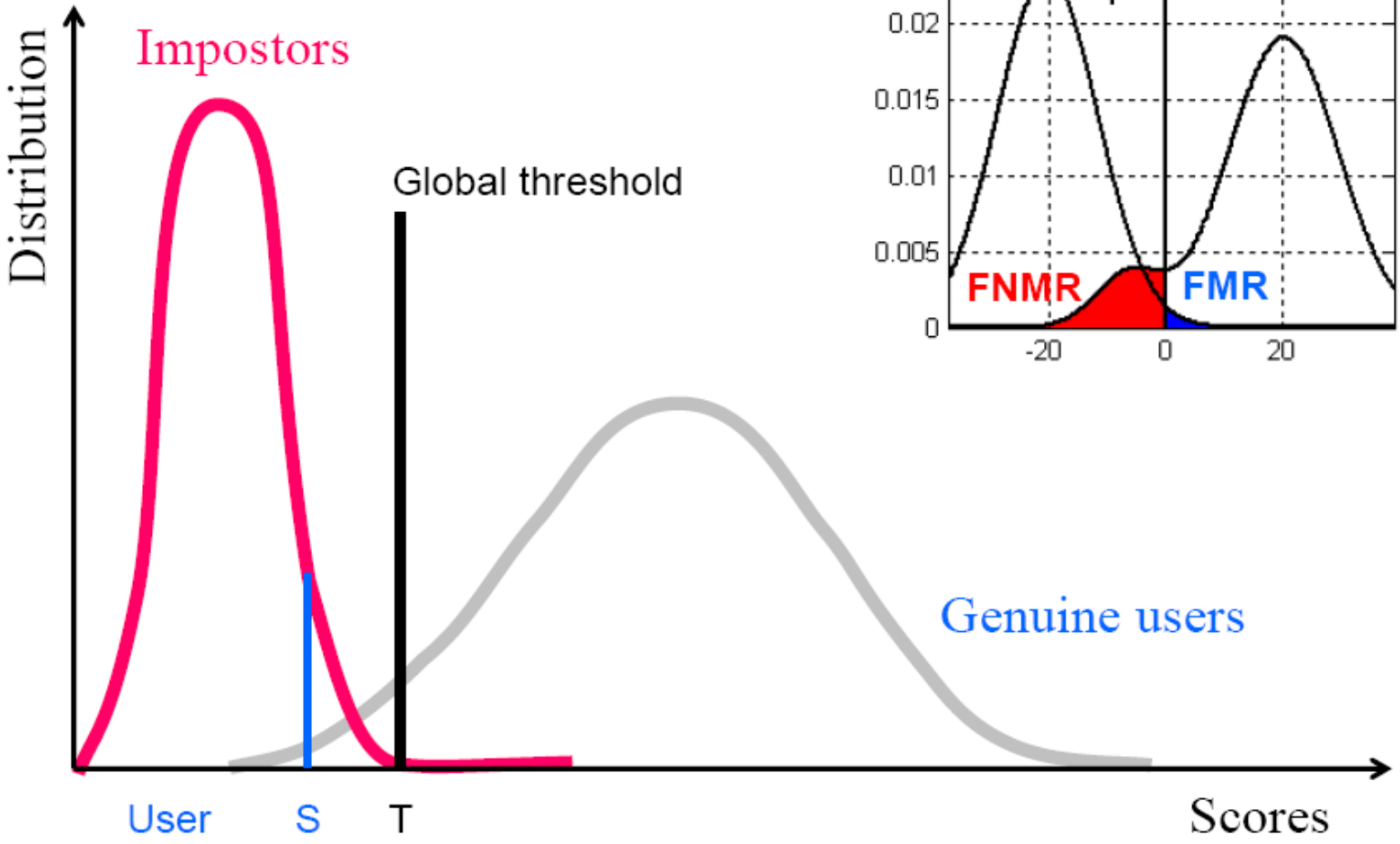
Biometric matching makes a decision by computing a measure of the likelihood that the two input samples from two persons are the « same » and hence that the subjects are the same real-world identity.

FA & FR

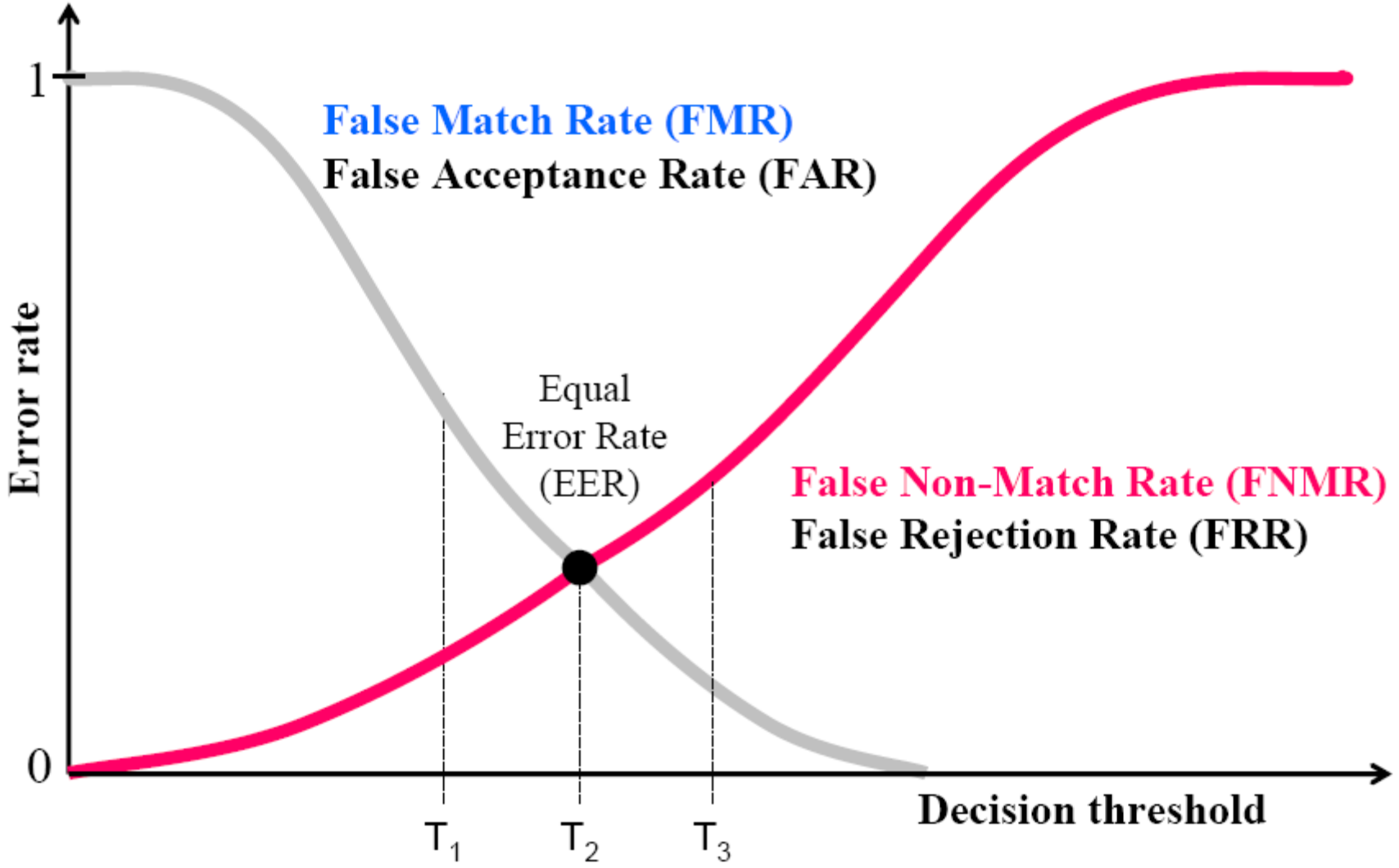
- **False Accept (FA):** Deciding that a (claimed) identity is a legitimate one while in reality it is an imposter; False Accept Rate (FAR)
- **False Reject (FR):** Deciding that a (claimed) identity is not legitimate when in reality the person is genuine; False Reject Rate (FRR)

- A **FA** results in security breaches, with an unauthorized person being admitted
- A **FR** results in convenience problems, since genuinely enrolled identities are denied access to the application

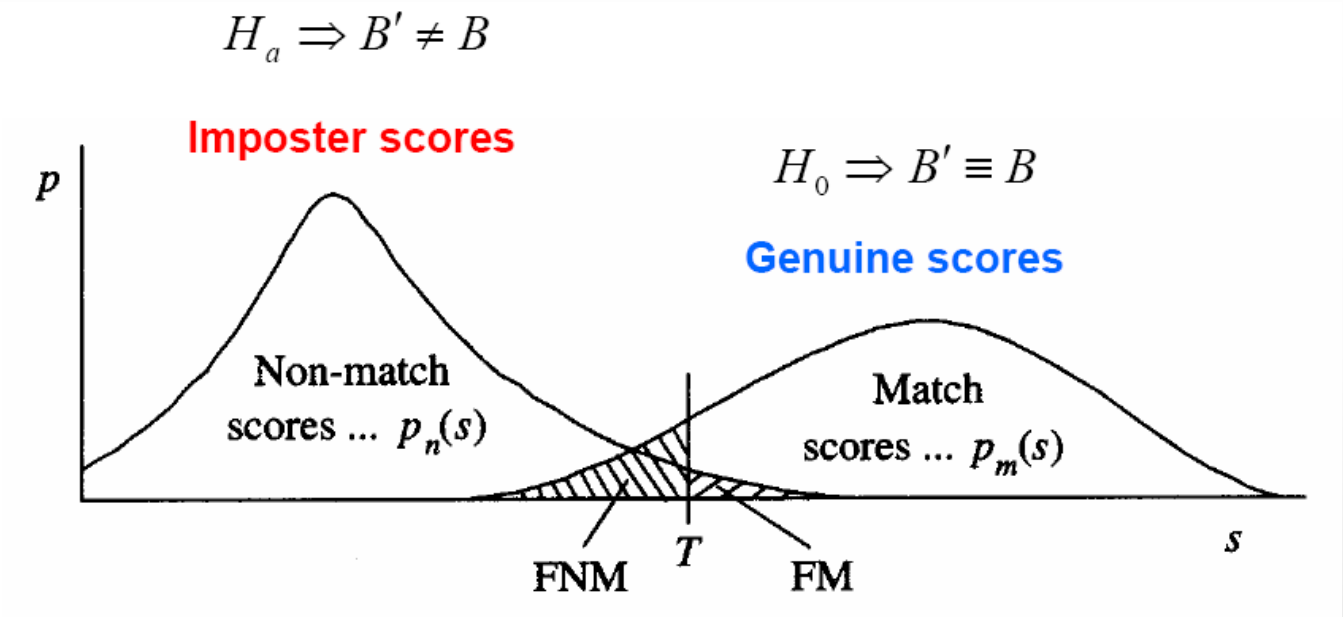
Performance evaluation



FMR and FNMR


1
0
Error rate
False Match Rate (FMR)
False Acceptance Rate (FAR)
Equal
Error Rate
(EER)
False Non-Match Rate (FNMR)
False Rejection Rate (FRR)
T1
T2
T3
Decision threshold

Scores distribution



Given two biometric samples, we can construct two possible hypotheses:

The null hypothesis:	$H_0 \Rightarrow$	the two samples match
The alternate hypothesis:	$H_a \Rightarrow$	the two samples do not match

Two kinds of error

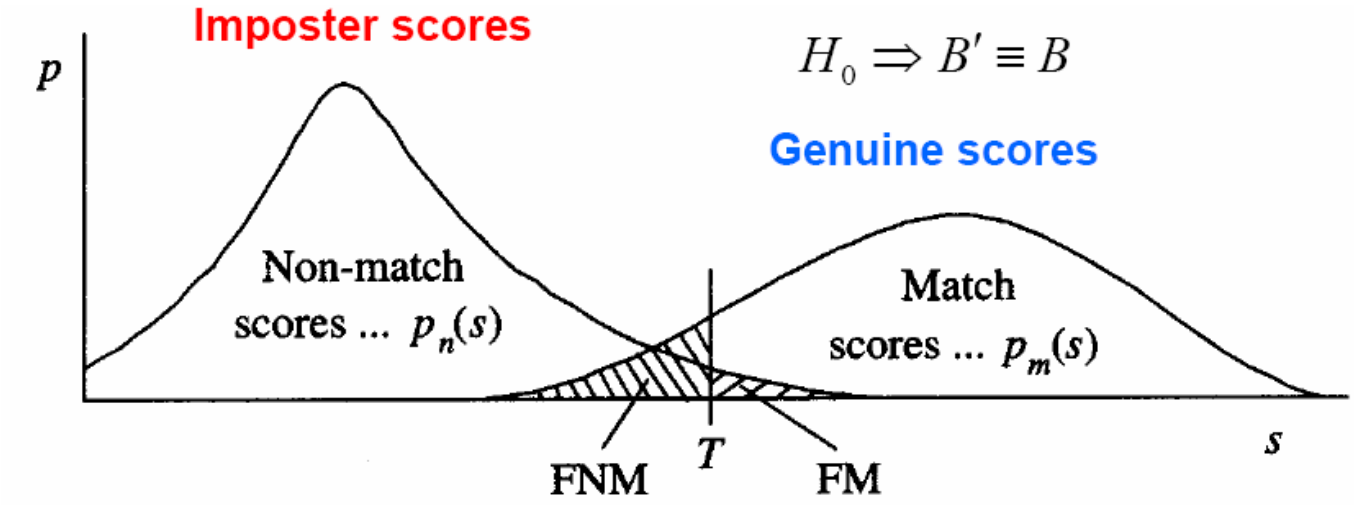
- Verification:

$$\text{Decide } H_0 \text{ is true: if } s > T,$$
$$\text{Decide } H_a \text{ is true: if } s \leq T.$$

- Type II error False Match (FM): Deciding that two biometrics are from the same identity, while in reality they are from different identities; the frequency with which this occurs is called the False Match Rate (FMR)
- Type I error False Non-Match (FNM): Deciding that two biometrics are not from the same identity, while in reality they are from the same identity: the frequency with which this occurs is called the False Non-Match Rate (FNMR)
- Correct Match: correctly deciding that two biometric samples match
- Correct Non-Match: correctly deciding that the samples do not match

Two kinds of error

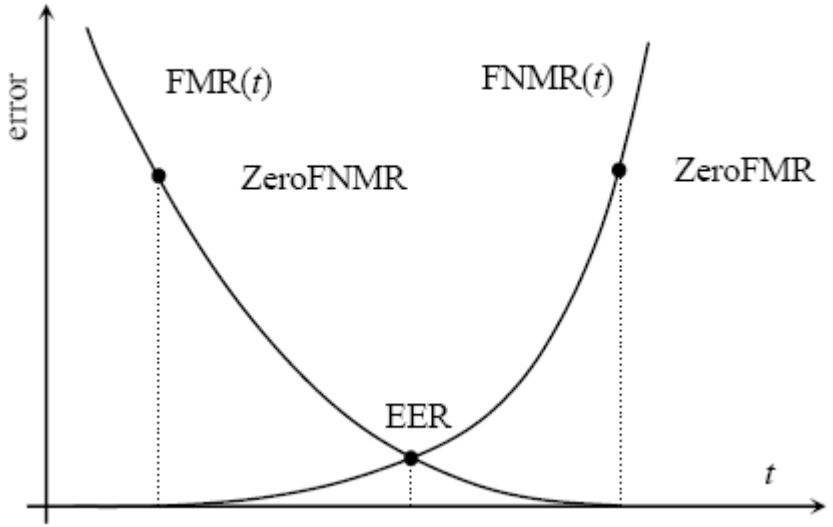
$H_a \Rightarrow B' \neq B$



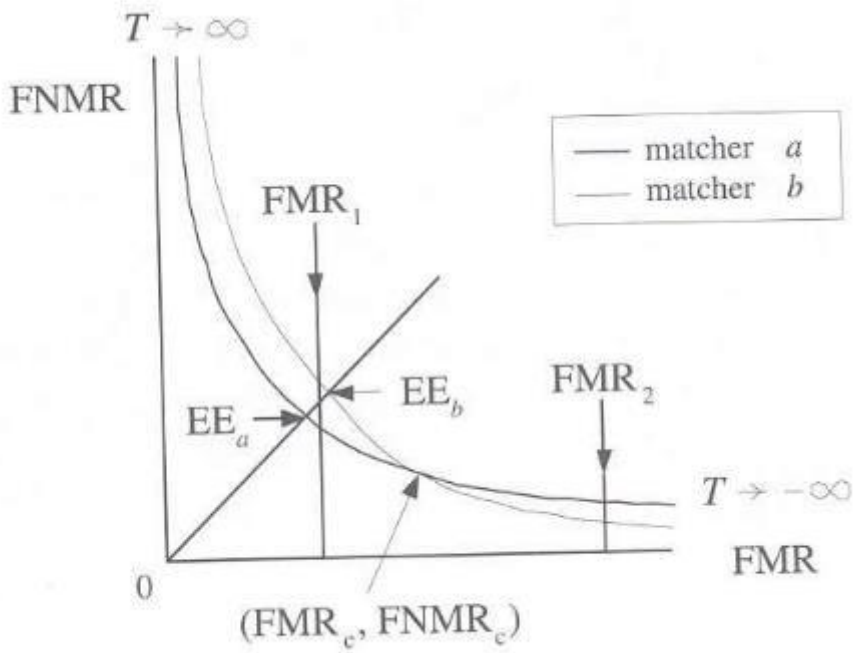
$$\mathrm{FNMR}(T) = \int_{s=-\infty}^{T} p_m(s)ds$$

$$\mathrm{FMR}(T) = \int_{s=T}^{\infty} p_n(s)ds$$

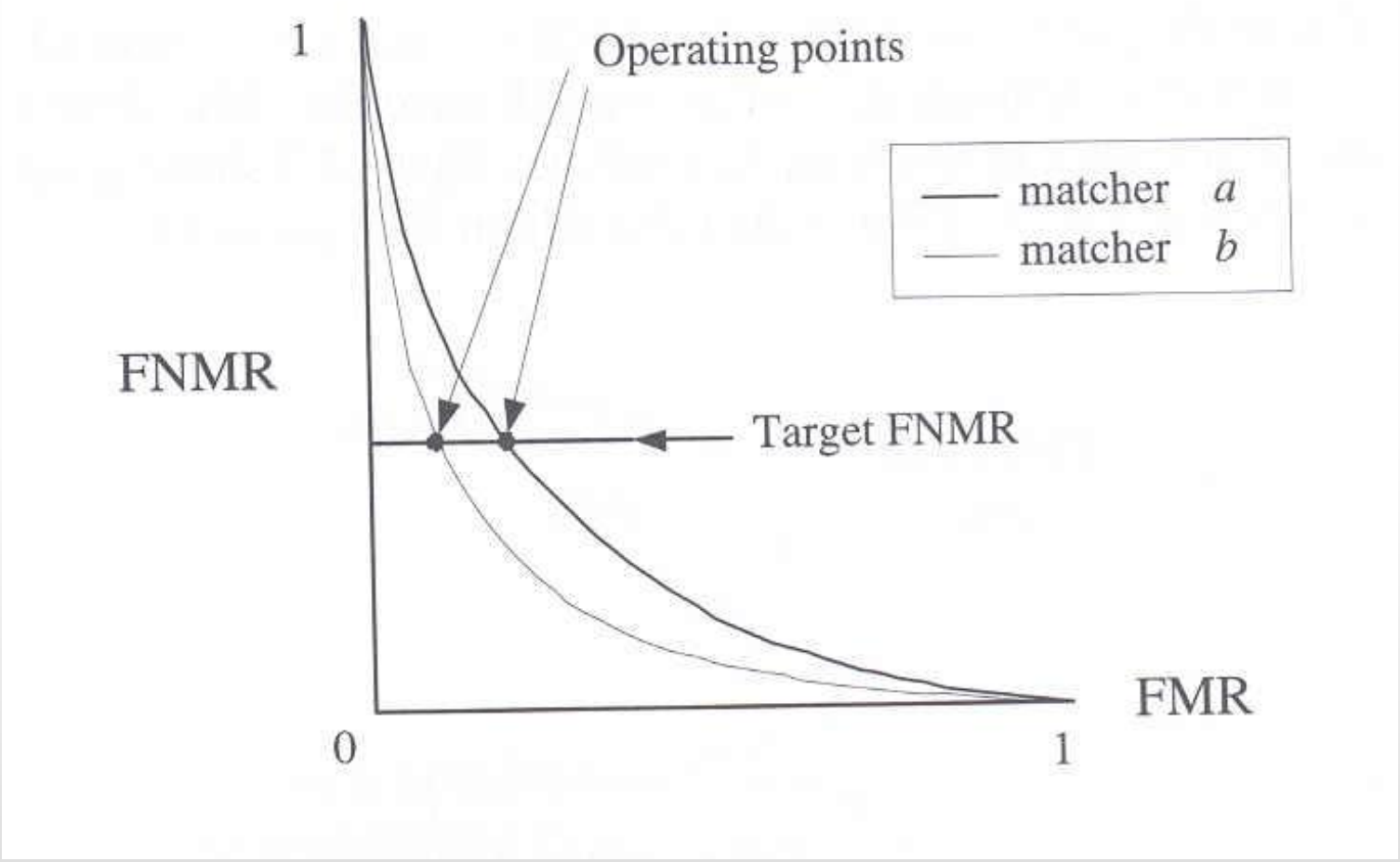
The Equal Error Rate



- ROC:

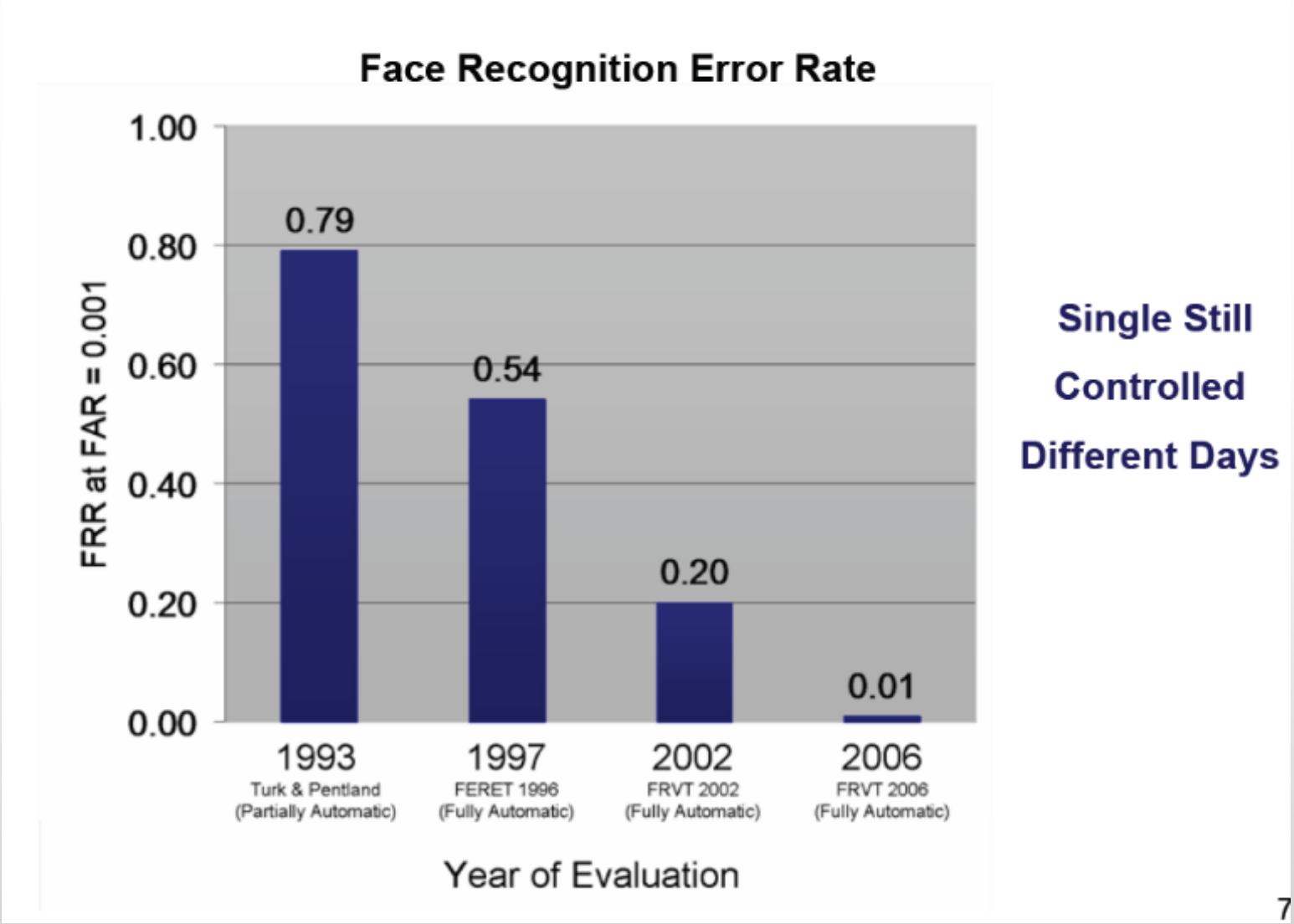


Using the ROC Curve



Matcher *b* is always better than matcher *a* since for every possible FNMR, its FMR is lower

Face recognition FRR & FAR



4 Overview of biometrics techniques

Main sorting

Biometrics can be sorted into two classes

1. Physiological
   Examples: face, fingerprint, hand geometry and iris recognition
2. Behavioral
   Examples: face, fingerprint, hand geometry and iris recognition

Biometric Identifiers

Common

- Fingerprint Recognition
- Face Recognition
- Iris Recognition
- Signature verification
- Hand Geometry
- Speaker Recognition

Others

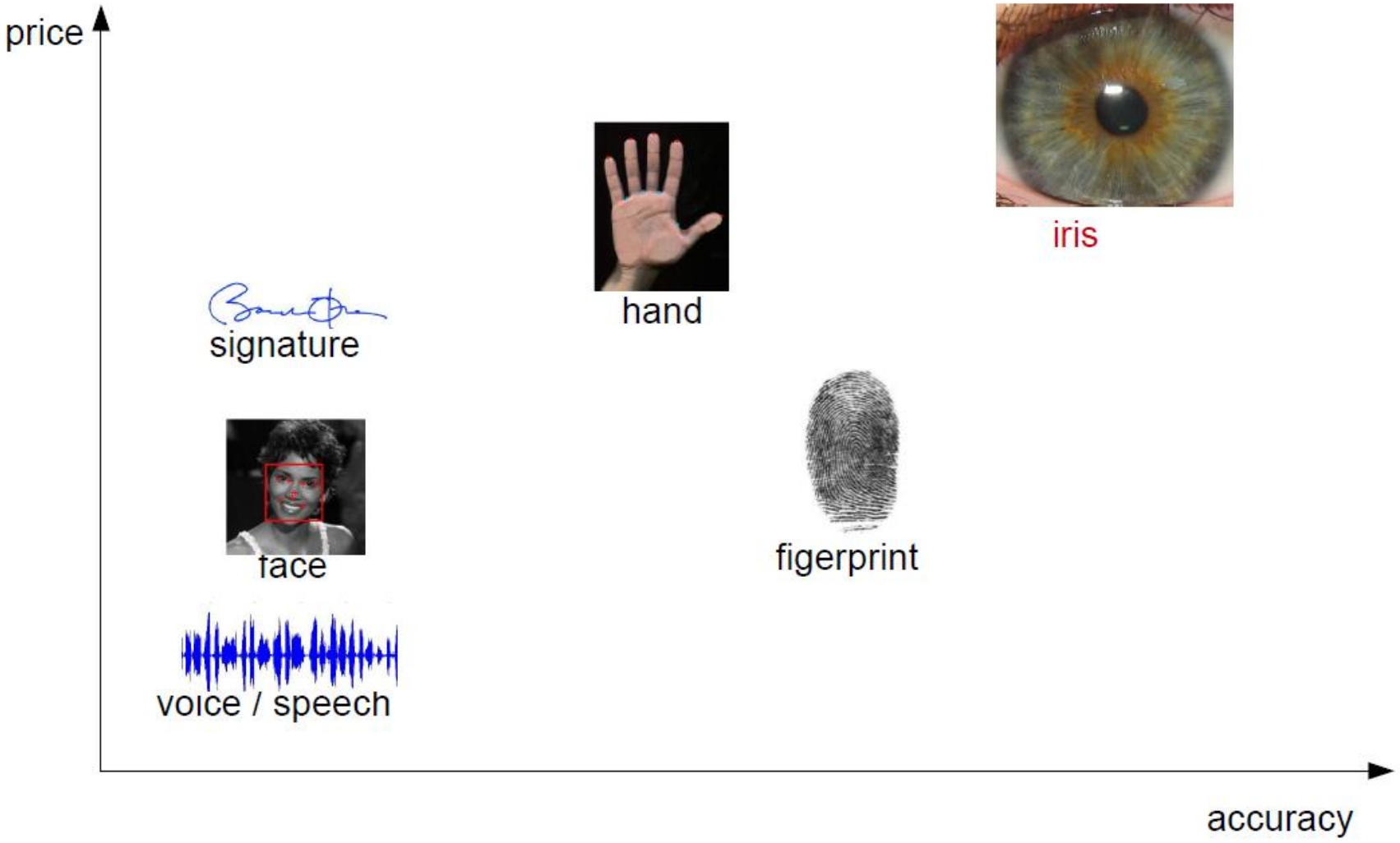
- DNA
- Vein recognition
- Retina recognition
- Thermograms
- Gait
- Keystroke
- Ear recognition
- Skin reflection
- Lip motion
- Body odor

More biometric identifiers

Vein Pattern
Sweat Pores
Fingernail Bed
Hand Grip
Brain Wave Pattern
Footprint and Foot Dynamics

•*See details in ***Chapter 7 Esoteric Biometrics*** of ***Biometrics*** by John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, New York : McGraw-Hill/Osborne, c2003

Price vs accuracy



Overview of biometric techniques

- Fingerprint recognition
- Face recognition
- Voice recognition
- Iris Recognition
- Dynamic signature

1. Fingerprint Recognition (D.Novak)

- An extremely useful biometrics technology since fingerprints have long been recognized as a primary and accurate identification method.

Acquisition devices

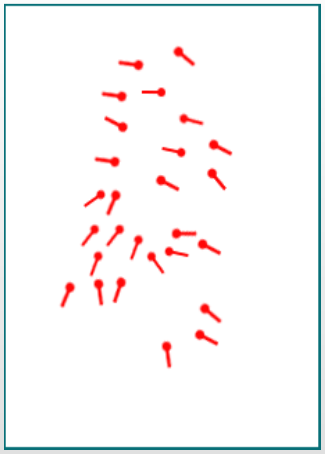
1. **Ink and paper**
2. **Ink-less sensing**
   - Optical methods (FTIR)
   - CMOS capacitance
   - Thermal sensing
   - Ultrasound sensing

Minutiae

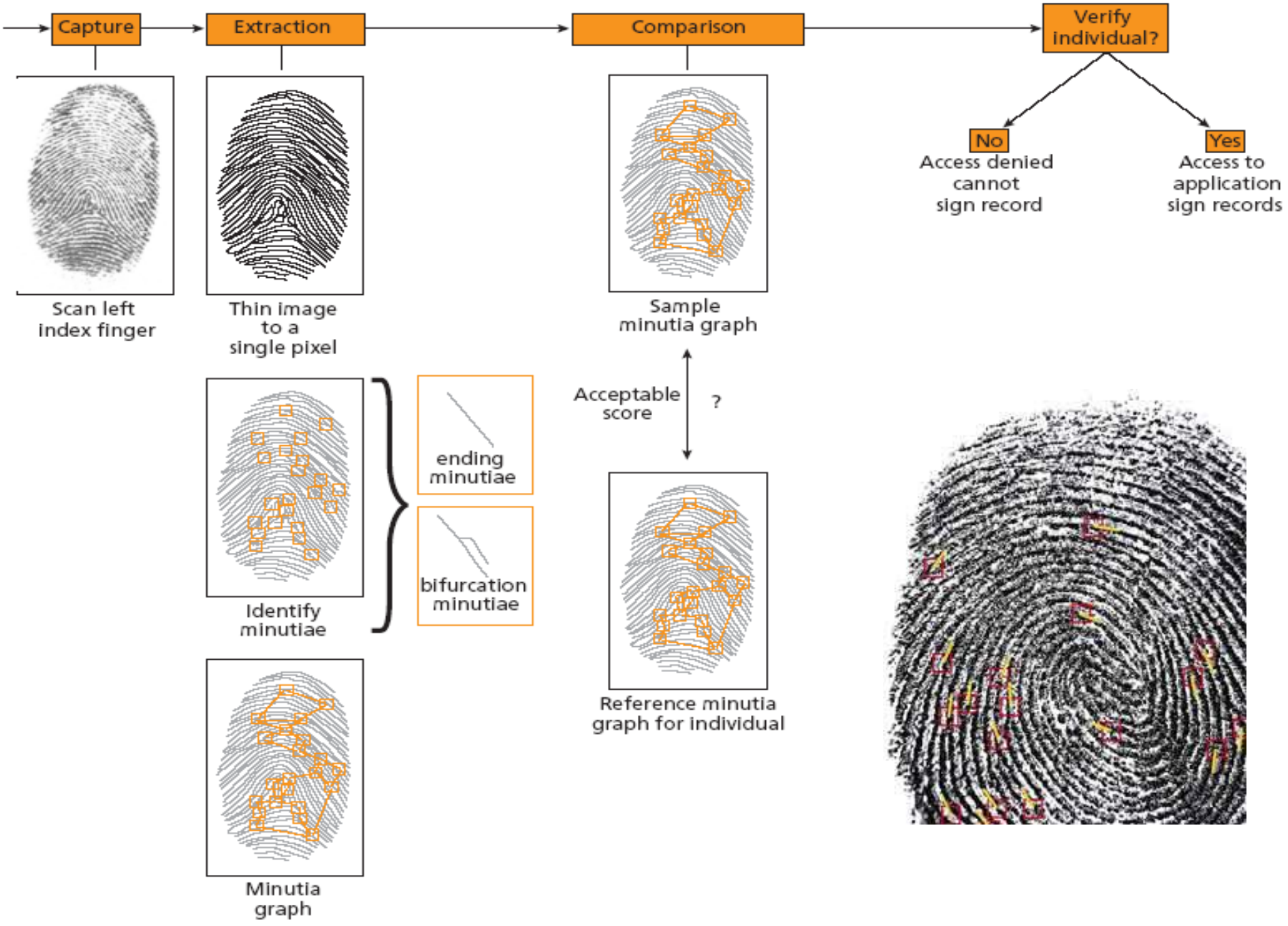
- Uses the **ridge endings** and **bifurcations** on a person‘s finger to plot points known as **Minutiae**
- The number and locations of the minutiae vary from finger to finger in any particular person, and from person to person for any particular finger

Finger Image

Finger Image + Minutiae



Minutiae


Capture
Extraction
Comparison
Verify individual?
No
Access denied cannot sign record
Yes
Access to application sign records
Scan left index finger
Thin image to a single pixel
Sample minutia graph
Acceptable score
?
ending minutiae
bifurcation minutiae
Identify minutiae
Minutia graph
Reference minutia graph for individual

Face recognition

2. Face Recognition (V. Franc)

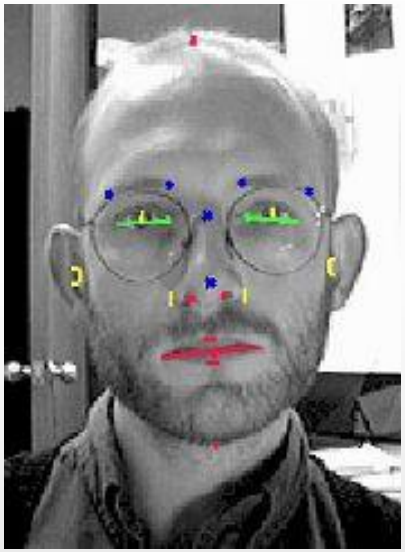
- Uses an image or series of images either from a camera c photograph to recognize a person.
- Principle: analysis of the unique shape, pattern and positioning of facial features.

- Face is the most common biometric characteristic used by humans
- Sensing at a distance
- Easy to capture from low-cost cameras
- Non-contact data acquisition (free from contagious disease)

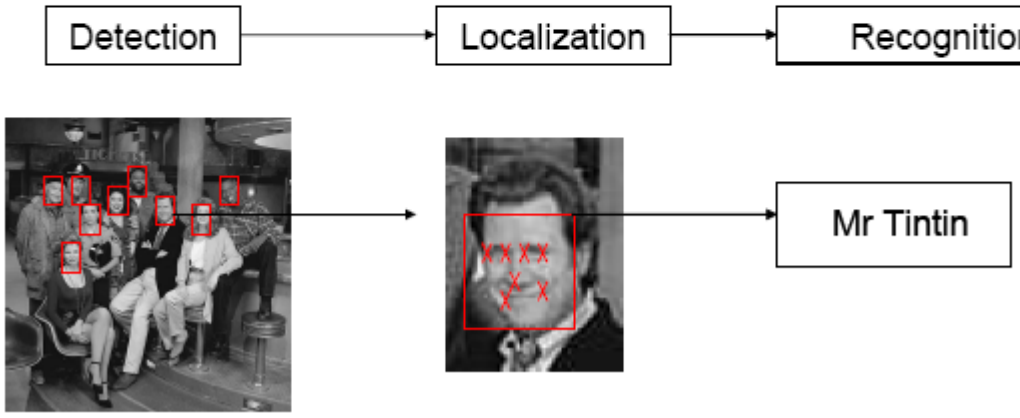
- Non-intrusive technique which people generally accept as biometric characteristic
- Overt (user aware) and covert (user unaware, e.g. ubiquitous surveillance cameras) applications
- Legacy databases (passport, visa and driver's license)

Details

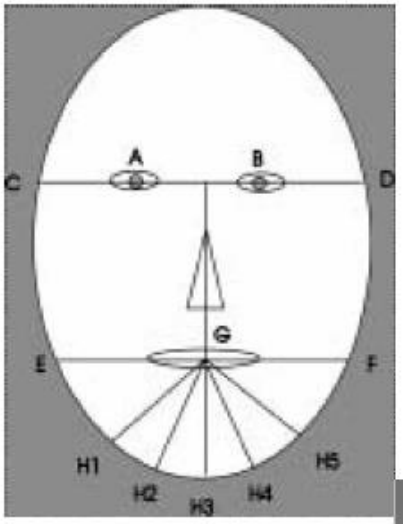
- Source of data: Single image, video sequence, 3D image and Near Infrared
- Models: weak models of the human face that model face shape in terms of facial texture

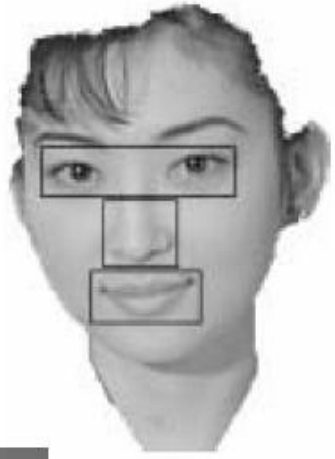


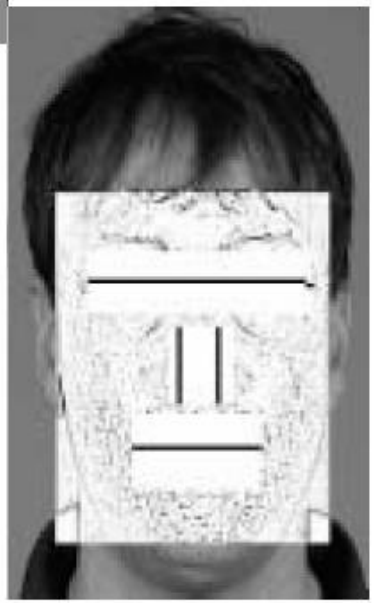
- **Face detection** – discriminating faces from all other possible images. This is 2-class classification task of assigning an image to the face class or the non-faces class.
- **Face localization** – finding precisely the position of one face, whose presence is already known in a single image

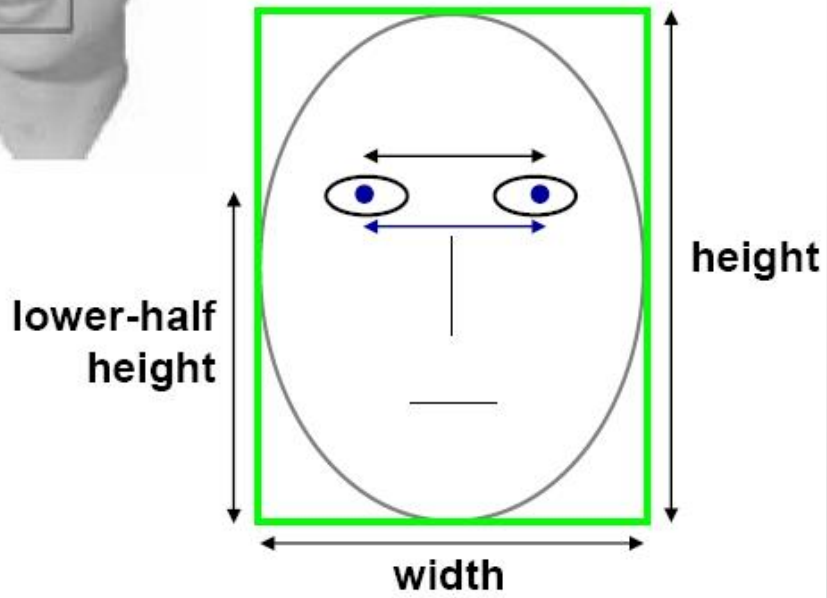


Feature based approach

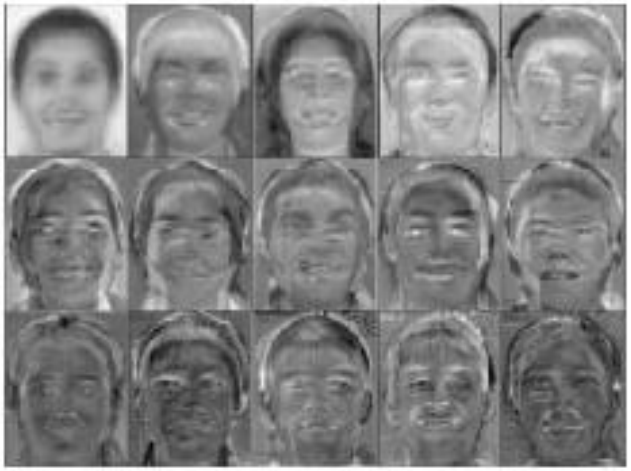








Example: Eigenfaces

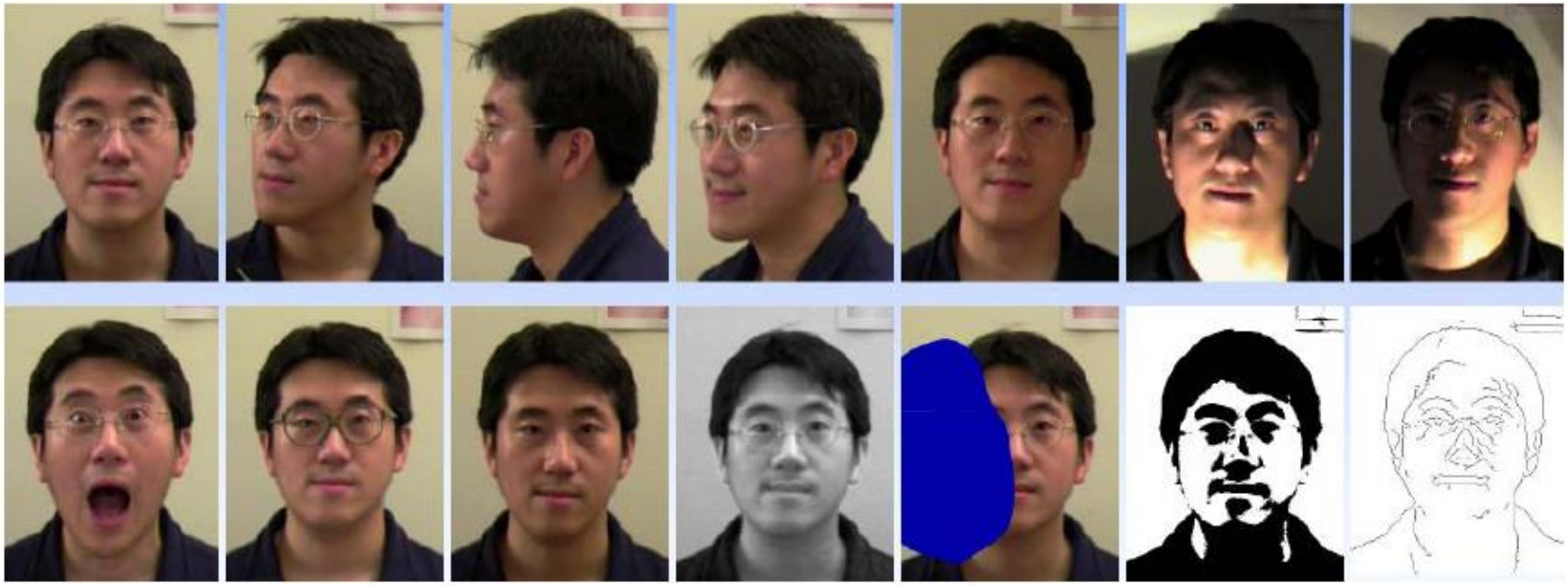


Perfect reconstruction with all eigenfaces

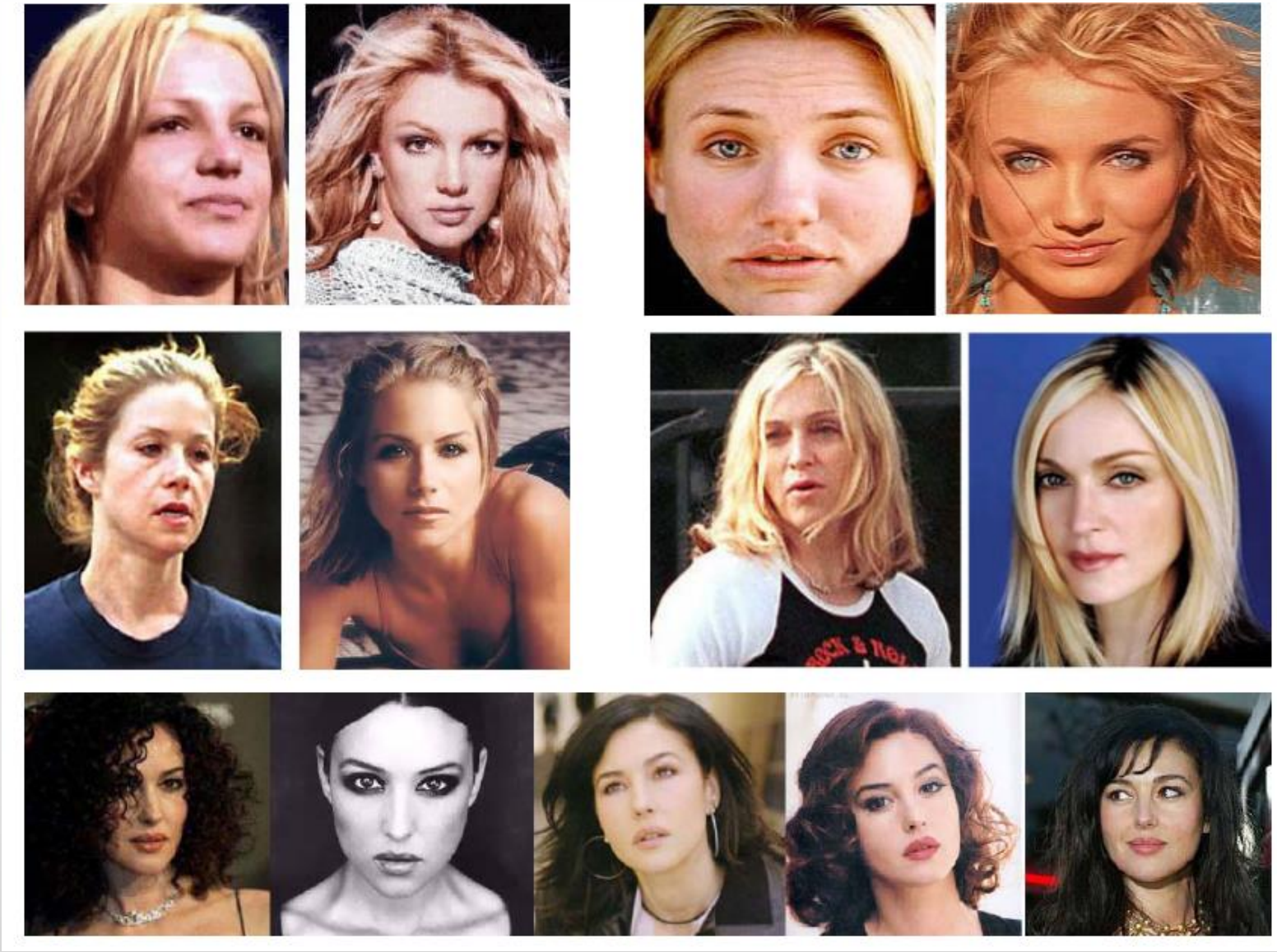
Reasonable reconstruction with just a few eigenfaces

Intra-class variability

- Faces with intra-subject variations in pose, illumination, expression, accessories, color, occlusions, and brightness



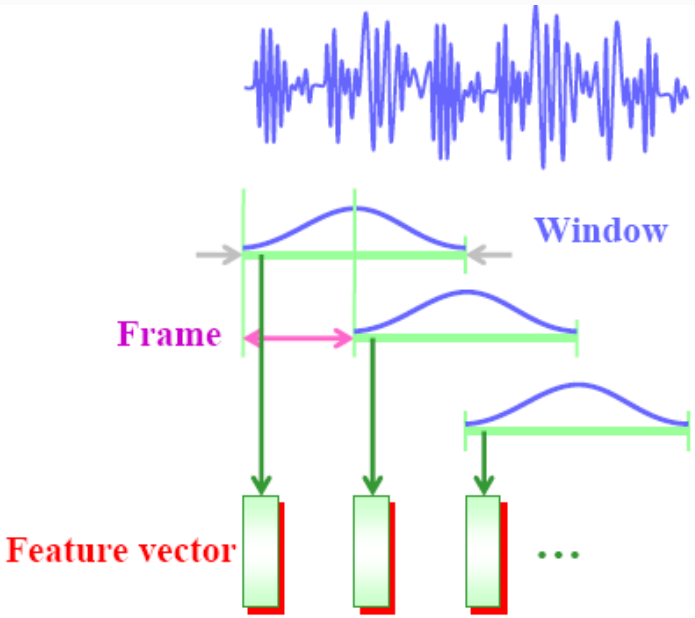
The power of make up

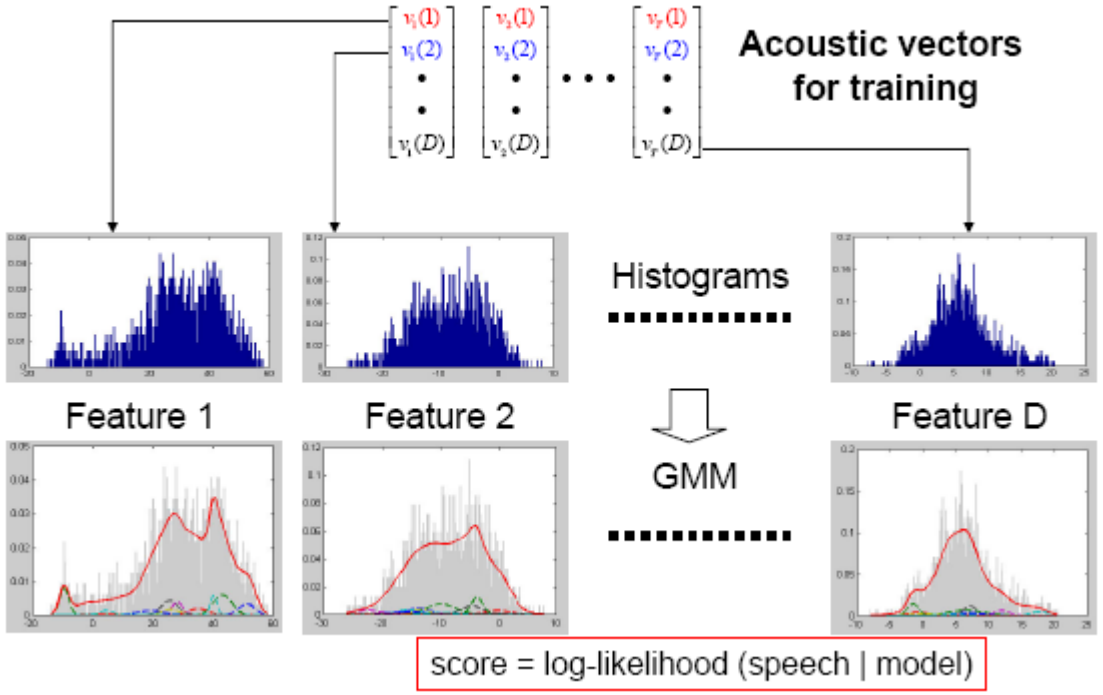


Voice recognition

3. Voice Recognition (P. Polak)

- Voice recognition is not the same as speech recognition, it is speaker recognition
- Considered both physiological and behavioral
- Popular and low-cost, but less accurate and sometimes lengthy enrollment





Features

- Advantages
  - Less requirements for users
    - do not have to go through a separate process for verification
  - Very little hardware is required,
    - ideally suited to telephone-based system for a remote identification
  - Zero client-side cost, no special reader needs to be installed
- Disadvantages
  - Acoustic features :
    1. Misspoken or misread phrases;
    2. The human voice's tremendous variability, due to colds, aging, and simple tiredness
  - Can be captured surreptitiously by a third party and replayed

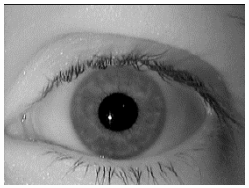
Iris recognition

4. Iris recognition (E. Bakstein)

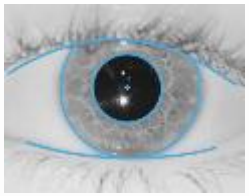
- Analysis of the iris of the eye, which is the **colored ring** of tissue that surrounds the pupil of the eye.
- Widely regarded as the safest, accurate biometrics technology and capable of performing 1-to-many matches at extraordinarily high speeds, without sacrificing accuracy.

- Not to be confused with: retinal scans!

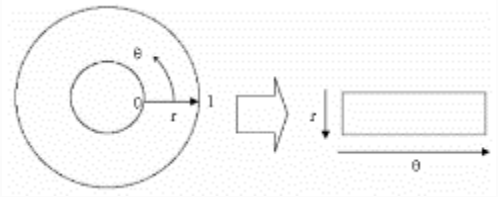
Iris recognition process



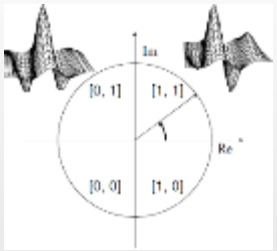
iris image



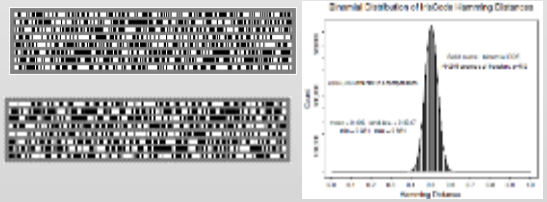
iris region segmentation



unwrapping



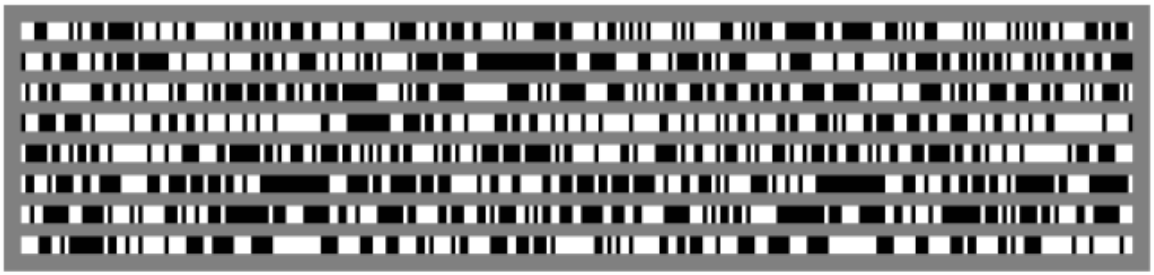
feature extraction & encoding



iris code comparison (database)

Result

Iris code



Iris Code

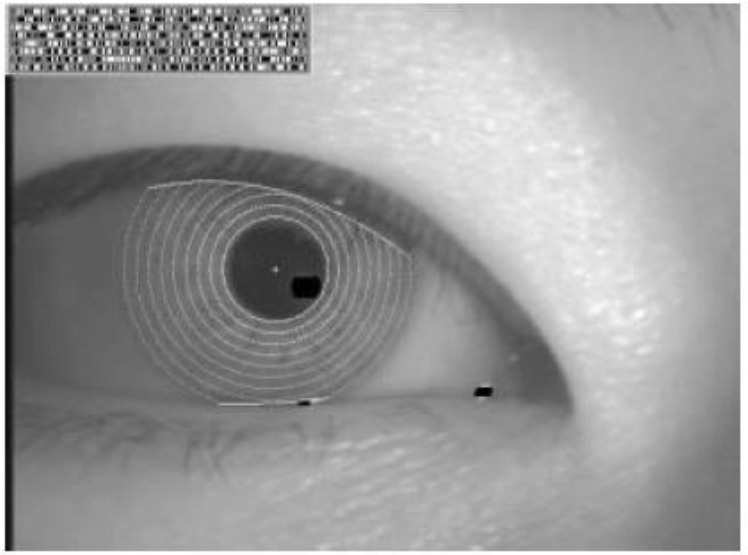
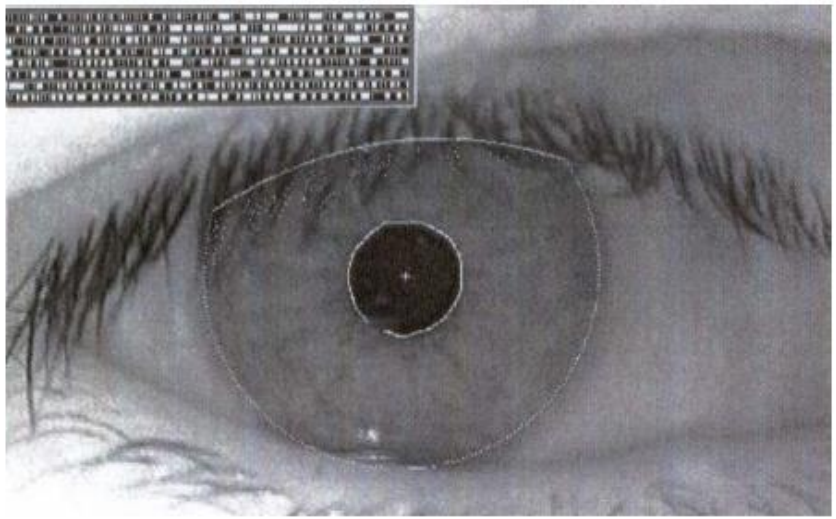
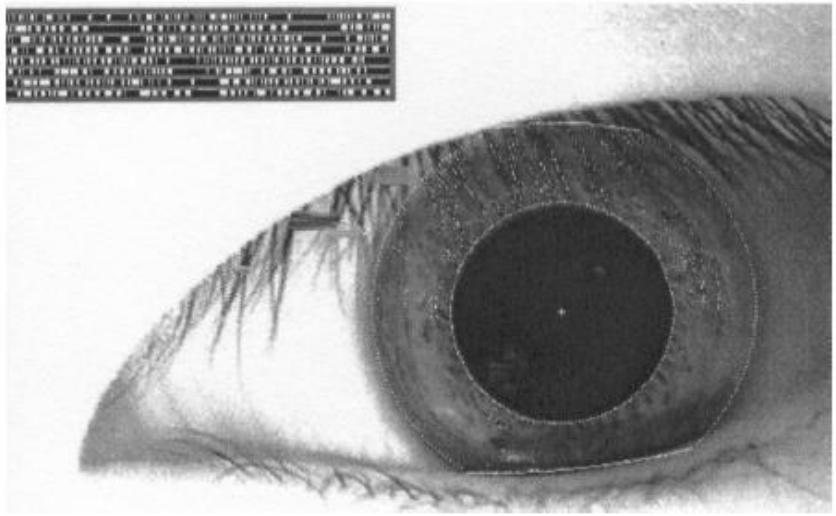
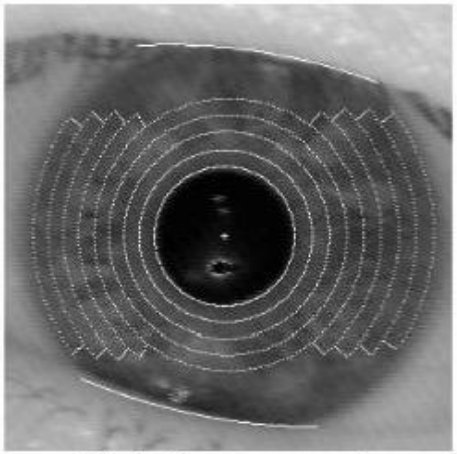


Image size is 64 x 256 bytes and the iris code is 8 x 32 bytes

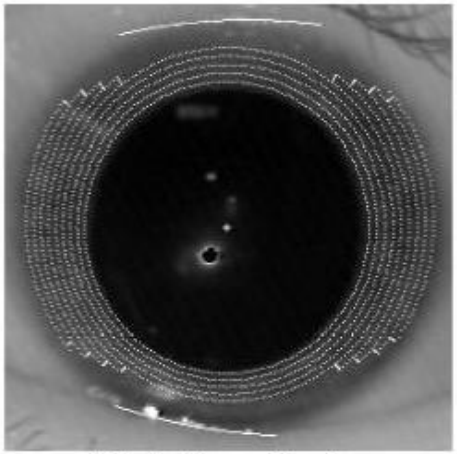
Iris mapping







Dilatation normale



Dilatation élevée

- The iris mapping has to be invariant to shift, distance, magnification, and pupillary dilation

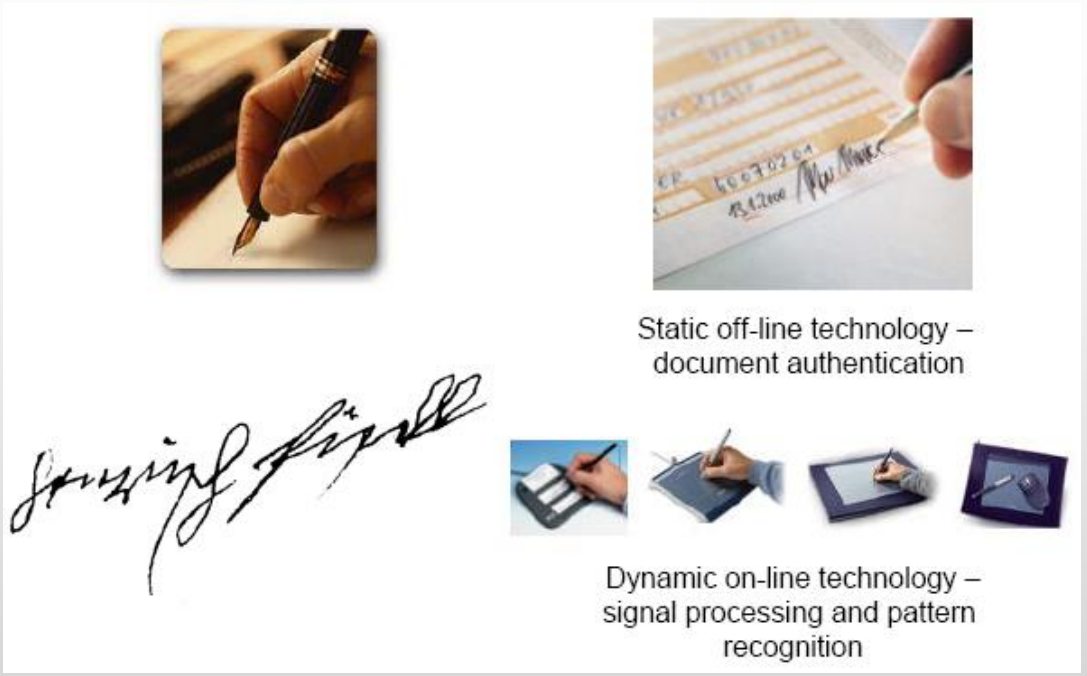
Dynamic signature

5. Signature Verification (J. Schneider / P.Vostatek)

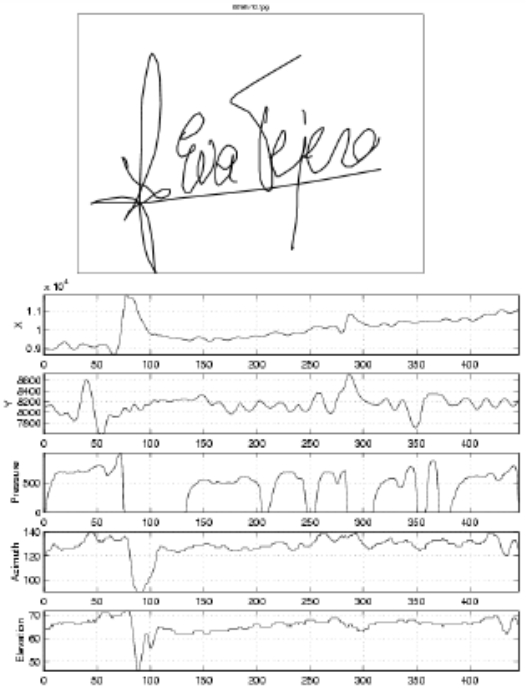
- Static/Off-line: the conventional way
- Dynamic/On-line: using electronically instrumented device

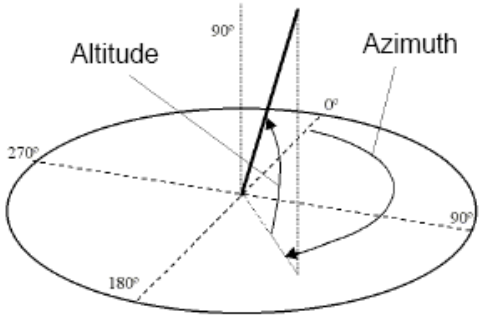
Principle: the **movement of the pen** during the signing process rather than the static image of the signature.

Many aspects of the signature in motion can be studied, such as **pen pressure**, the **sound the pen makes**

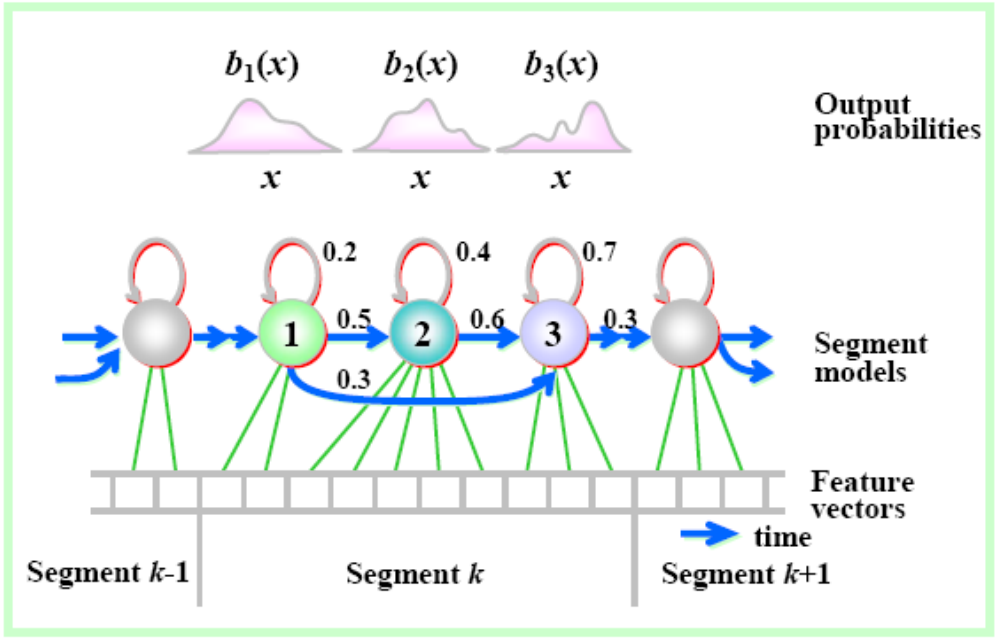


Dynamic signature

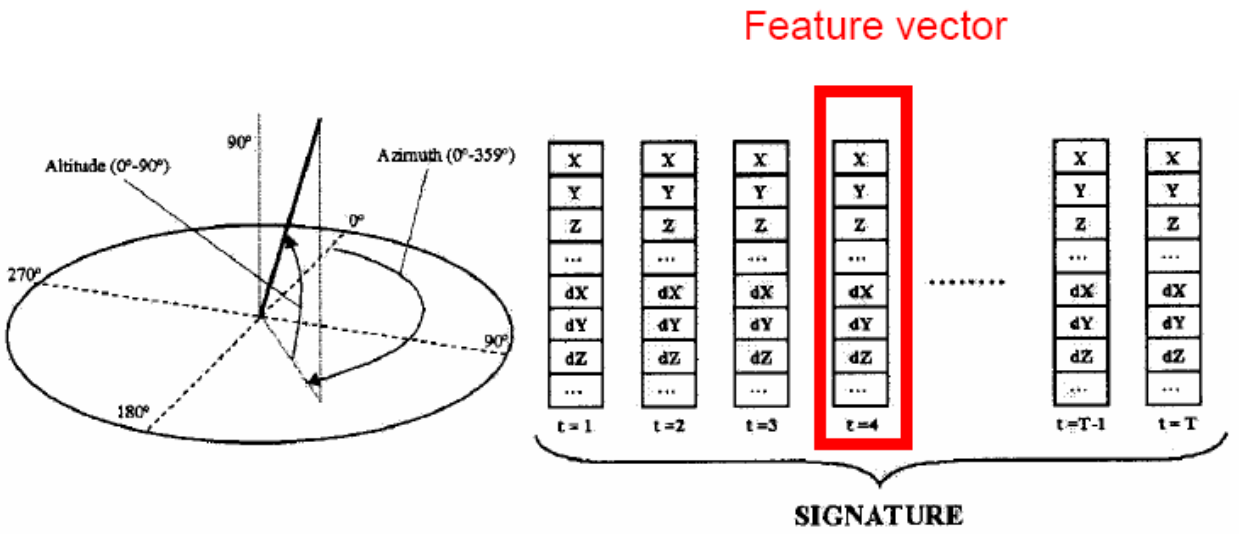




Features:
1. coordinate X
2. coordinate Y
3. pressure
4. pen azimuth (0° - 359°)
5. pen altitude (0° - 90°)



Dynamic signature



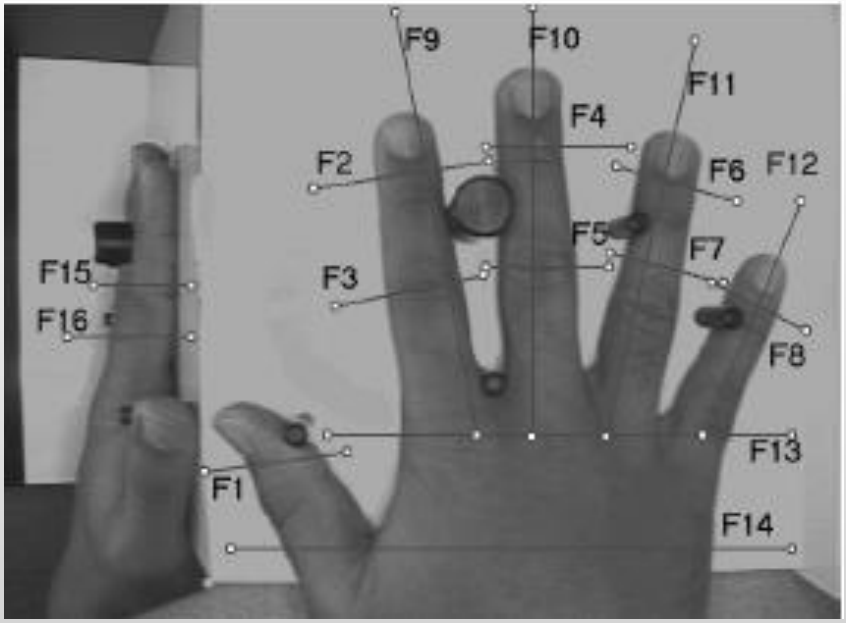
Acquisition:

-acquisition area: 127·106 mm
-pressure levels: 1024
-resolution: 2540 lines/inch (100 lines/mm)
-precision: +/- 0.25 mm
-detection height: 10 mm
-sampling frequency: 100 pps (points per s)

Hand geometry

5. Hand geometry

- Two main forms:
  - Full hand readers
  - Two finger readers
- How it works
  - A **camera captures an image of the hand**, with the help of a mirror to get also the edge. **The silhouette of the hand is extracted**, and some **geometric characteristics** stored.



$$\sum_{j=1}^{d} | y_j - f_j | < \epsilon_a, \quad (1)$$

$$\sum_{j=1}^{d} \frac{| y_j - f_j |}{\sigma_j} < \epsilon_{wa}, \quad (2)$$

$$\sqrt{\sum_{j=1}^{d} (y_j - f_j)^2} < \epsilon_e, and \quad (3)$$

$$\sqrt{\sum_{j=1}^{d} \frac{(y_j - f_j)^2}{\sigma_j^2}} < \epsilon_{we}, \quad (4)$$

where σ_j^2 is the feature variance of the jth feature and ϵ_a, ϵ_{wa}, ϵ_e, and ϵ_{we} are threshold values for each respective distance metric.

Popular in the past

BenGurion Airport – Tel-Aviv,

Hand Geometry

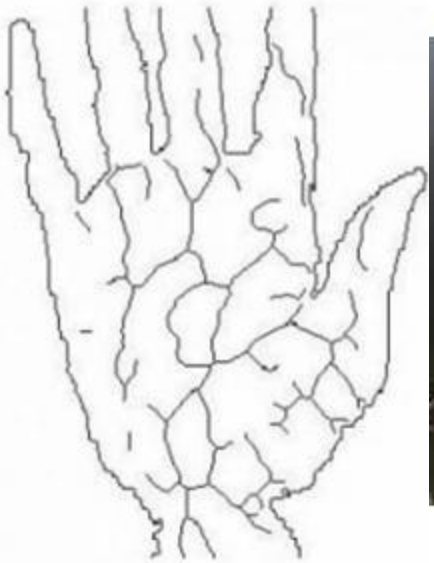
JFK International Airport

1993-2002 INPASS system

Replaced later by Global Entry (fingerprint)

Not to be confused with: vein recognition

- Identification of vein pattern, commonly on the palm.



Other biometric modalities

Experimental or not so common

Biometrics in Early Stages

DNA	Retina recognition	Thermograms
Gait	Keystroke	Ear recognition
Skin reflection	Lip motion	Body odor

I. DNA profiling

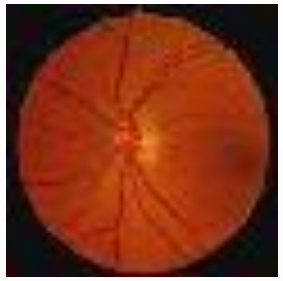
- also *DNA fingerprinting*
- The “ultimate identifier”
- Identify information from every cell in the body in a digital form
- Not yet fully automated, not fast and expensive
- Theoretical limitation: Identical twins have the same DNA
- Privacy issue – DNA contains information about race, paternity, and medical conditions for certain disease
- Only a small portion of DNA sequenced
- Multiple methods exist, see https://en.wikipedia.org/wiki/DNA_profiling

Comparison Chart: DNA

DNA	Conventional Biometrics
Requires an actual physical sample	Uses an impression, image, or recording
Not done in real-time; not all stages of comparison are automated	Done in real-time; “lights-out” automated process
Does a comparison of actual samples	Uses templates or feature extraction

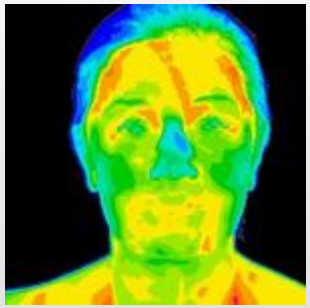
II. Retina recognition

- The pattern of blood vessels that emanate from the optic nerve and disperse throughout the retina depends on individuals and never changes.
- **No two retinas are the same, even in identical twins.**
- Commercial products: Retinal Technologies



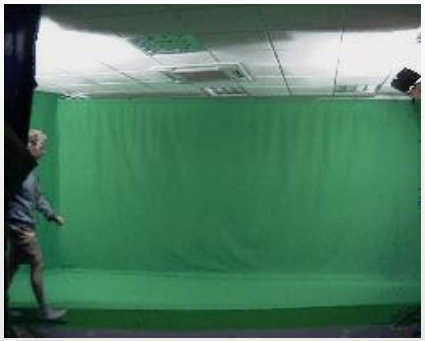
III. Thermograms

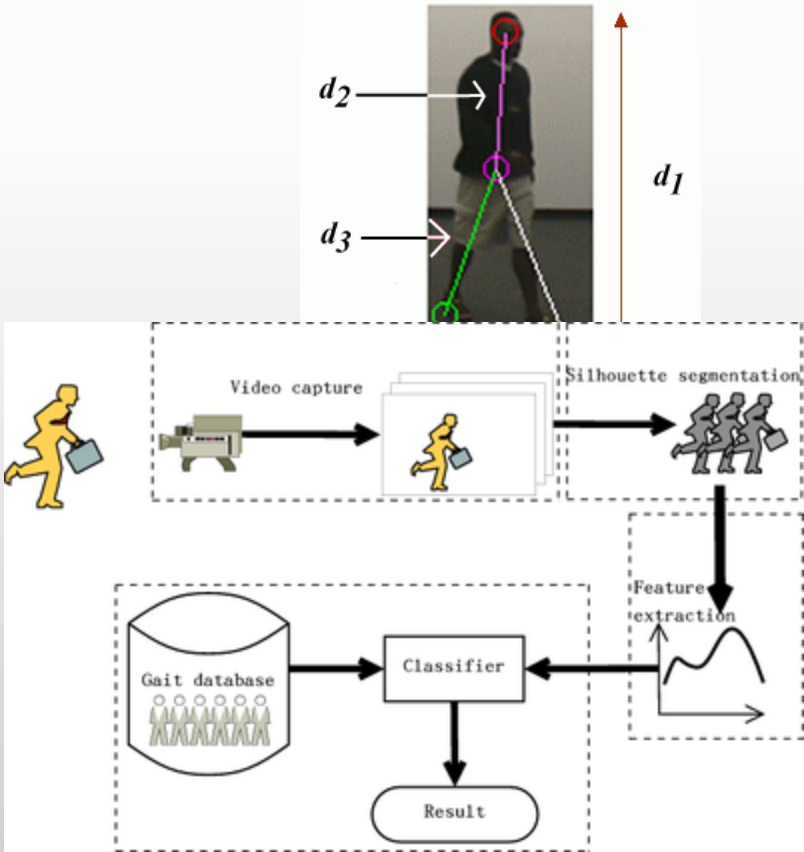
- Thermograms requires an infrared camera to detect the heat patterns of parts of the body that are unique to every human being (such as the face)
- Normally expensive because of the sensors
- Useful paper: Illumination Invariant Face Recognition Using Thermal Infrared Imagery (Solikinski & als)



IV. Gait

- The final objective: to recognize persons using sta cameras in any conditions.
- Gait recognition is particularly studied as it may e identification at distance.
- Gait video

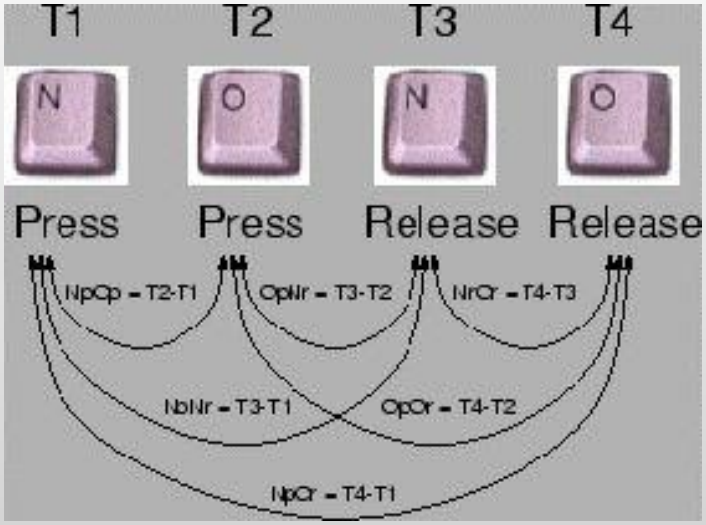




Češi vyhráli policejní olympiádu

V. Keystroke

- The **rhythms** with which one **types at a keyboard** are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics
- 100% software-based, requiring no sensor more sophisticated than a home computer
- VIDEO



VI. Ear recognition

- Ear geometry recognition uses the shape of the ear to perform identification
- Suggestions have been made that the shapes and characteristics of the human ear are widely different
- **An infrared image can be used to eliminate hair**
- Might be recognized at a distance

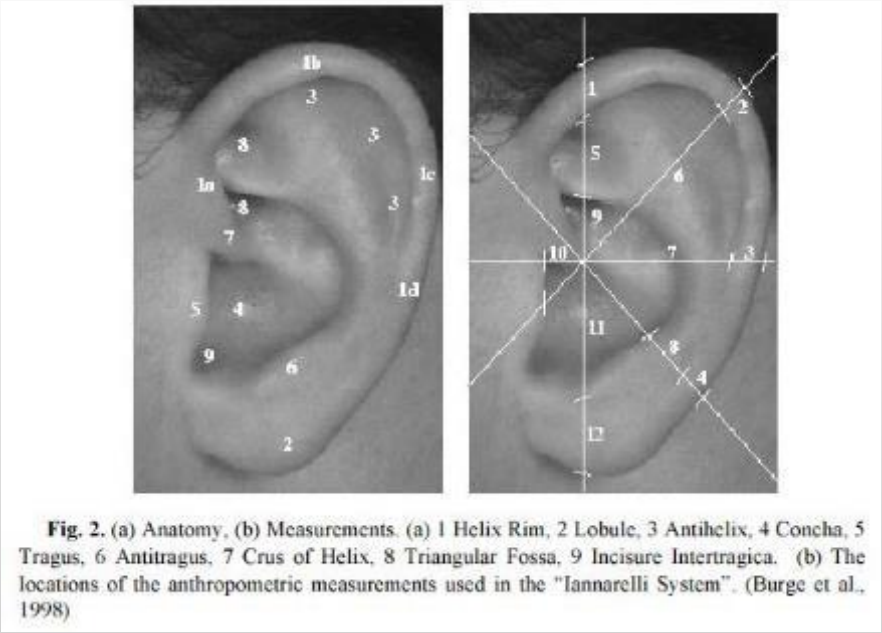
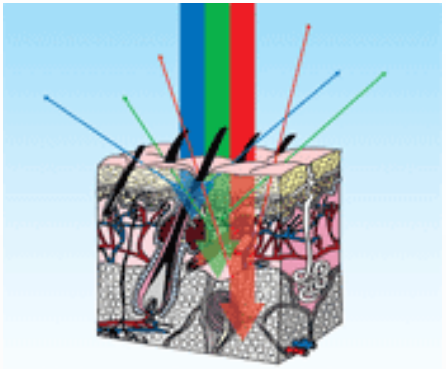


Fig. 2. (a) Anatomy, (b) Measurements. (a) 1 Helix Rim, 2 Lobule, 3 Antihelix, 4 Concha, 5 Tragus, 6 Antitragus, 7 Crus of Helix, 8 Triangular Fossa, 9 Incisure Intertragica. (b) The locations of the anthropometric measurements used in the "Iannarelli System". (Burge et al., 1998)

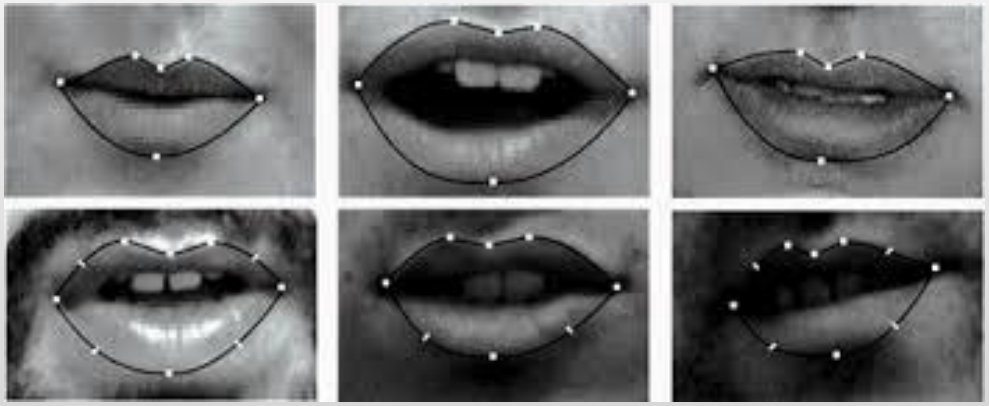
VII. Skin reflection

- Fingerprint-based
- Lumidigm Inc. has established that the absorption spectrum of the skin depends on the individuals.
- In a range of wavelengths over 6mm patch, several LEDs send light into the skin, and photodiodes read the scattered light, which is analyzed to perform the authentication.



VIII. Lip motion

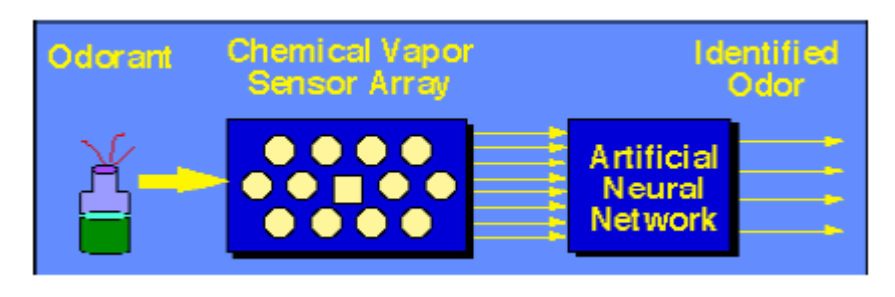
- Compares the characteristic lip motions of people while they speak.
- **Helps identification associated with speaker recognition**.
- Different imaging conditions: Infrared (high security & cost) and Near Infrared (cheap, normally used for active sensing)



IX. Body odor

- People with differing immunity genes produce different body odors
- Electronic/artificial noses: developed as a system for the automated detection and classification of odors, vapors, gases.

Prometheus (Alpha Mos) , an example of electronic nose



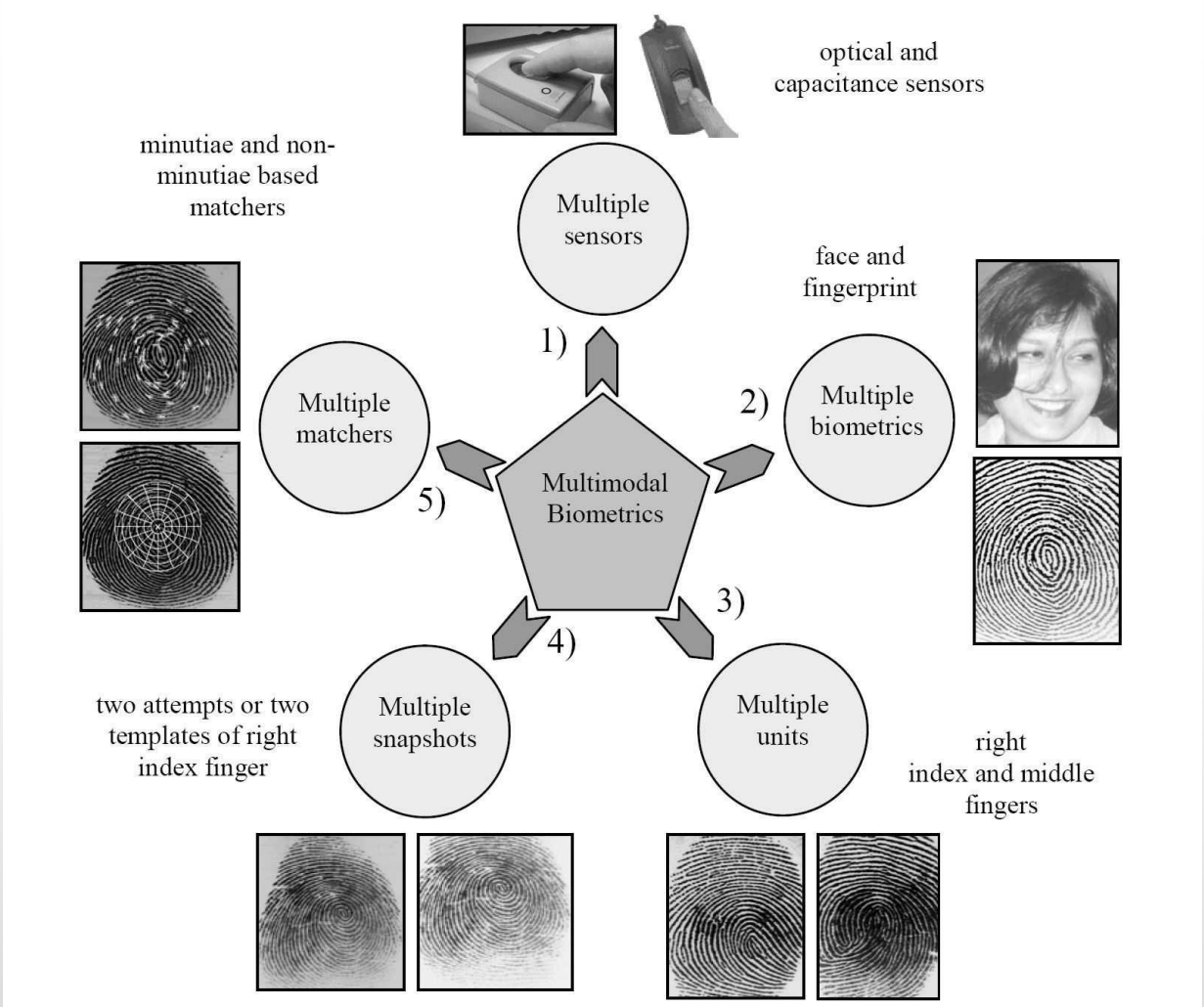
Schematic Diagram of Artificial nose

Artificial noses are not yet sophisticated enough to do all the job

X. Heartbeats

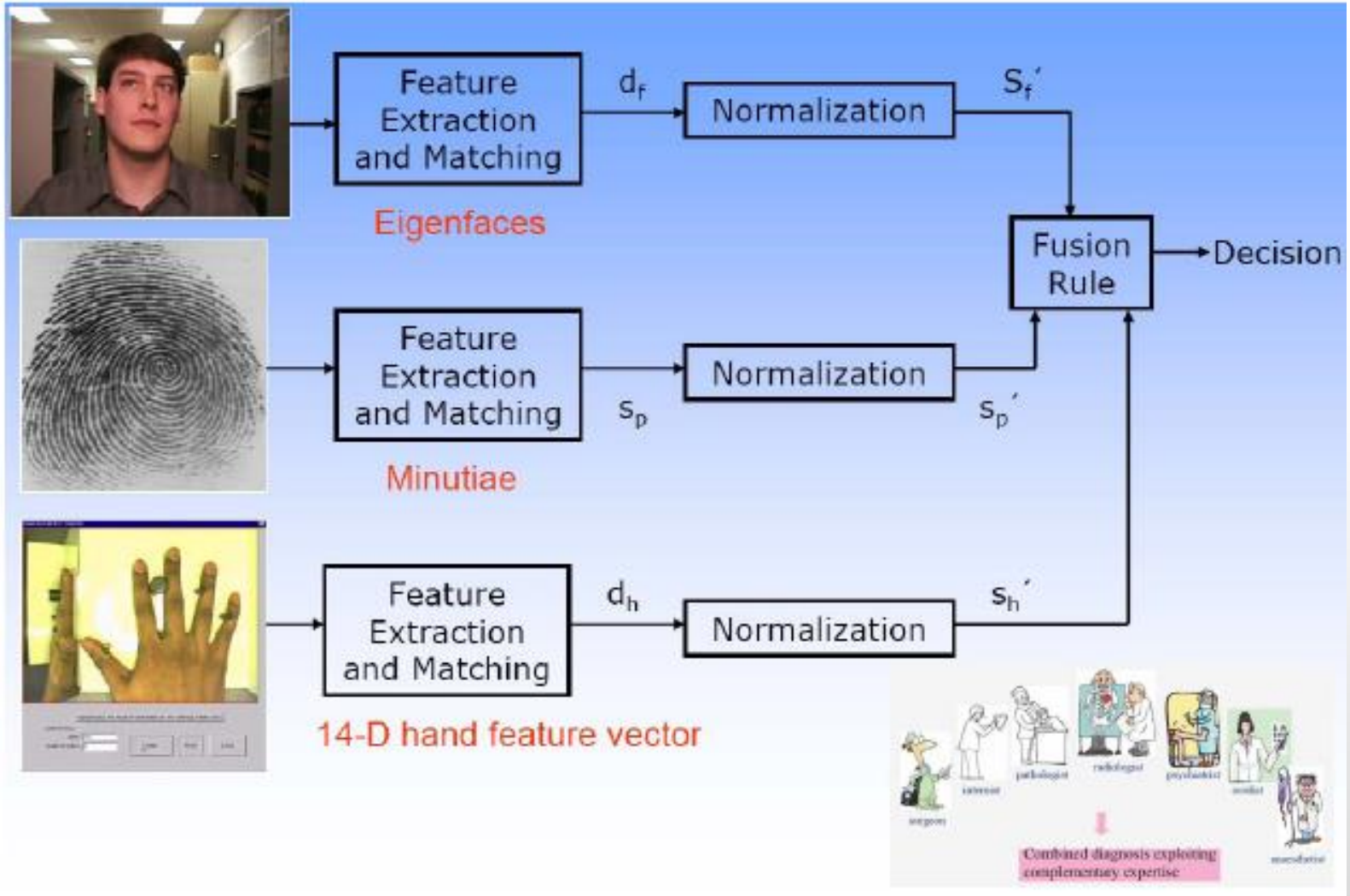
- Based on differing hearbeat patterns in each person
- Bionym Nimy wristband – commercially available (preorder, as of 09/2013)
- Security?

Multimodal Biometrics



http://www.cse.msu.edu/~rossarun/pubs/RossMultimodalOverview_EUSIPCO04.pdf

Fusion after normalization



Comparision of Biometric Technologies

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very High	Very High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

Thank you!