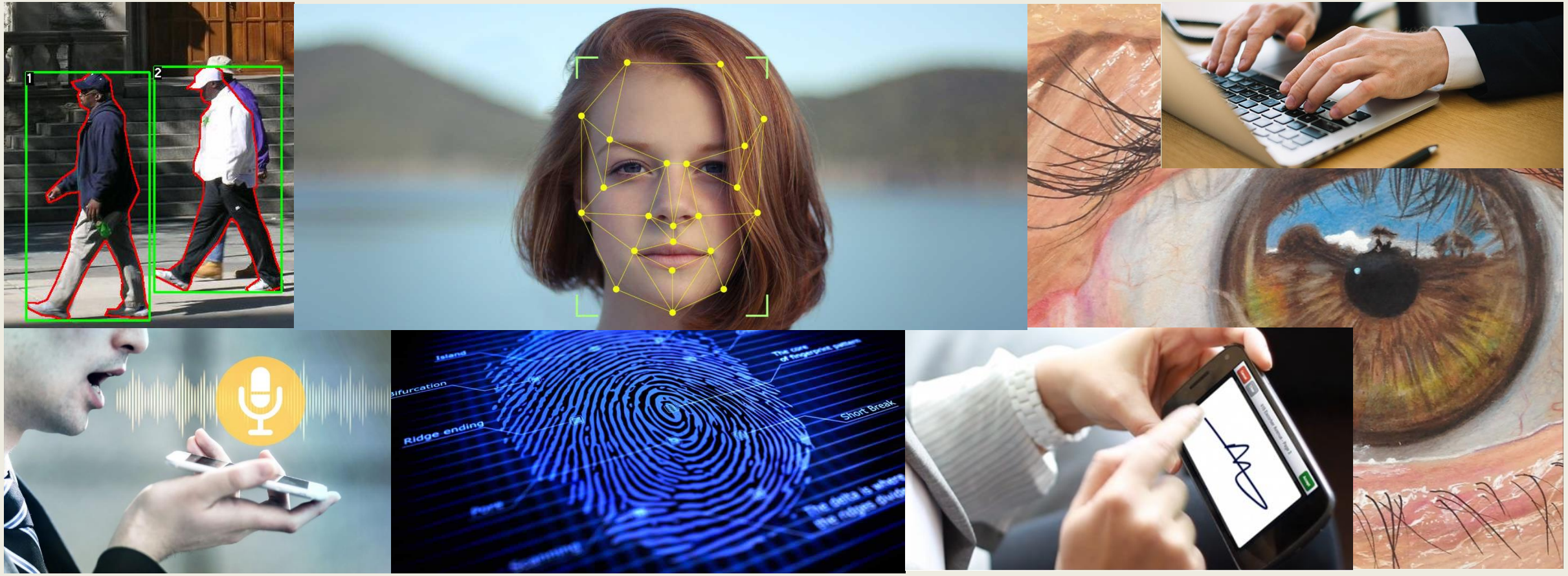
Introduction to Biometrics



Ruben Tolosana
ruben.tolosana@uam.es

BiDA Lab
Biometrics & Data Pattern Analytics Lab

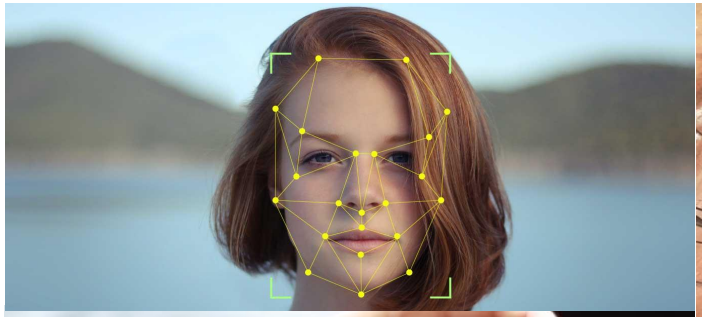
UAM
Universidad Autónoma de Madrid

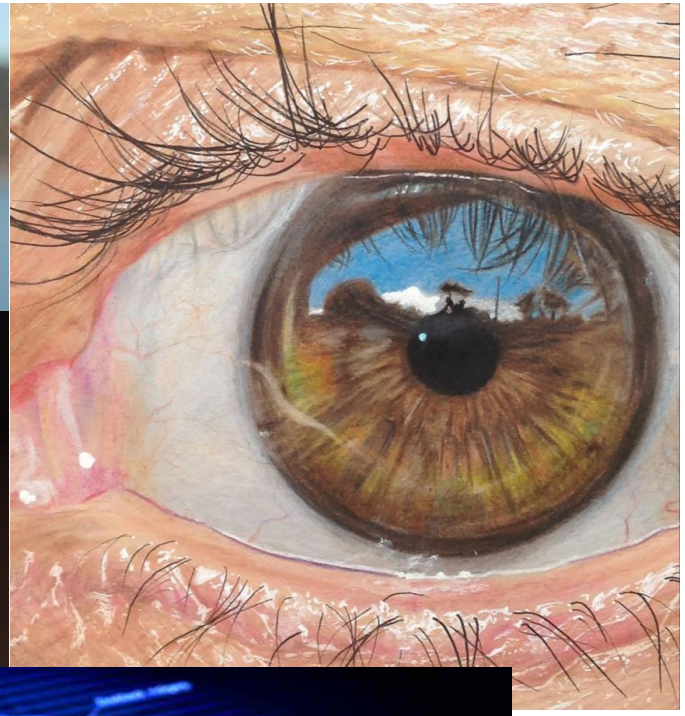
Outline

- Our Biometrics Course
- Biometrics and Data Pattern Analytics – BiDA Lab
- What is Biometric Recognition?
- Biometric Traits
- Biometric Authentication
- Biometric Modalities
- Applications

Biometric Course

- Introduction + Evaluation Metrics.
- Face Recognition.
- Fingerprint Recognition.
- Iris Recognition.
- Signature Recognition.
- Practical work!





Biometrics and Data Pattern Analytics BiDA Lab - UAM

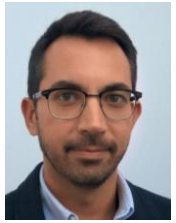
Senior Staff:

- Full Professor
- **Vice-Rector Innov. UAM**
- **IEEE Fellow**
- **IAPR Fellow**

Javier ORTEGA-GARCIA

- Associate Professor
- **Best Researcher (STEM) < 40 (Community of Madrid) 2015**
- **(IAPR) *Young Biometrics Investigator Award* 2017**

Julian FIERREZ



- Associate Professor
- *PhD by Swansea Univ.*
- Juan de la Cierva Fellow
- Various research stays abroad

Ruben VERA-RODRIGUEZ

- Associate Professor
- *Security Forum Award* 2013
- Various research stays (incl. Harvard)

Aythami MORALES

Postdoc Researcher:

Ruben Tolosana

Engineers: (PhD Candidates)

J. Hernandez

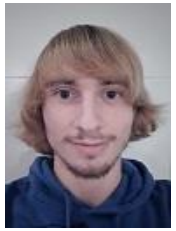
A. Acien

Ignacio Serna

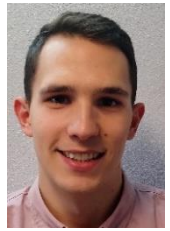
A. Peña

R. Daza

IT Support:

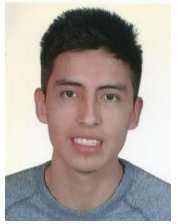


I. Bartolome



S. Romero

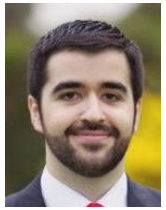
J.C. Ruiz



S. Rengifo

x4 PhD Marie Curie (PRIMA and TRESPASS ITNs)

Javier Galbally
JCR European Commision



Marcos Martinez
IT Head MINETAD

Fernando Alonso
Halmstad Univ.

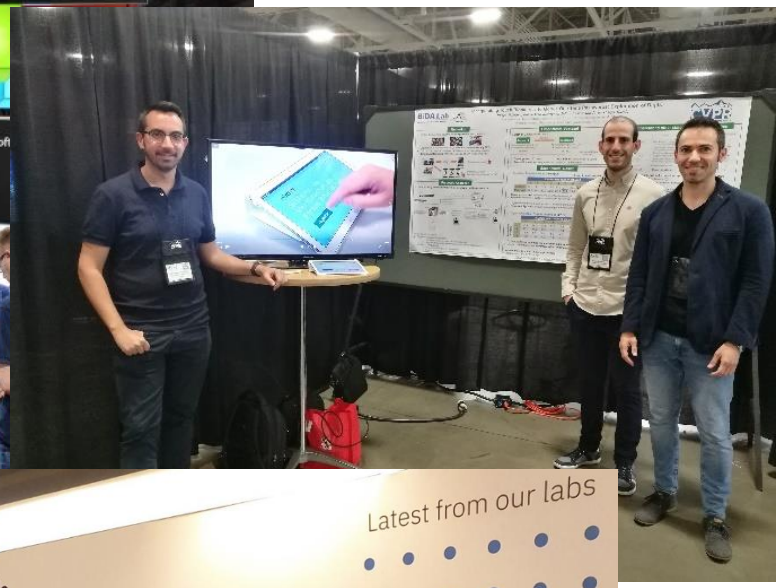
Marta Gomez-Barrero
Darmstadt Univ.

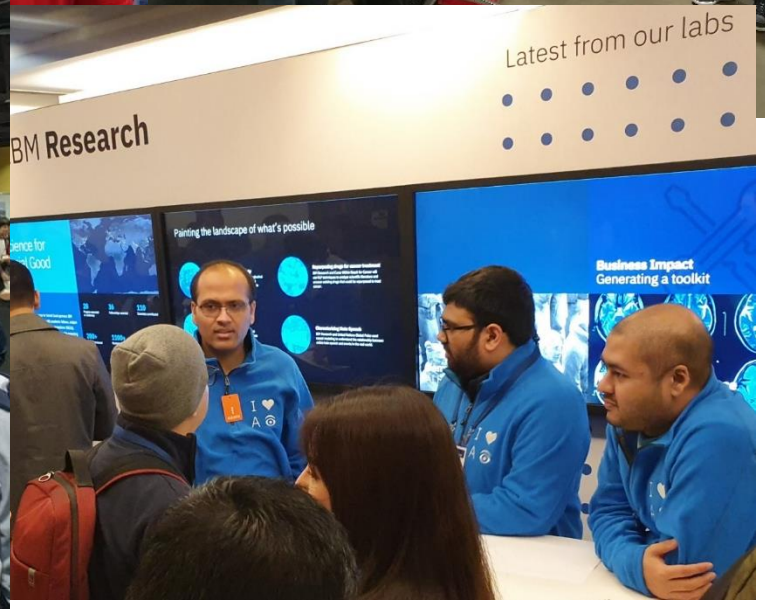
Pedro Tome
IT Head Evo Bank

Ester G.-Sosa
Nokia Labs. Madrid

Recent PhD Graduates: now Researchers at other relevant institutions

Biometrics and Data Pattern Analytics BiDA Lab - UAM





AAAI-20, New York

CVPR
JUNE 14-19 2020

ECCV'20
ONLINE
23-28 AUGUST 2020

ACM mm

ICPR 2020

BiDALab-UAM ©

What is Biometric Recognition?

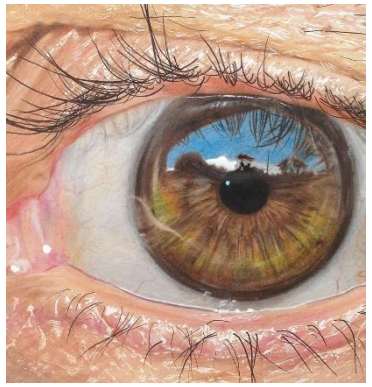
Definition:

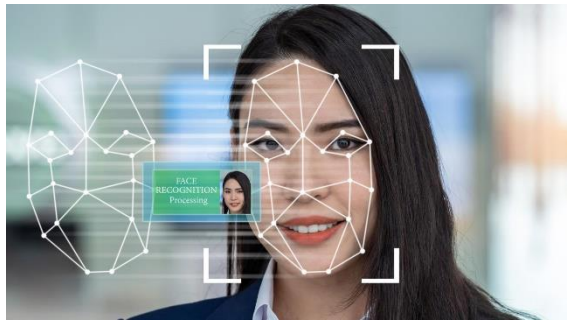
- Biometric recognition is the science of establishing the identity of a person based on physical or behavioral attributes associated with an individual.

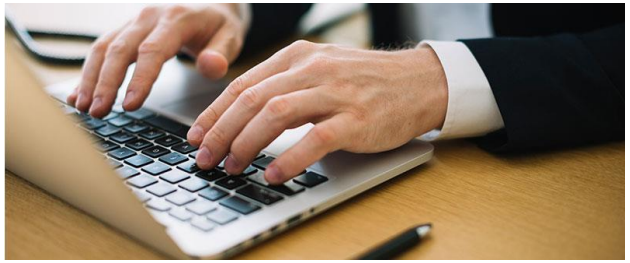
The term "biometrics" is derived from the Greek words bio (life) and metric (measure).

Biometric Traits

- Face
- Fingerprint
- Speech
- Signature
- Iris
- Gait
- Palm Vein
- ....
- Keystroke
- Ear







Biometrics Traits

Physiological – Morphological Traits

- Fingerprints
- Face
- Infrared facial thermography
- Iris
- Ear
- Retinal scan
- Hand & finger geometry
- Blood vessel imaging
- Body profile & body parts

Physiological – Biological Traits

- DNA
- EKG, EEG
- Odor

Behavioral Traits

- Speech – Voice
- Signature
- Handwriting
- Gait
- Keystroke dynamics
- Mouse dynamics
- Web-based biometrics

• A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

History of Biometrics

- Handprints may "have (...) acted as a nonforgeable signature" of its originator at least 31,000 years old.
- Evidence suggests fingerprints were used as a personal mark around 500 B.C.
- Early Chinese merchants used fingerprints to settle business transactions.
- Chinese used fingerprints and footprints to differentiate people.
- Early Egyptian uses:
  - Traders were identified by their physical descriptors.
  - Differentiate between trusted traders of known reputation and previous successful transactions, and those new to the market.

Chauvet cave (France)

History of Biometrics

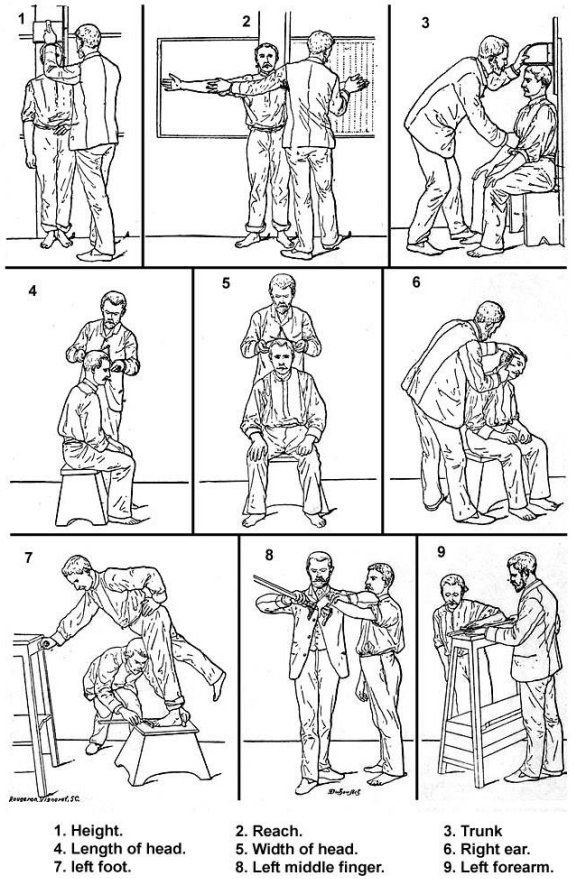
- 1858: First systematic capture of hand images for ID purposes is recorded
- 1870: Bertillon develops anthropometrics to identify individuals
- 1892: Galton develops a classification system for fingerprints
- 1896: Henry develops a fingerprint classification system
- 1936: Concept of using the iris pattern for identification is proposed
- 1960s Face recognition becomes semi-automated
- 1960: First model of acoustic speech production is created
- 1965: Automated signature recognition research begins
- 1969: FBI pushes to make fingerprint recognition an automated process
- 1974: First commercial hand geometry systems become available
- 1986: Exchange of fingerprint minutiae data standard is published
- 1988: First semi-automated facial recognition system deployed
- 1992: Biometric Consortium is established within US Government
- 1997: First commercial, generic interoperability standard is published
- 1999: FBI's IAFIS major components become operational

FBI

History of Biometrics

Bertillonage Anthropometric System:

- Alphonse Bertillon relied on the precise measurement of various attributes of the body for identifying recidivists. These measurements included, among others, the height of the individual, the length of the arm, geometry of the head, and the length of the foot.



1. Height.
4. Length of head.
7. left foot.

2. Reach.
5. Width of head.
8. Left middle finger.

3. Trunk
6. Right ear.
9. Left forearm.

- A. K. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, 79, 80-105, 2016.

User Authentication

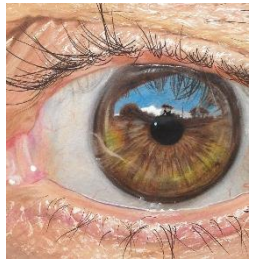
Several techniques can be applied for authenticating a user's identity:

Traditional approaches:

- Knowledge-based: something the user knows, such as a password or PIN.
- Token-based: something the user has, such as a key, an smart card or a credit card.

Biometric approaches:

- Something the user is or produces, such as a fingerprint, an iris or the voice.



- A. K. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, 79, 80-105, 2016.

Biometrics vs. Passwords

Passwords:

- Broadly used.
- One of the oldest authentication methods.

But…

- Can be lost, stolen or forgotten.
- Hard to remember many passwords (for different applications).
- Hard to remember difficult passwords (for higher security).

Shoulder surfing
(visual access to passwords)

Smudge attack
(finger grease traces
on screen)

- A. K. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, 79, 80-105, 2016.

Biometrics vs. Passwords

Passwords: Estimates of annual identity fraud damages per year:

- $1 billion in credit card transactions.
- $1 billion in fraudulent cellular phone use.
- $3 billion in ATM withdrawals.
- ...

It is easy to crack passwords because most of them are weak (related to personal details, typical words or sequential numbers).

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368

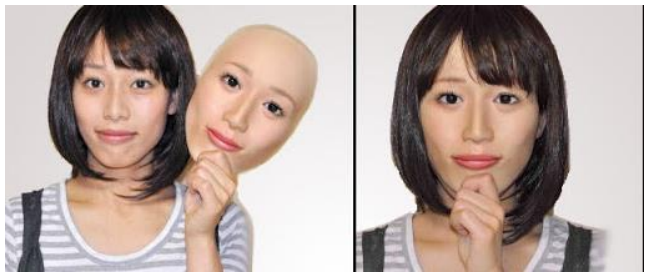
Biometrics vs. Passwords

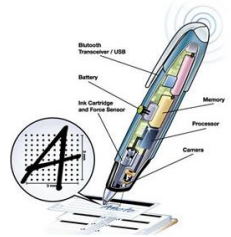
Biometrics:

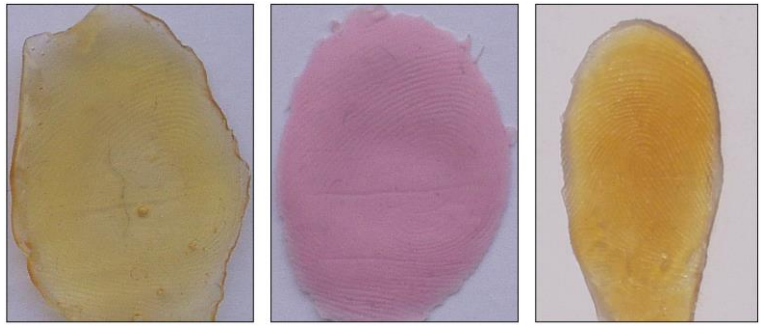
- Cannot be lost or forgotten, but must be enrolled.

But… many challenges:

- Acquisition quality.
- Device interoperability.
- Variability factors.
- Attacks to biometric systems.
- Aging.
- … many more.







- A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

Ideal Characteristics of Biometrics

If a biological, physiological, or behavioral trait has the following properties:

- Universality.
- Uniqueness.
- Permanence.
- Collectability.

Then it can potentially serve as a biometric for *a given application*.

- A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

Ideal Characteristics of Biometrics

Universality:

- Every person should possess this trait.
- In practice, this is usually not the case.
- Otherwise, population of non-universality must be small (< 1%...).
- Nonetheless, 2~3% of global population has erased fingerprints (manual workers).

- A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

Ideal Characteristics of Biometrics

Universality:

- Every person should possess this trait.
- In practice, this is usually not the case.
- Otherwise, population of non-universality must be small (< 1%...).
- Nonetheless, 2~3% of global population has erased fingerprints (manual workers).

Uniqueness:

- The given trait should be sufficiently different across individuals:
  - Genotypical – Genetically linked (e.g. identical twins will have some very similar biometric traits).
  - Phenotypical – Non-genetically linked.

- Uniqueness is difficult to prove analytically.

• A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

Ideal Characteristics of Biometrics

Permanence:

- The trait should be sufficiently invariant over a period of time.
- Degree of permanence has a major impact on the system design and long term operation of biometrics. (e.g. enrollment, adaptive matching design, etc.).
- Short- vs. long-term stability (multi-session vs. aging effects).

- A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

Ideal Characteristics of Biometrics

Permanence:

- The trait should be sufficiently invariant over a period of time.
- Degree of permanence has a major impact on the system design and long term operation of biometrics. (e.g. enrollment, adaptive matching design, etc.).
- Short- vs. long-term stability (multi-session vs. aging effects).

Collectability:

- The characteristic can be quantitatively measured.
- In practice, the biometric collection must be:
  - Non-intrusive
  - Reliable and robust
  - Cost-effective for a given application

- A. K. Jain, K. Nandakumar and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, 79, 80-105, 2016.

System-Level Criteria

The previous criteria was for evaluating the viability of a trait as a biometric.

Once incorporated within a system the following criteria are key to assessing a practical biometric application:

Performance

Identification accuracy, speed, robustness, resource requirements.

Acceptability

How people are willing to accept/use a particular biometric trait.

Circumvention

How easy is it to fool the system by fraudulent methods.

• A. K. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, 79, 80-105, 2016.

System-Level Criteria

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	High	High
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	High	Medium	Medium
Signature	Medium	Medium	High
Face	High	High	High

- A. K. Jain, K. Nandakumar and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, 79, 80-105, 2016.

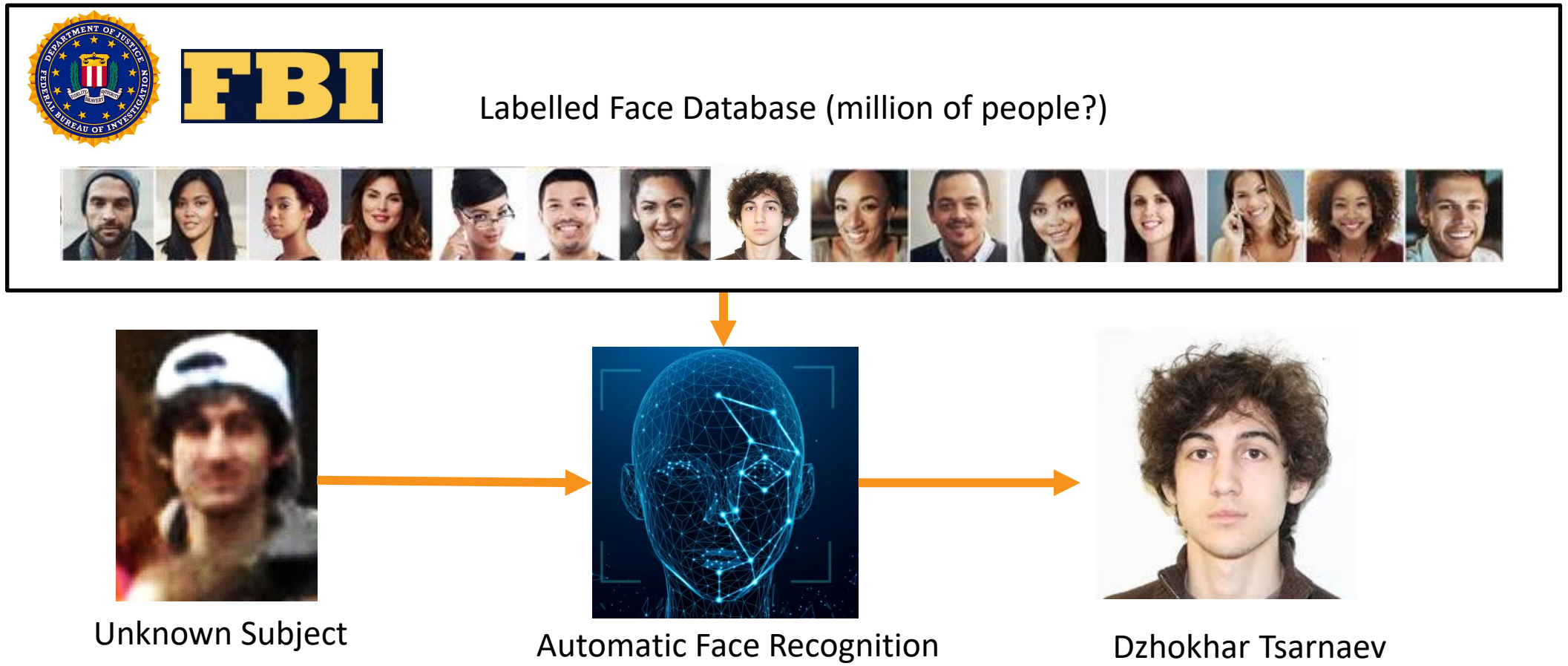
Morpho Finger on the Fly

- URL: https://www.safran-group.com/media/20160105_fbi-certifies-morphowave-desktop-contactless-fingerprint-scanner

Identification vs. Verification

Identification systems answer the question:

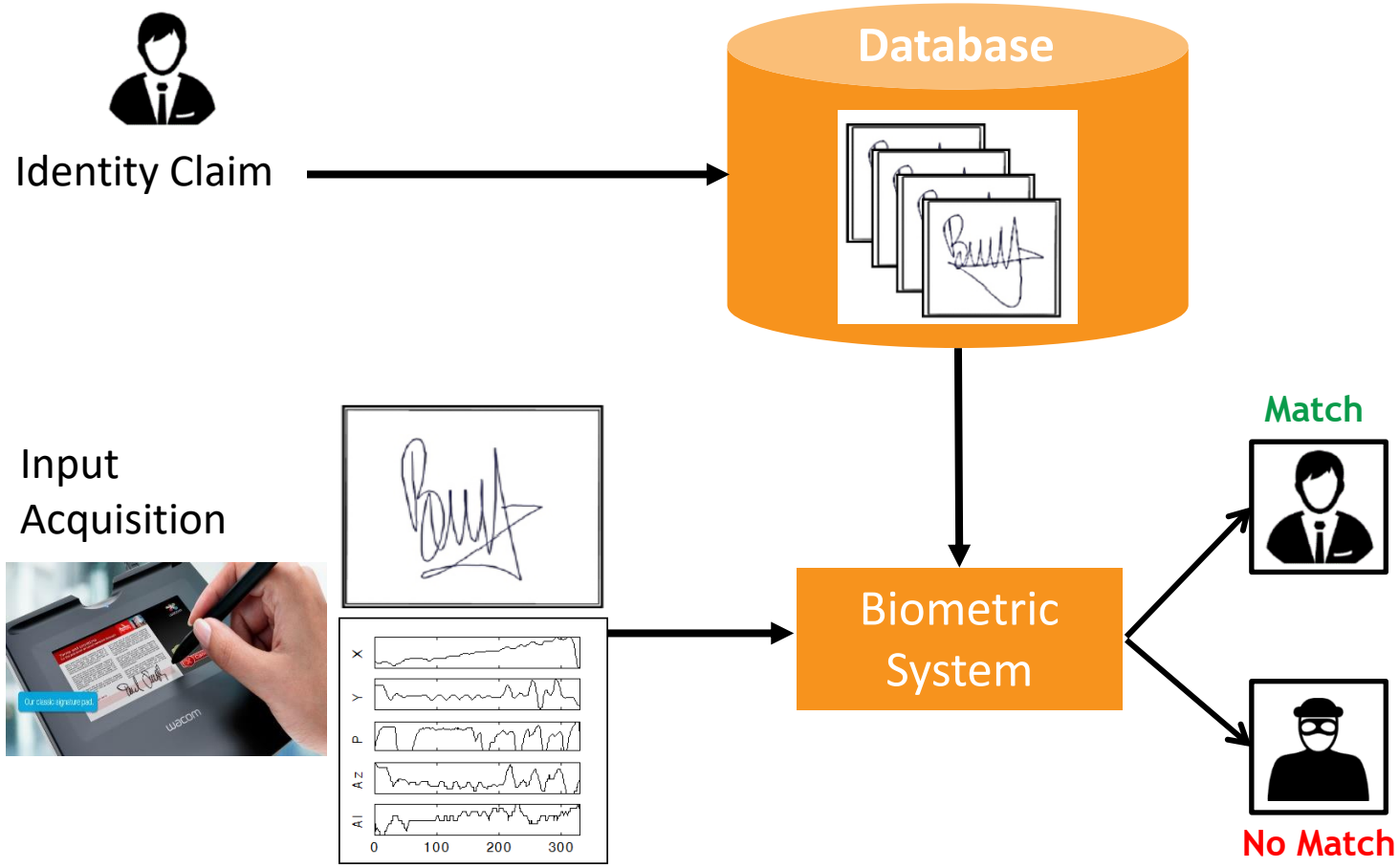
- "Who is the person?"
- The answer returned by the system is an identity such as a name or ID number.



Identification vs. Verification

Verification systems answer the question:

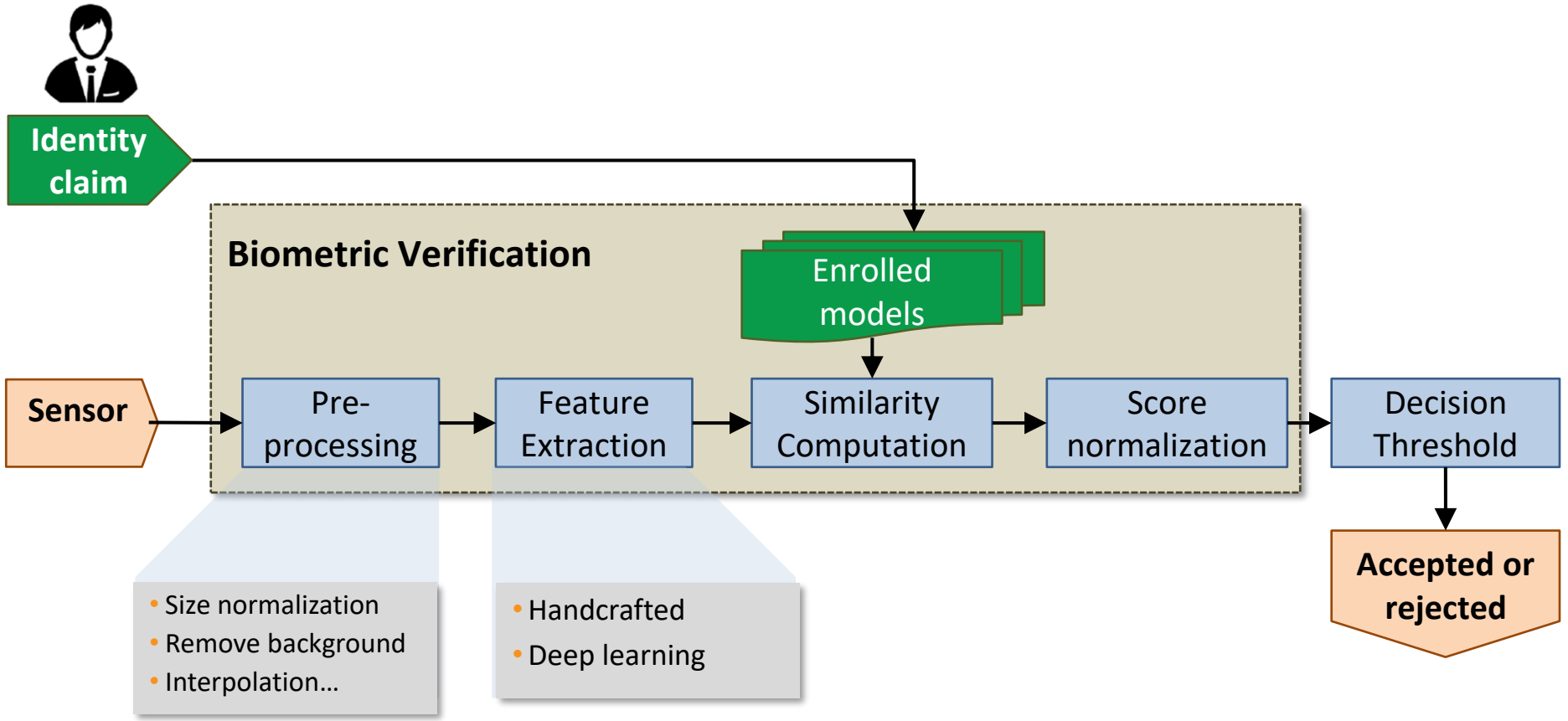
- "Is a given person who he claims to be?"
- The answer returned by the system is match or no match.



Identification vs. Verification

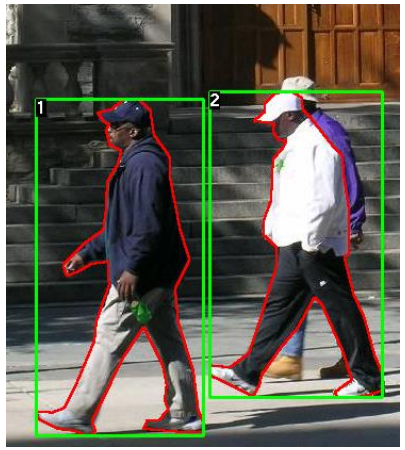
Identification	Verification
It determines the identity of the person.	It determines whether the person is indeed who he claims to be.
No identity claim One-to-many mapping. Cost of computation is proportional to the number of user records.	Identity claim from the user One-to-one mapping. The cost of computation is independent of the number of records of users.

Biometric Verification System



Applications

- Passport control
- Civil (birth) certificates
- Computer and smartphone logins
- Access to secured physical or virtual areas
- Surveillance
- Bank transactions and ATMs
- E-commerce
- Medicine and Psychology
- e-Administration & e-Government transactions
- Drivers licence



Santander

Bankia

CaixaBank

e-Government

Privacy and Legal Issues/Concerns

System Design and Implementation must adequately address these issues to satisfy the user, the law, and society:

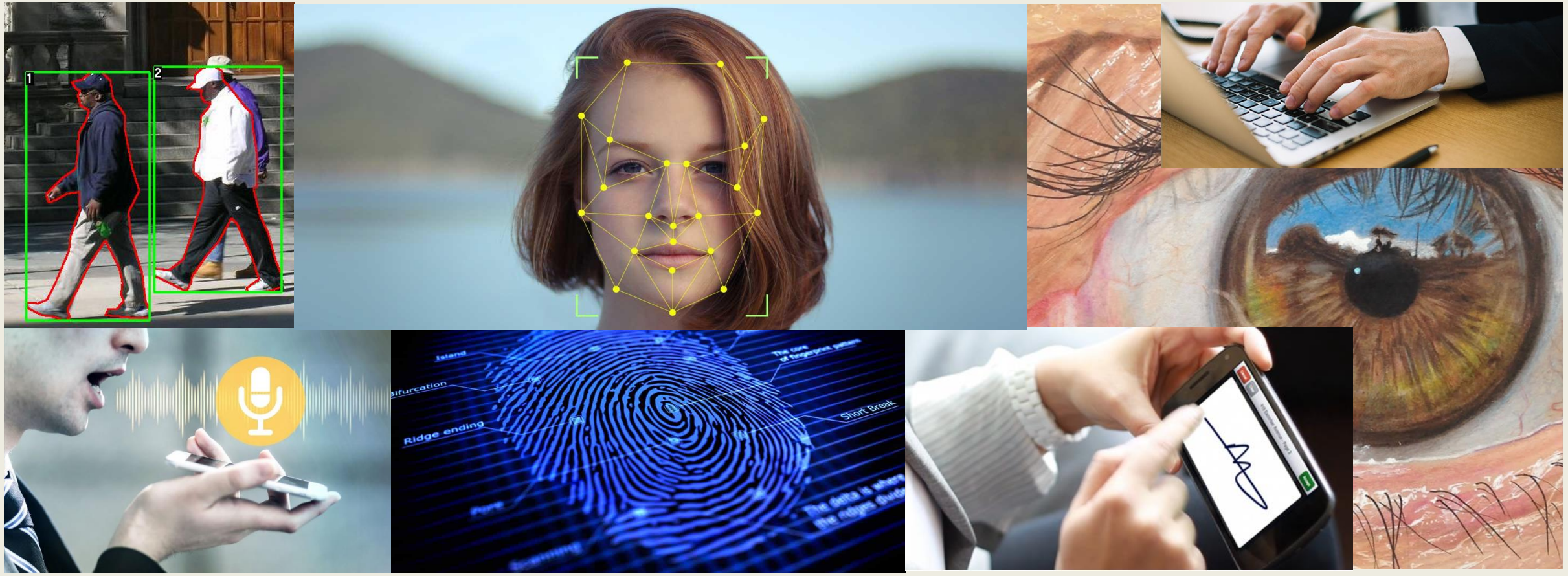
- Is the biometric data like personal information (e.g. such as medical information) ?
- Can medical information be derived from the biometric data? Or other sensitive information such as gender, demographic group, etc.
- Does the biometric system store information enabling a person's "identity" to be reconstructed or stolen?
- Is any third party having access to biometric information?

Privacy and Legal Issues/Concerns

And...

- What happens to the biometric data after the intended use is over?
- Is the security of the biometric data assured during transmission and storage?
  - Contrast process of password loss or theft with that of a biometric.
  - How is a theft detected and "new" biometric recognized?
- Notice of biometric use: is the public aware of the fact that a biometric system is being employed?

Introduction to Biometrics



Ruben Tolosana
ruben.tolosana@uam.es

BiDA Lab
Biometrics & Data Pattern Analytics Lab

UAM
Universidad Autónoma de Madrid