Artificial Intelligence for Biometrics

Vincenzo Piuri

Università degli Studi di Milano

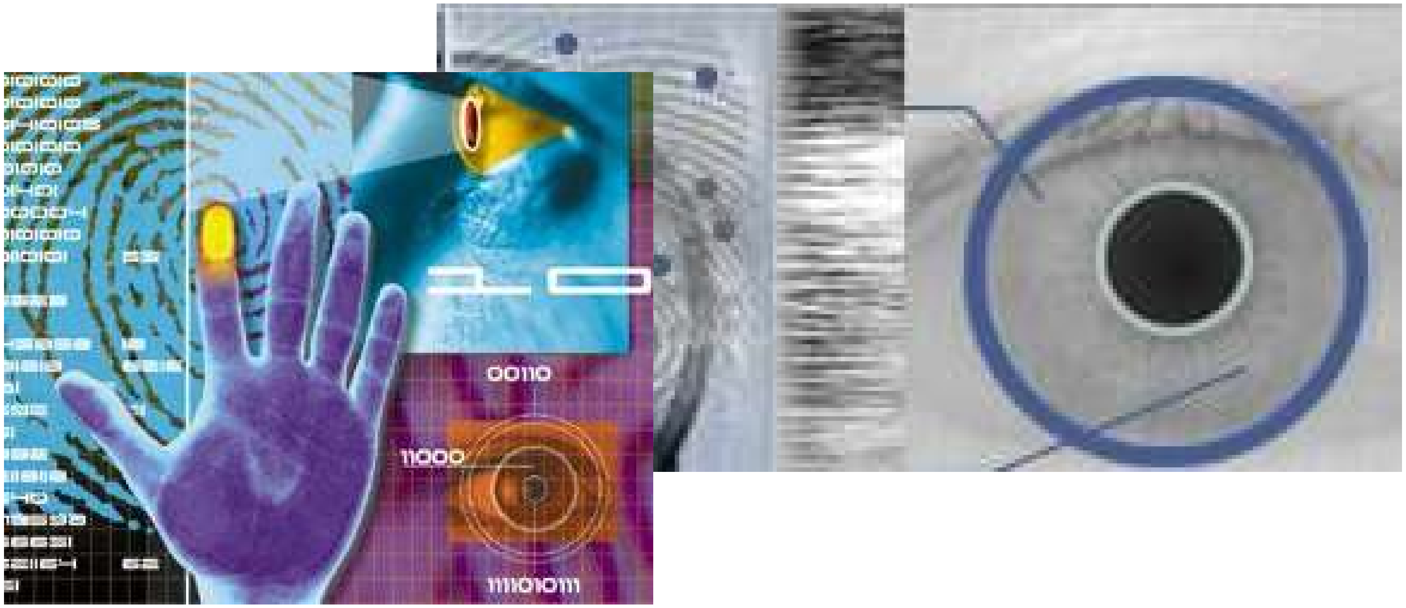
vincenzo.piuri@unimi.it

https://piuri.di.unimi.it

SECRYPT 2024 – Dijon, France – 8-10.7.2024

EdgeAI GLACIATION SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Biometrics



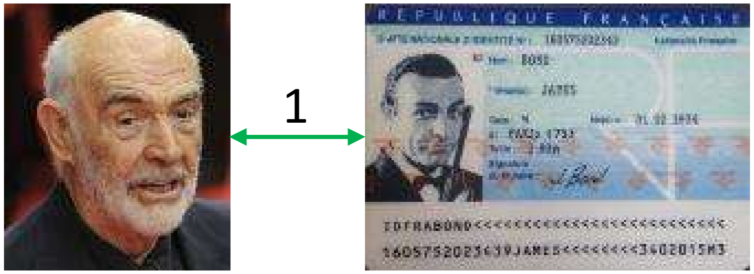
Biometrics is defined by the International Organization for Standardization (ISO) as:

“**the <u>automated</u> recognition of individuals based on their <u>behavioral</u> and <u>biological</u> characteristics**”

Verification vs Identification

Verification (Autenthication):
Am I who I say to be?

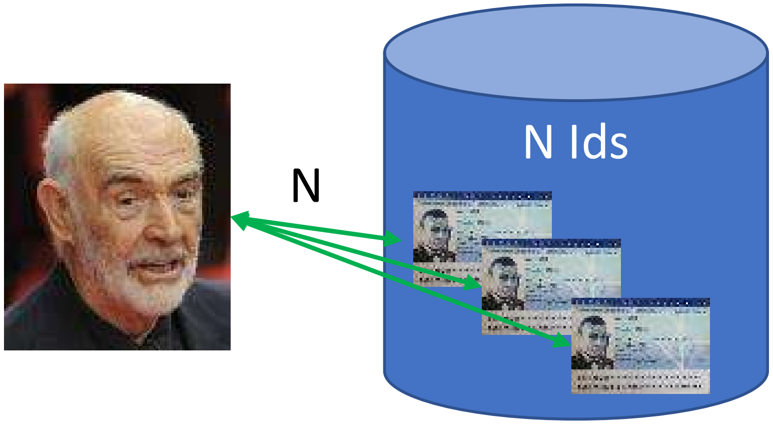
one-to-one **(1:1)** operation



Identification: *Who am I?*

one-to-many **(1:N)** operation

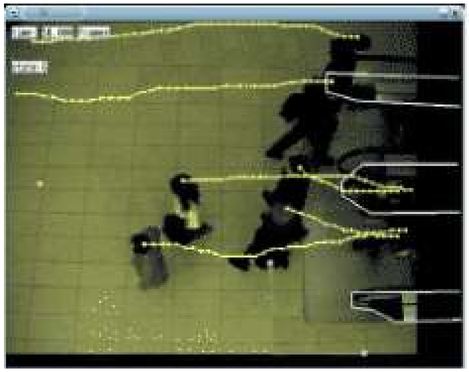
- STANDARD IDENTIFICATION:
  finds 1 result (best candidate)
- SCREENING:
  finds k possible results (candidates)

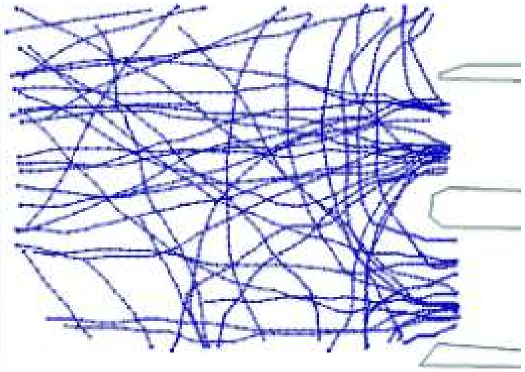


N times longer!
Error increases!
(w.r.t. Verification)

Behavior Recognition for Security

- Motion





- Gesture

- Emotion

- …

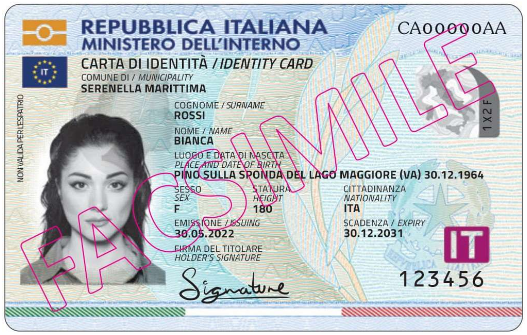
Biometric Applications

Physical Access Control

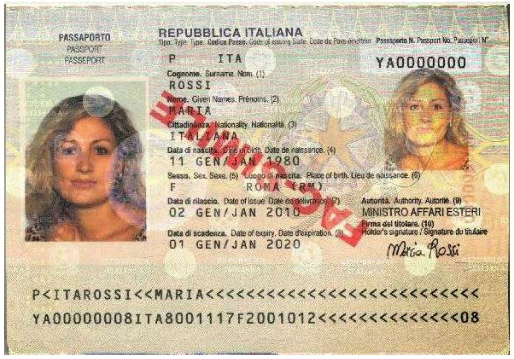
- Critical areas
- Restricted areas
- Private areas
- Public buildings
- Sports arenas
- Bank caveau
- Transportations
- …

Government Applications

- Identity card, passport
- Electoral cards, driver license
- Healthcare card
- Automated Border Control
- Police identification



REPUBBLICA ITALIANA
MINISTERO DELL'INTERNO
CA00000AA
CARTA DI IDENTITÀ / *IDENTITY CARD*
COMUNE DI / *MUNICIPALITY*
SERENELLA MARITTIMA
NON VALIDA PER L'ESPATRIO
COGNOME / *SURNAME*
ROSSI
NOME / *NAME*
BIANCA
LUOGO E DATA DI NASCITA
PLACE AND DATE OF BIRTH
PINO SULLA SPONDA DEL LAGO MAGGIORE (VA) 30.12.1964
SESSO *SEX* F
STATURA *HEIGHT* 180
CITTADINANZA *NATIONALITY* ITA
EMISSIONE / *ISSUING* 30.05.2022
SCADENZA / *EXPIRY* 30.12.2031
FIRMA DEL TITOLARE
HOLDER'S SIGNATURE
Signature
1X2F
IT
123456
FACSIMILE



PASSAPORTO
PASSPORT
PASSEPORT
REPUBBLICA ITALIANA
Tipo. Type. Type. Codice Paese. Code of issuing State. Code du Pays émetteur. Passaporto N. Passport No. Passeport N°
P ITA YA0000000
Cognome. Surname. Nom. (1)
ROSSI
Nome. Given Names. Prénoms. (2)
MARIA
Cittadinanza. Nationality. Nationalité. (3)
ITALIANA
Data di nascita. Date of birth. Date de naissance. (4)
11 GEN/JAN 1980
Sesso. Sex. Sexe. (5) Luogo di nascita. Place of birth. Lieu de naissance. (6)
F ROMA (RM)
Data di rilascio. Date of issue. Date de délivrance. (7)
02 GEN/JAN 2010
Autorità. Authority. Autorité. (9)
MINISTRO AFFARI ESTERI
Firma del titolare. (10)
Holder's signature / Signature du titulaire
Maria Rossi
Data di scadenza. Date of expiry. Date d'expiration. (8)
01 GEN/JAN 2020
FACSIMILE

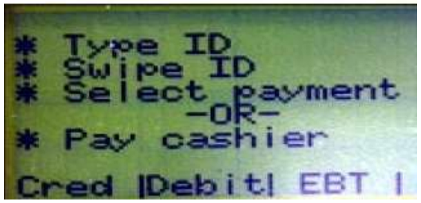
```
P<ITAROSSI<<MARIA<<<<<<<<<<<<<<<<<<<<<<<<<<<
YA00000008ITA8001117F2001012<<<<<<<<<<<<<<08
```

Surveillance

- Buildings
- Public areas
- …

Logical Access Control to Services

- Home banking, ATM
- Credit cards
- Supermarkets
- E-commerce
- Cellular phones
- Computers
- Data
- …



* Type ID
* Swipe ID
* Select payment
-OR-
* Pay cashier
Cred |Debit| EBT |

9:41
Tuesday, September 12
MESSAGES
Rand Hill
Thanks for giving me a ride to work! I owe you a coffee. Cream and five sugars, right?
MESSAGES
Trev Smith
What do you want for lunch? Don't say salad. Please.

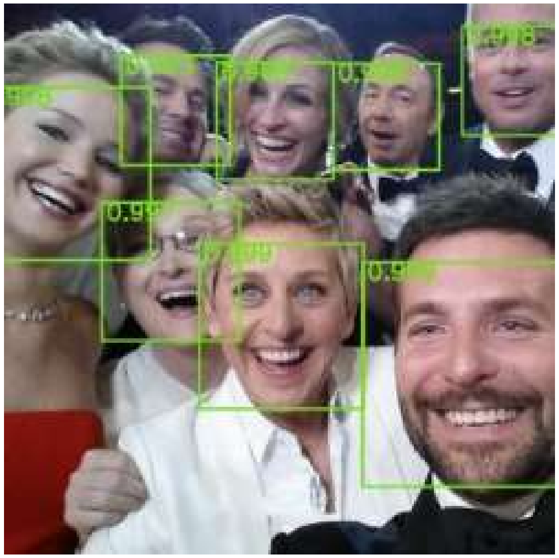
Smart Environments

- Smart home/building
- Smart entertainment systems
- Smart cars/transportation
- Intelligent traffic management
- Smart shops
- Information kiosks and augmented reality

AUTO CURTAIN
HOME ENTERTAINMENT
MOODS
GARAGE
ON OFF
AUTO LIGHTING
eCAM
SECURITY
HOME BACK UP SYSTEM
AUTO SPRINKLERS
HOME AUTOMATION
COMMUNICATION

Personalized Interactions

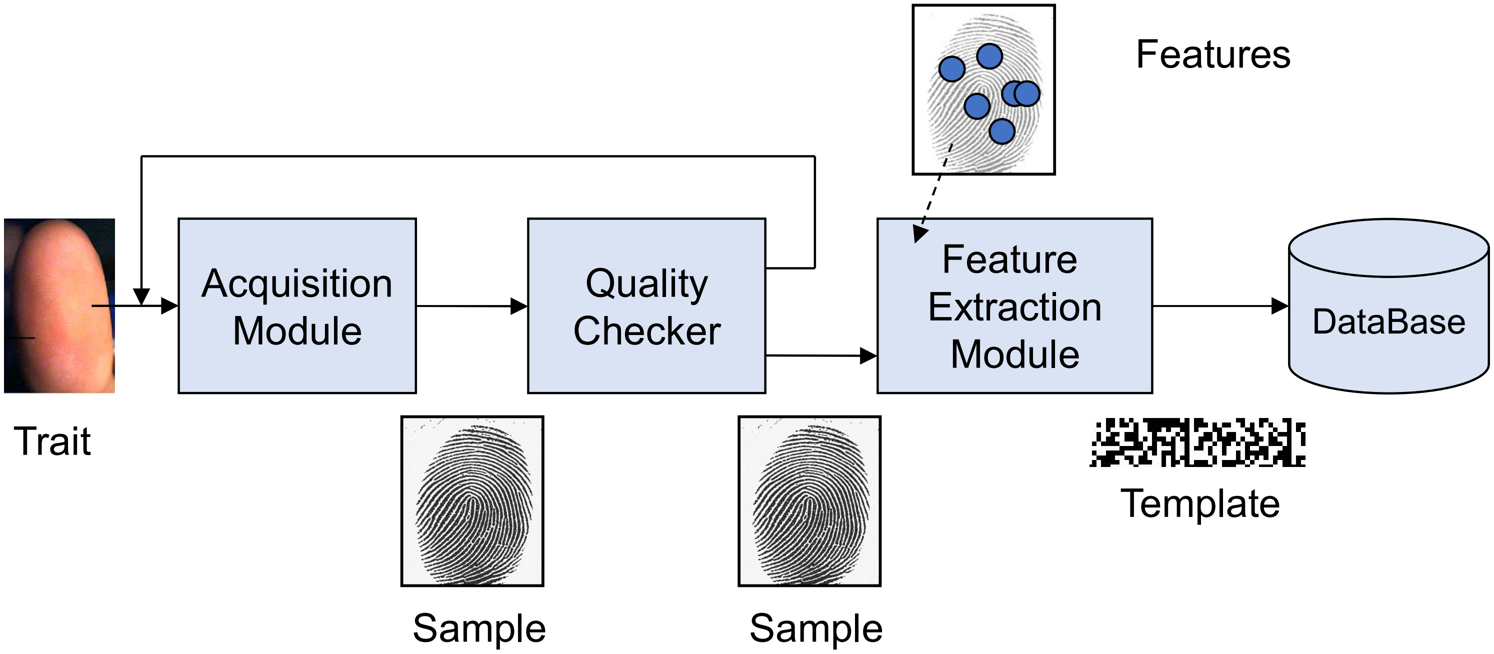
- Social networks
  face recognition for automated tagging
- Virtual assistants
  voice recognition for personalized speech recognition
- e-commerce systems
  emotion recognition for personalized interaction
- …



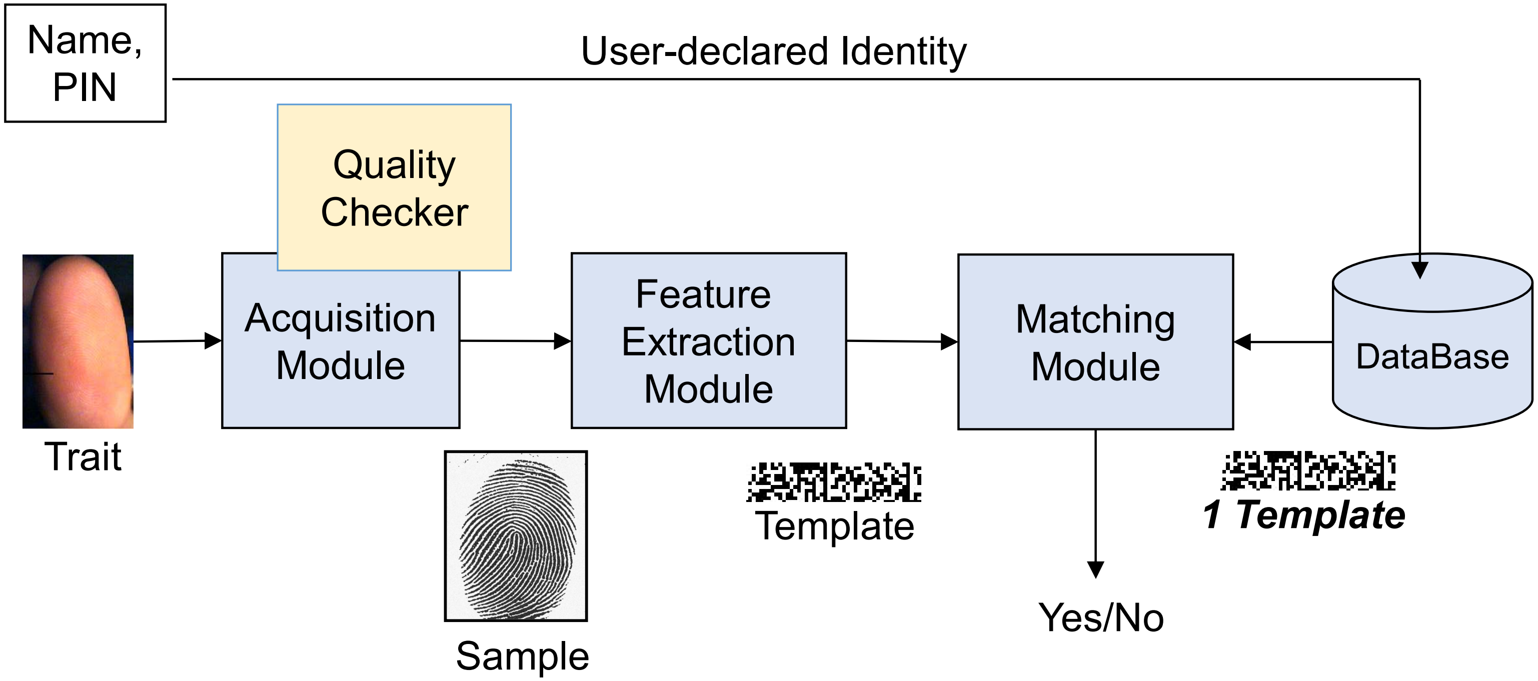
Biometric Systems Operation

Enrollment

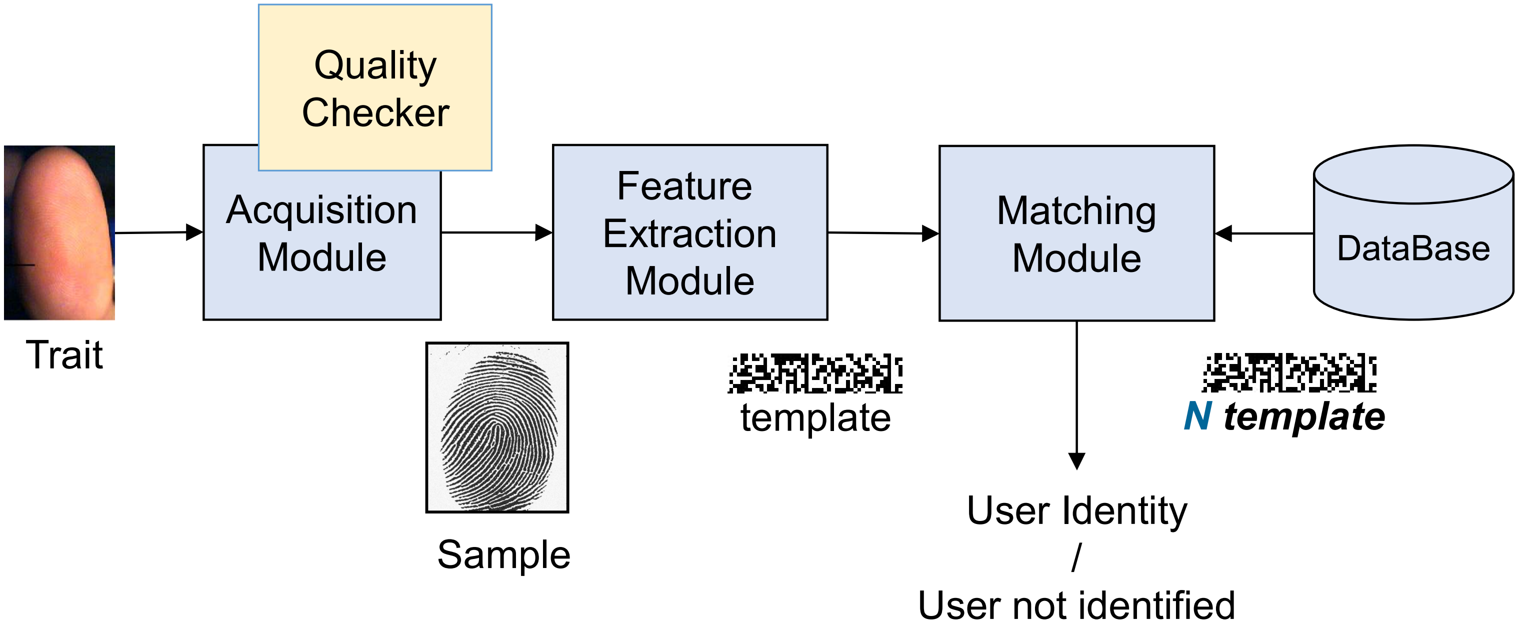
Biometric trait → Template → DataBase



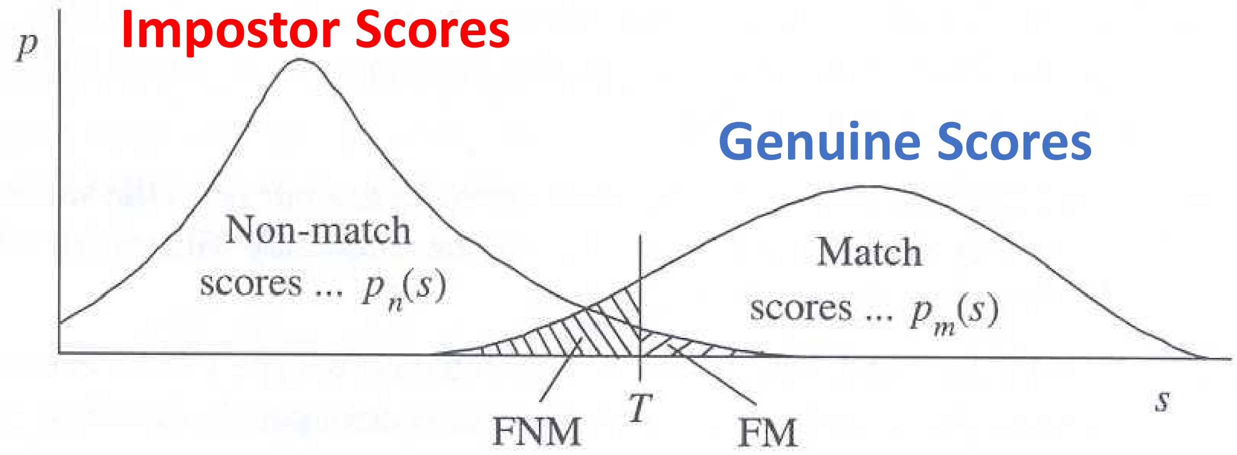
Verification (Autentication)



Identification



Impostor and Genuine Recognition

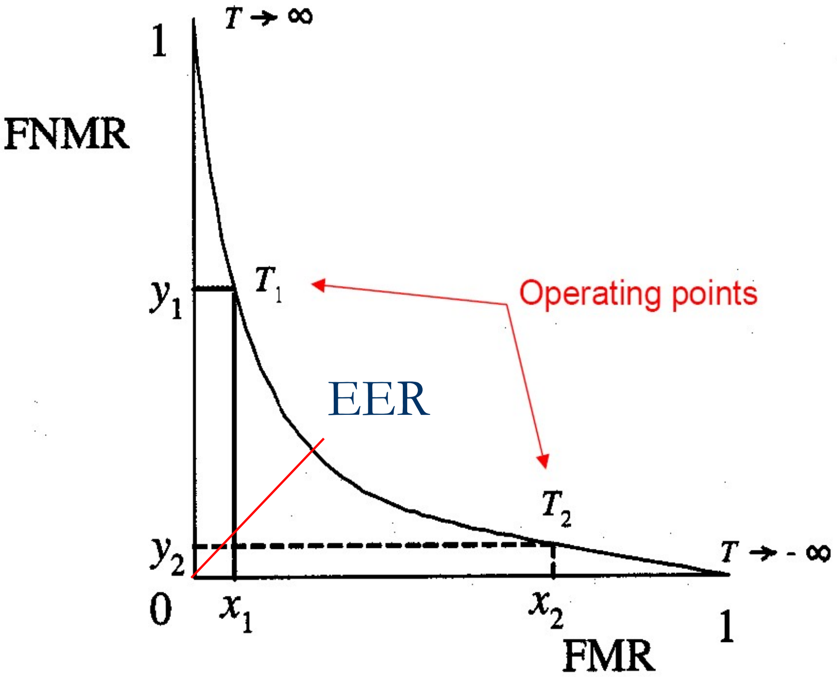

Impostor Scores

Genuine Scores

*False Match Rate (**FMR**)*

*False Non-Match Rate (**FNMR**)*

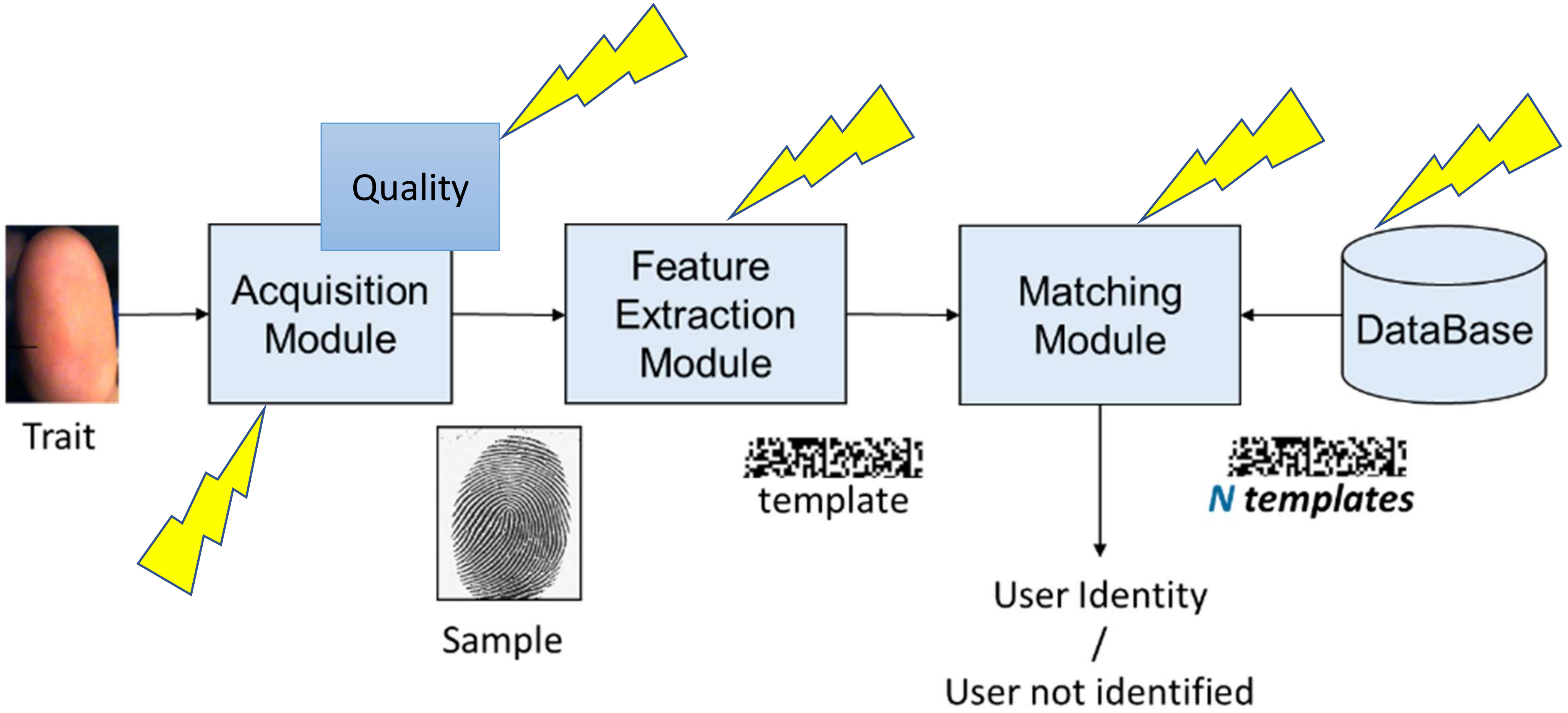
*Equal Error Rate (**EER**): FNMR=FMR*


Operating points

EER

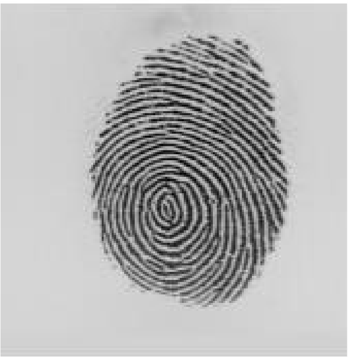
Biometric Systems and AI: Research Directions

Artificial Intelligence: Research Directions (1)

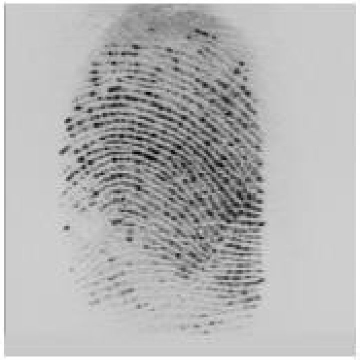


Artificial Intelligence: Research Directions (2)

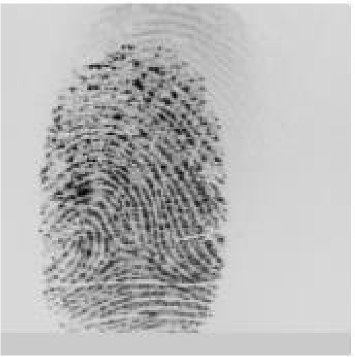
Quality Assessment



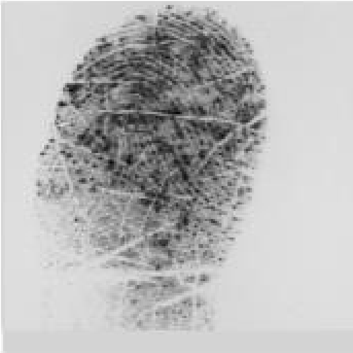
Quality = 0.93



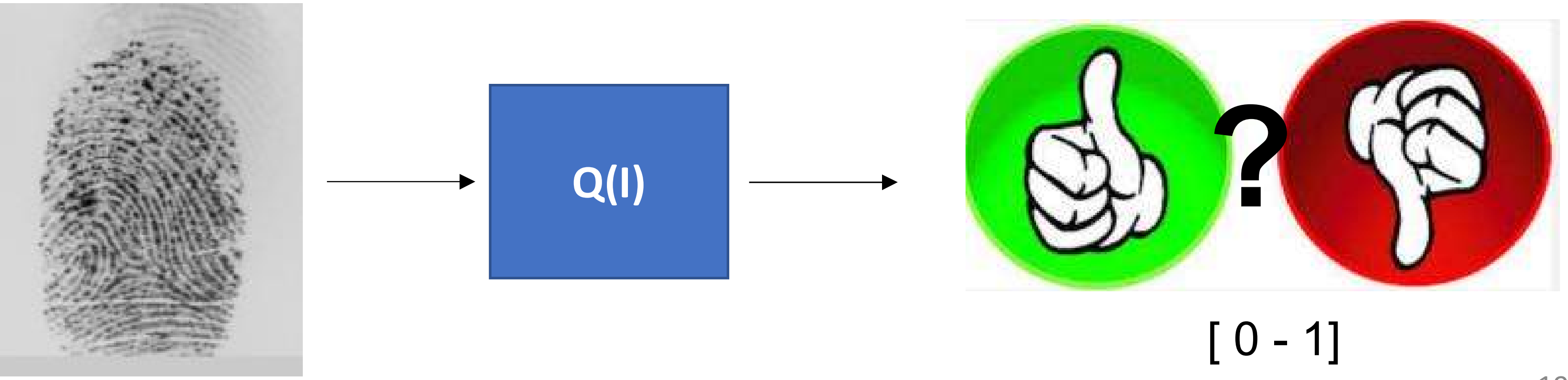
Quality = 0.63



Quality = 0.35



Quality = 0.19



Q(I)

?

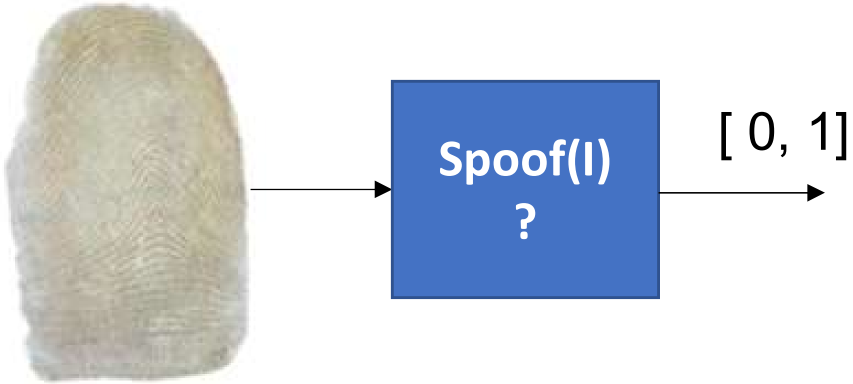
[0 - 1]

Artificial Intelligence: Research Directions (3)

Antispoofing

- Example: Synaptics PurePrint™ anti-spoof technology
- Examines fingerprint images using a NN to distinguish between fake and actual fingers

USB Dongle with fingerprint reader

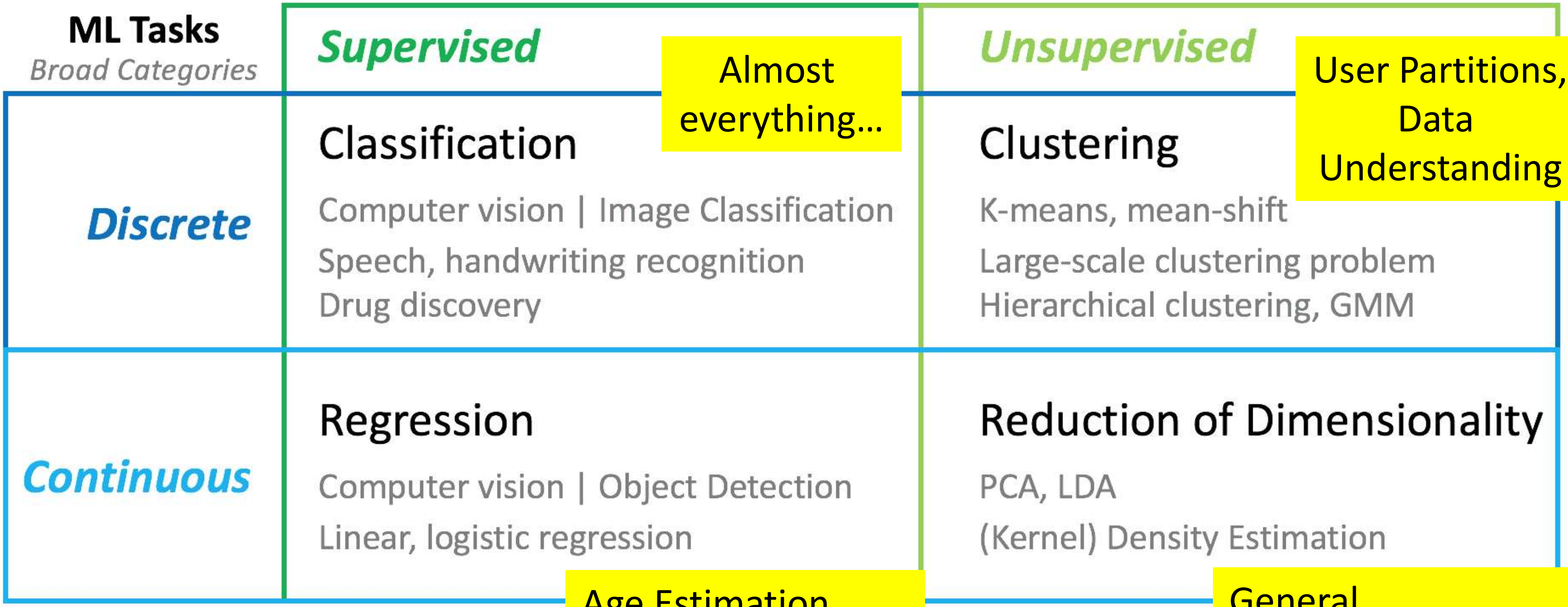


Spoof(I)
?

[0, 1]

Artificial Intelligence: Research Directions (4)

AI & Machine Learning Methods for Biometrics



ML Tasks *Broad Categories*	***Supervised***	***Unsupervised***
Discrete	Classification Computer vision | Image Classification Speech, handwriting recognition Drug discovery	Clustering K-means, mean-shift Large-scale clustering problem Hierarchical clustering, GMM
Continuous	Regression Computer vision | Object Detection Linear, logistic regression	Reduction of Dimensionality PCA, LDA (Kernel) Density Estimation

Almost everything…

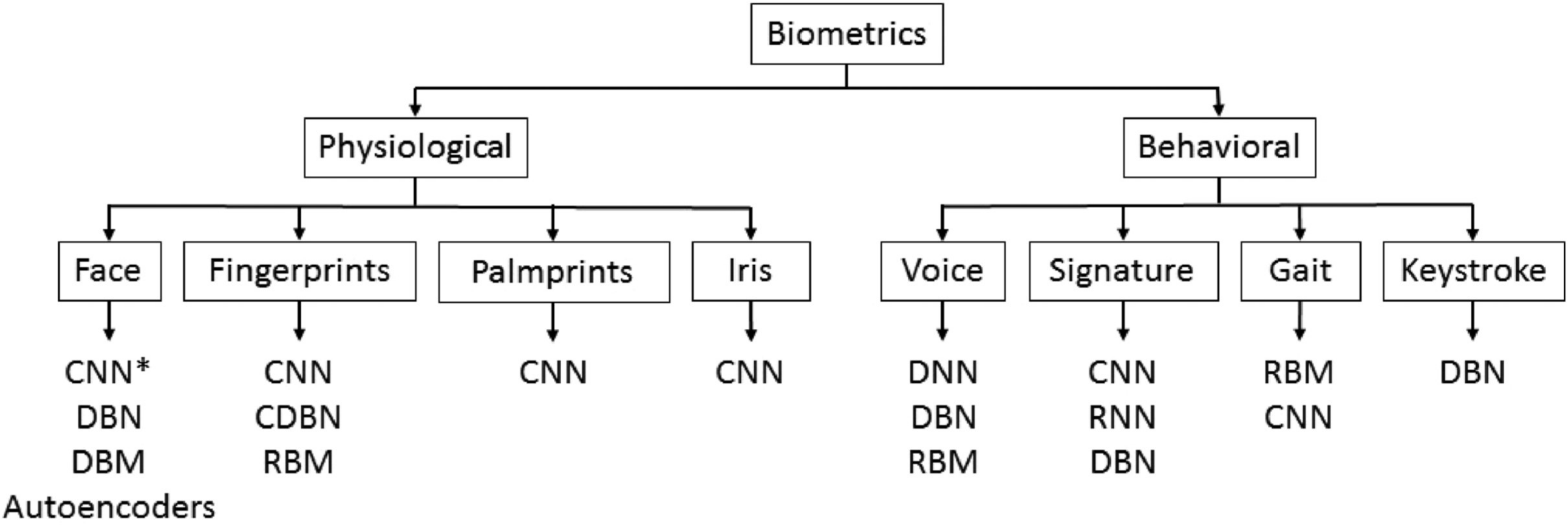
User Partitions, Data Understanding

Age Estimation, Soft Biometrics, Quality Assessment

General… Data Understanding, Input processing…

Artificial Intelligence: Research Directions (5)

Deep Learning for Biometrics



Biometrics

Physiological

Behavioral

Face

Fingerprints

Palmprints

Iris

Voice

Signature

Gait

Keystroke

CNN*
DBN
DBM
Autoencoders

CNN
CDBN
RBM

CNN

CNN

DNN
DBN
RBM

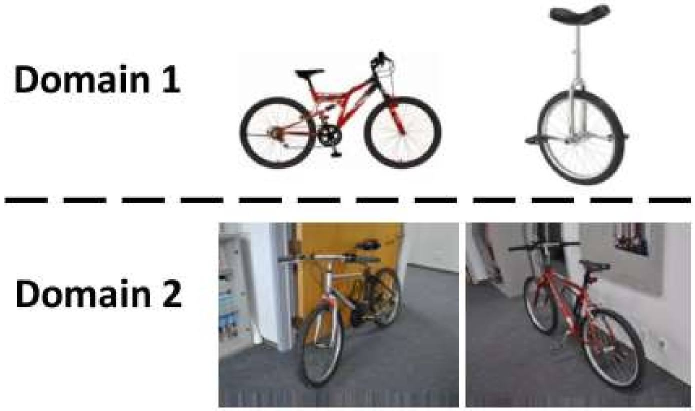
CNN
RNN
DBN

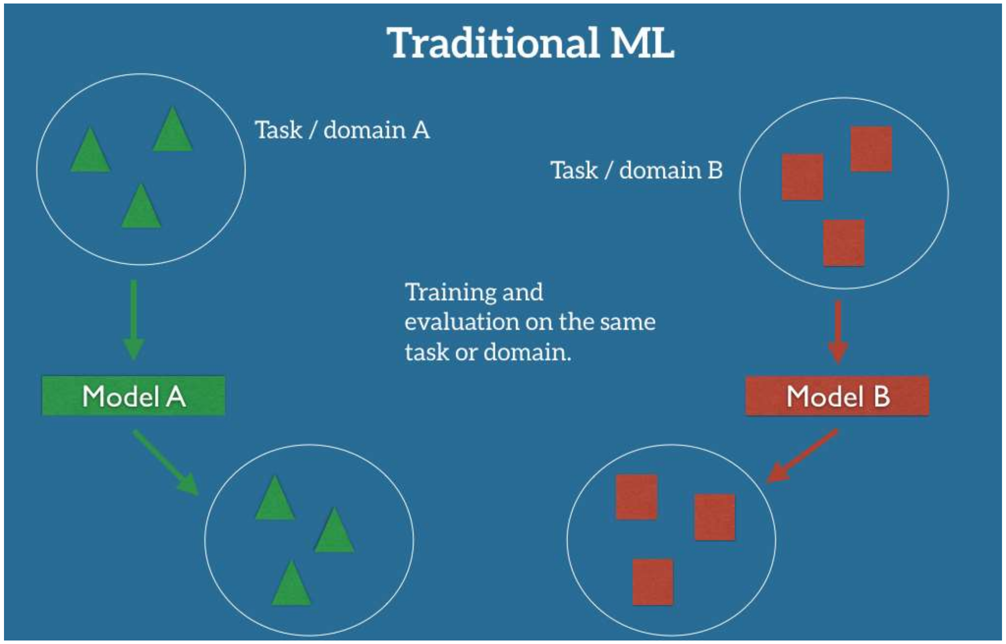
RBM
CNN

DBN

Artificial Intelligence: Research Directions (6)

Transfer Learning





Traditional ML

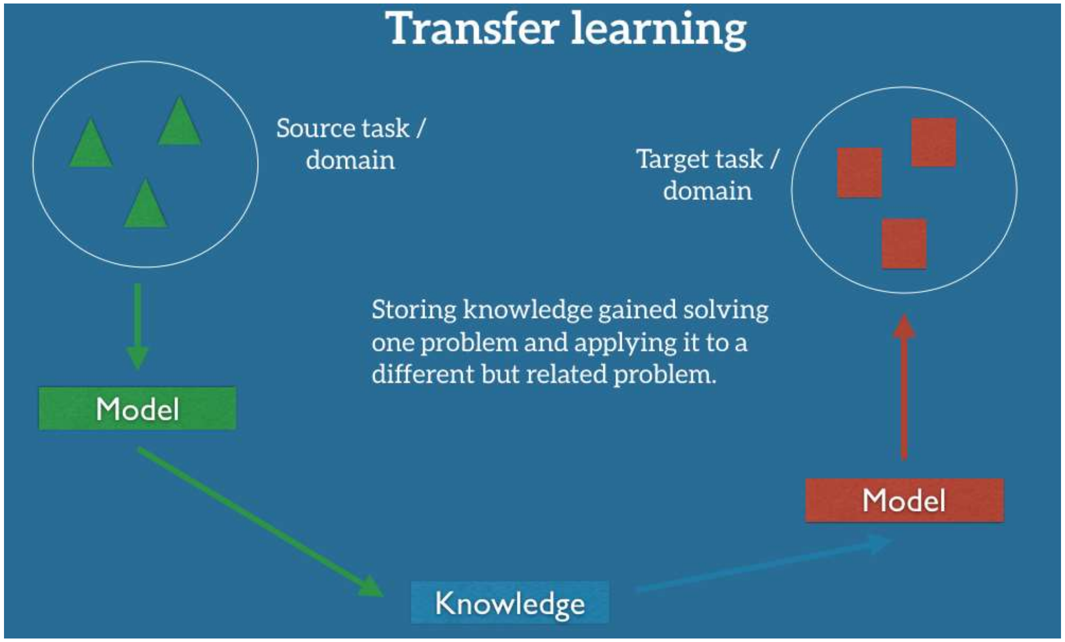
Task / domain A

Task / domain B

Training and evaluation on the same task or domain.

Model A

Model B



Transfer learning

Source task / domain

Target task / domain

Storing knowledge gained solving one problem and applying it to a different but related problem.

Model

Model

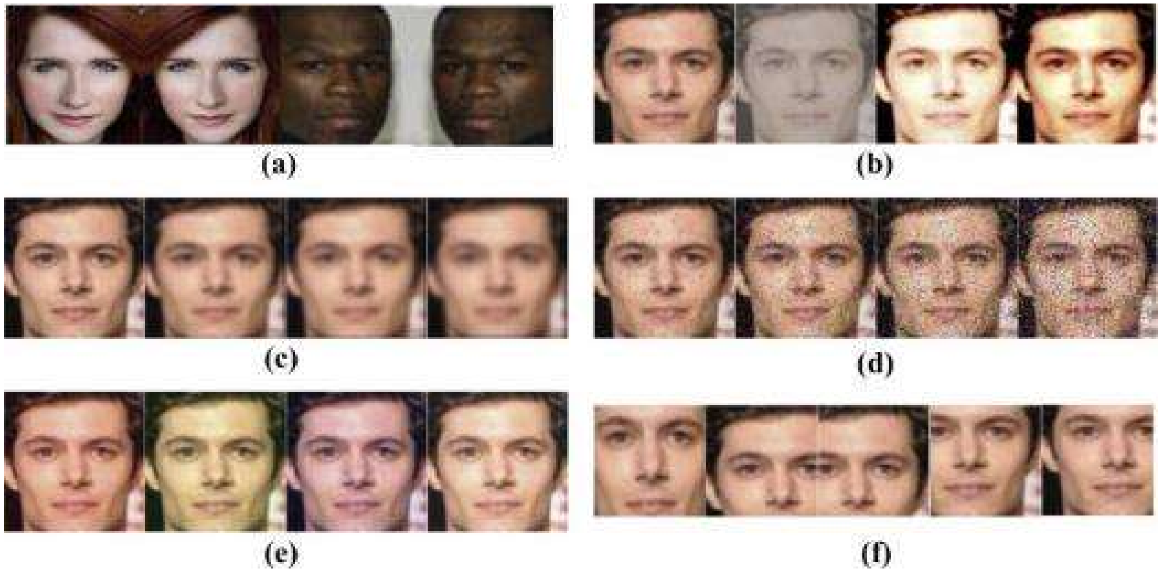
Knowledge

Artificial Intelligence: Research Directions (7)

AI for Data Augmentation

Landmark perturbation for face alignment.

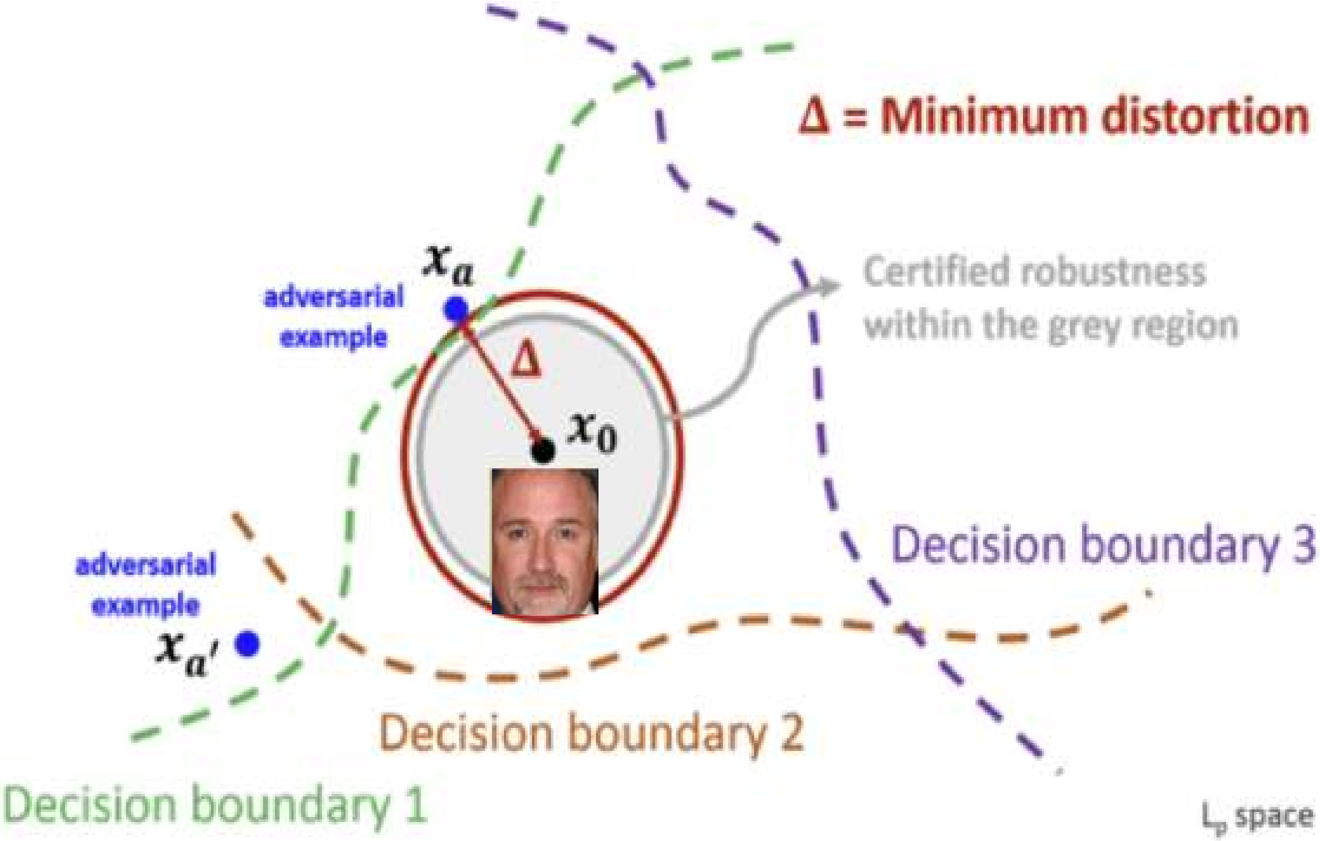
Flipping
patches (clipping)
color casting
blurring



Artificial Intelligence: Research Directions (8)

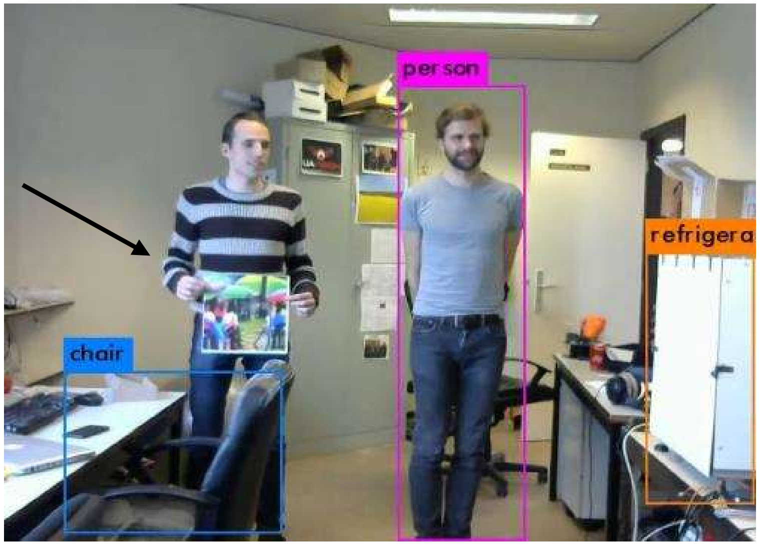
AI for Recognition Robustness

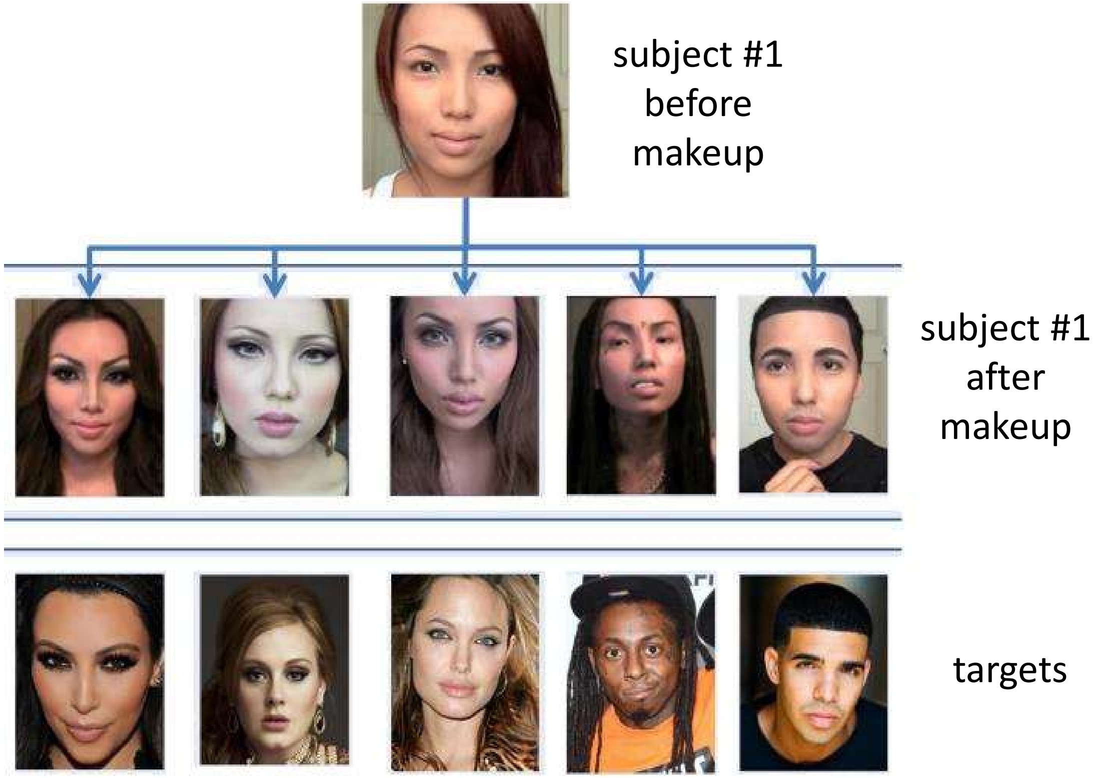
Generative Adversarial Networks



Artificial Intelligence: Research Directions (9)

AI for Identity Concealing Detection




subject #1 before makeup

subject #1 after makeup

targets

Human Beings are Multimodal

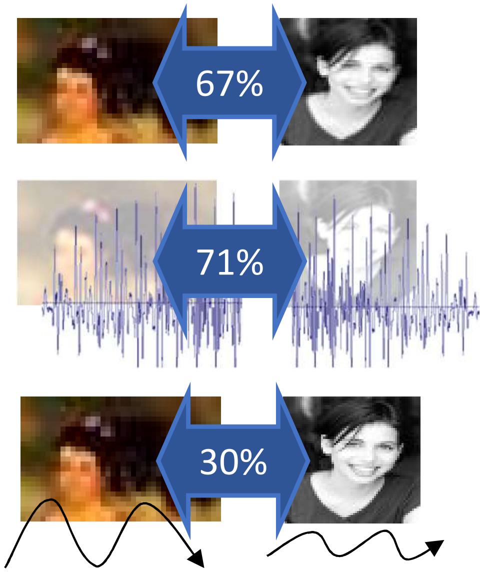
While waiting for your friend Laura, someone runs towards you and greeting you

→ The brain performs a multimodal matching

Face

Voice

Gait



Soft biometrics

- 57Kg
- 175cm
- Brunette

7%

- 79Kg
- 155cm
- Brown hair

67%+71%+30%+7%

It’s not Laura,
it’s Maria, her sister

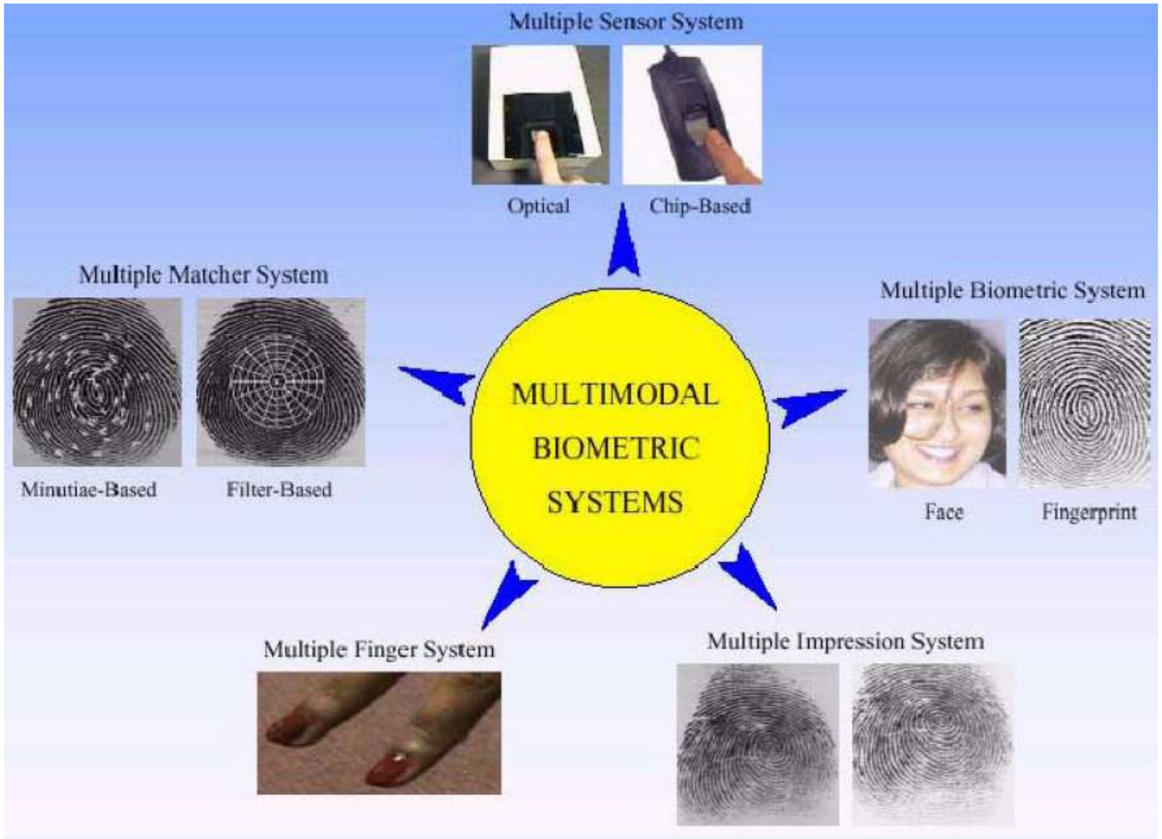
Multibiometrics

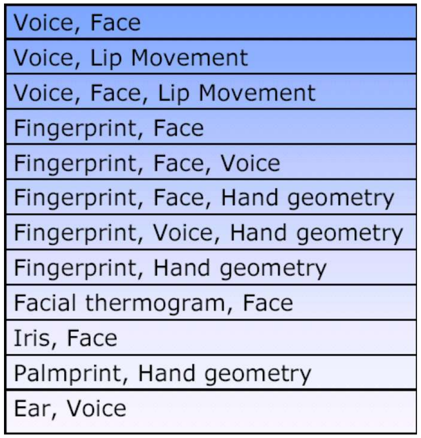
Data gathering

- Multiple sensors
- Multiple traits (multimodal)
- Multiple instances
- Multiple samples
- Multiple matchers

Fusion logics

- Sensor level
- Feature set level
- Matching score level
- Decision level

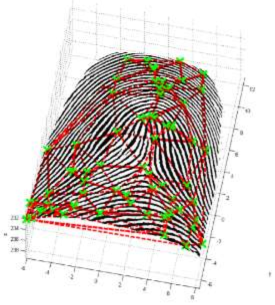


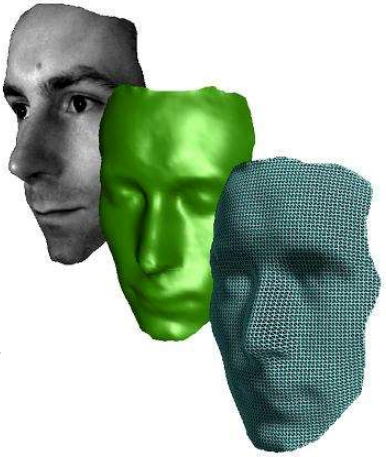


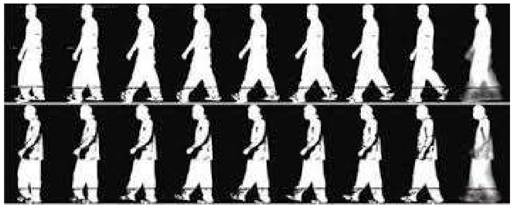
Voice, Face
Voice, Lip Movement
Voice, Face, Lip Movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand geometry
Fingerprint, Voice, Hand geometry
Fingerprint, Hand geometry
Facial thermogram, Face
Iris, Face
Palmprint, Hand geometry
Ear, Voice

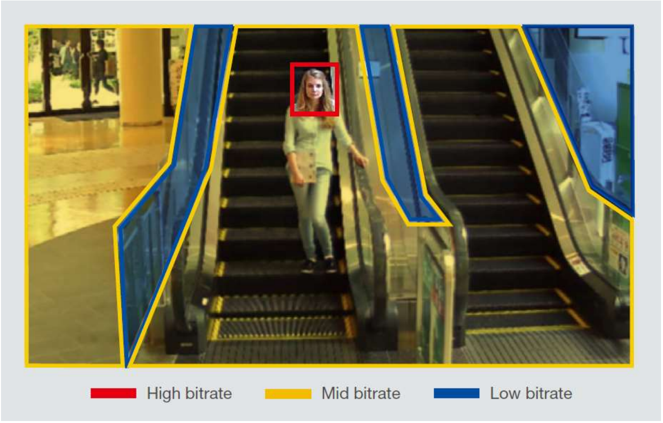
Multibiometrics: Research Directions

- New biometric modalities
- New sensors
- More advanced fusion techniques
- Application to mobile devices
- Advanced surveillance and behavior detection
- New antispoofing methods
- AI for multibiometrics
- …







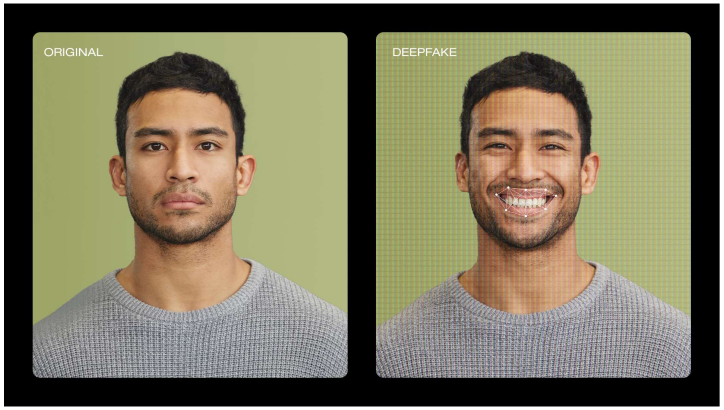


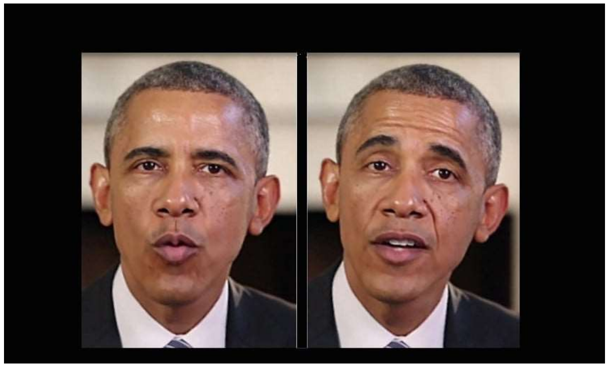
Continuous / Periodic Authentication: Research Directions

- Keystroke dynamics, mouse movements
- Face, iris
- Gesture
- Voice
- Gait for mobile devices
- Research directions:
  - user-friendly biometrics
  - soft biometrics
  - behavior prediction
  - IoT integration
  - AI for continuous/periodic authentication
  - …

Deepfake: Research Directions

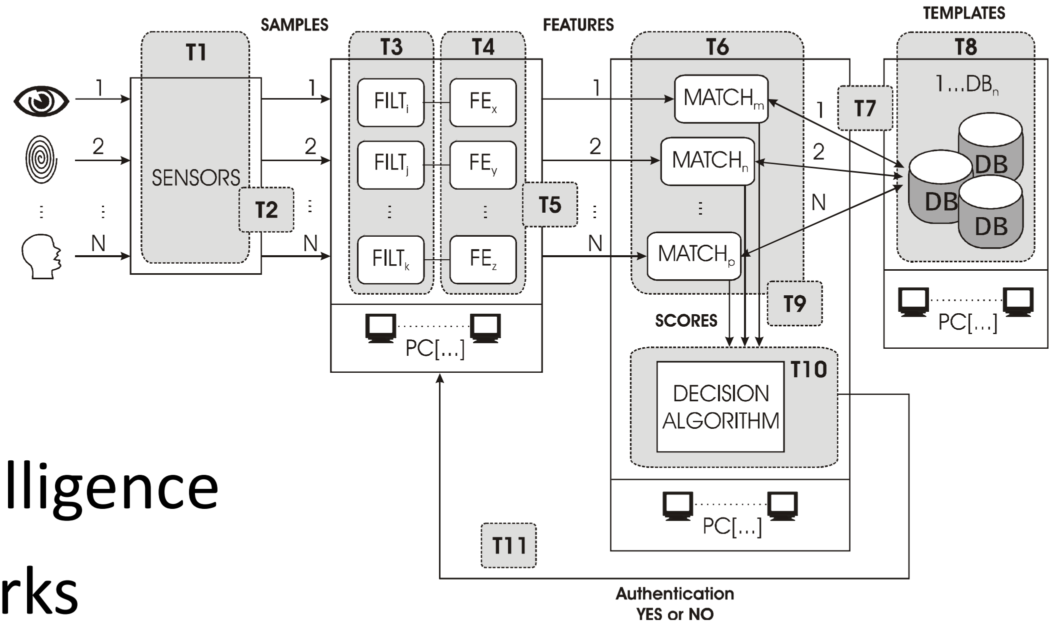
- Digital manipulation of biometric traits by means of generative techniques
- Create fake biometrics
- Fake photos and video are used for fake news
- AI for detecting deepfake





Distributed Biometric Systems: Research Directions

- Distributed search
- Distributed match
- Interoperability
- Trustability
- Applications in ambient intelligence
- Applications in social networks
- Applications in Industry 4.0
- Analysis by artificial intelligence approaches
- …

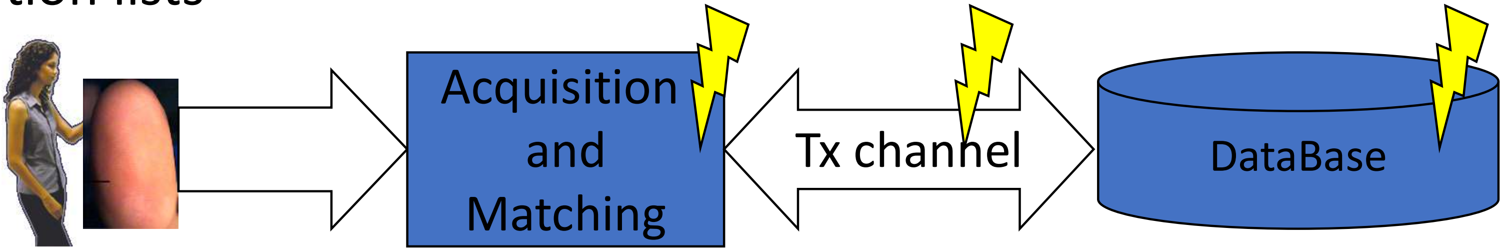


Biometric Privacy: Research Directions (1)

- Control over-use and disclosure of personal identity and information
- Biometric personal identity must be protected
- Biometric traits cannot be replaced
- Use of stolen biometric traits
  - Access to personal information
  - Impersonation
  - Misuse
  - Proscription lists

RFID
UNIONE EUROPEA
REPUBBLICA ITALIANA
PASSAPORTO

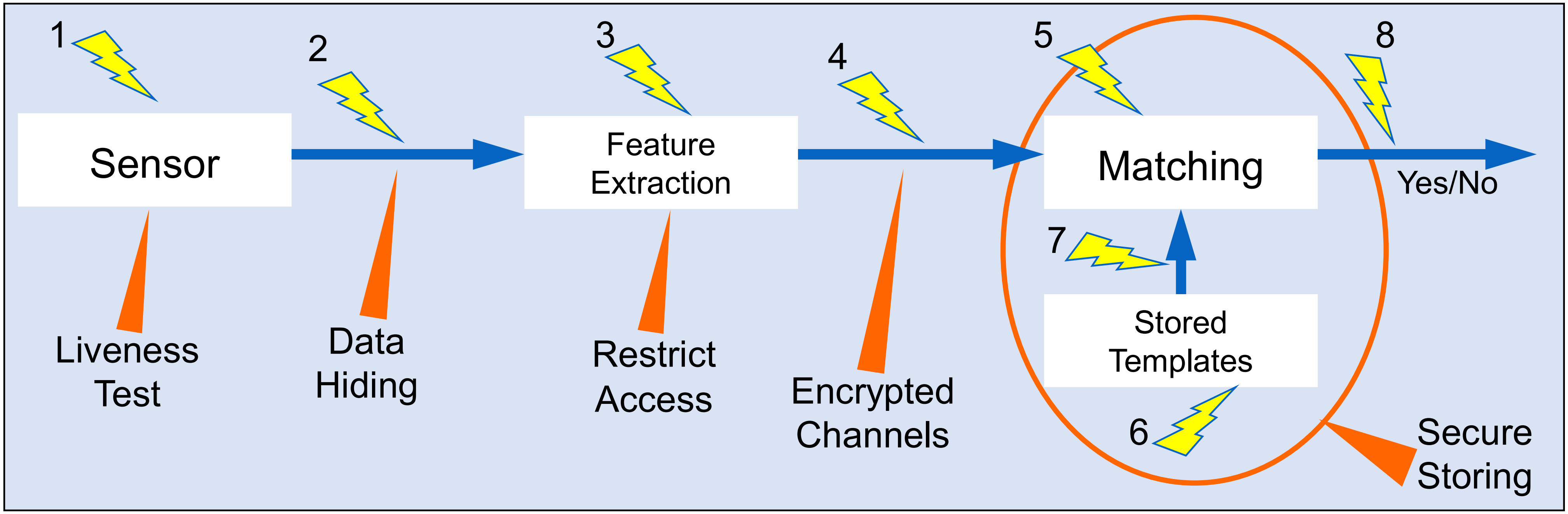
… using cards and documents



… using real time systems

Biometric Privacy: Research Directions (2)

Biometric Privacy Protection: Attack Points



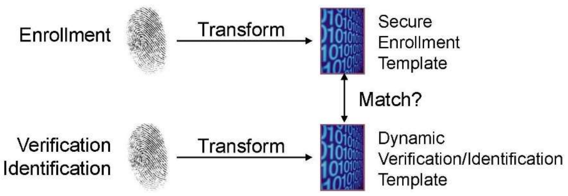
1. Fake biometrics
2. Replay attack
3. Override (Trojan Horse)
4. Tamper with features
5. Modify match score
6. Tamper with Templates DB
7. Intercept and Modify
8. Override the final decision

Biometric Privacy: Research Directions (3)

Biometric Privacy Protection: Techniques

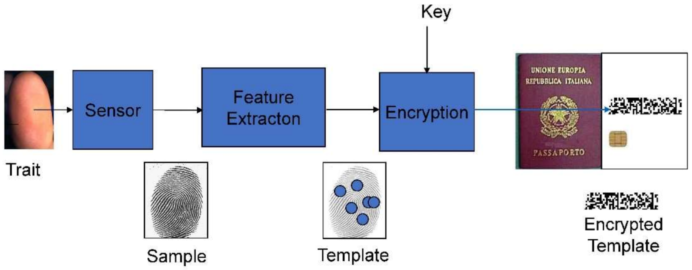
Techniques

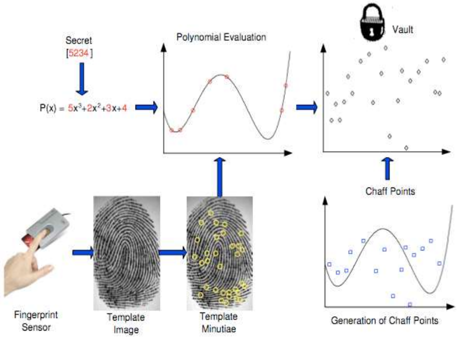
- Key-generating, Key-binding, Biometric encryption
- Feature Transformation, Helper Data Approach
- Fuzzy Commitment, Fuzzy Vault, Fuzzy Extractor
- Secure Sketch, Bio-Hashing, Revocable Bio-Token, Biotope
- Bio-Encryptor , …


Enrollment
Transform
Secure Enrollment Template
Match?
Verification Identification
Transform
Dynamic Verification/Identification Template

Research Directions

- Advanced non-invertible transformations
- Cancellable / revokable biometrics
- Advanced homomorphic encryption for processing in the encrypted domain
- AI for processing in encrypted domain
- Anonymization
- Decentralized biometric cryptosystems, …

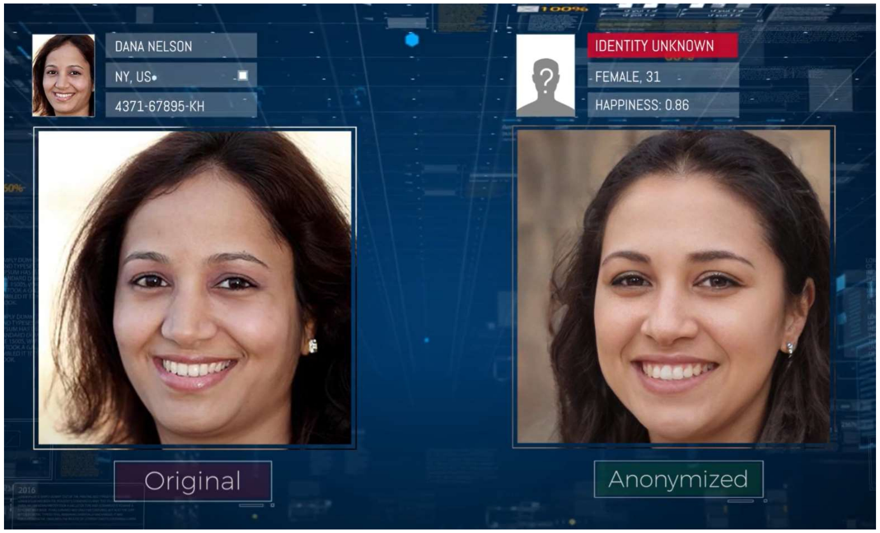


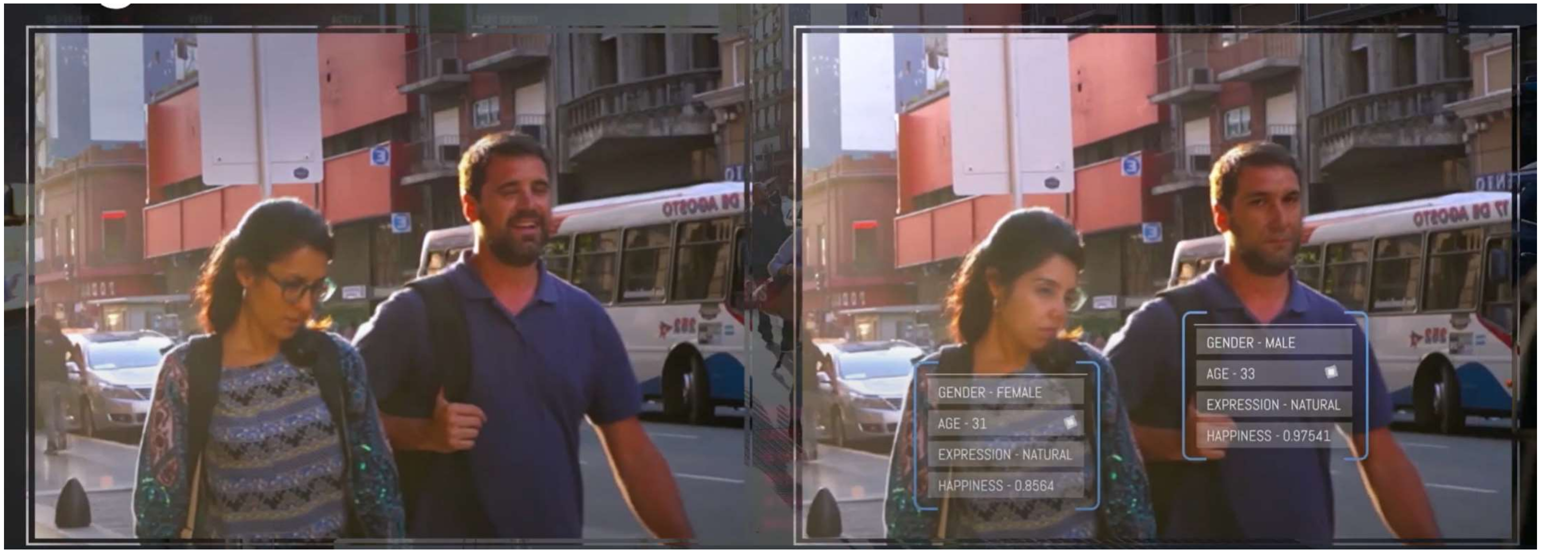


Biometric Privacy: Research Directions (4)

Image and Video Anonymization

Personally Identifiable Information can be removed by advanced computer vision, AI and deep learning, while preserving key biometric attributes

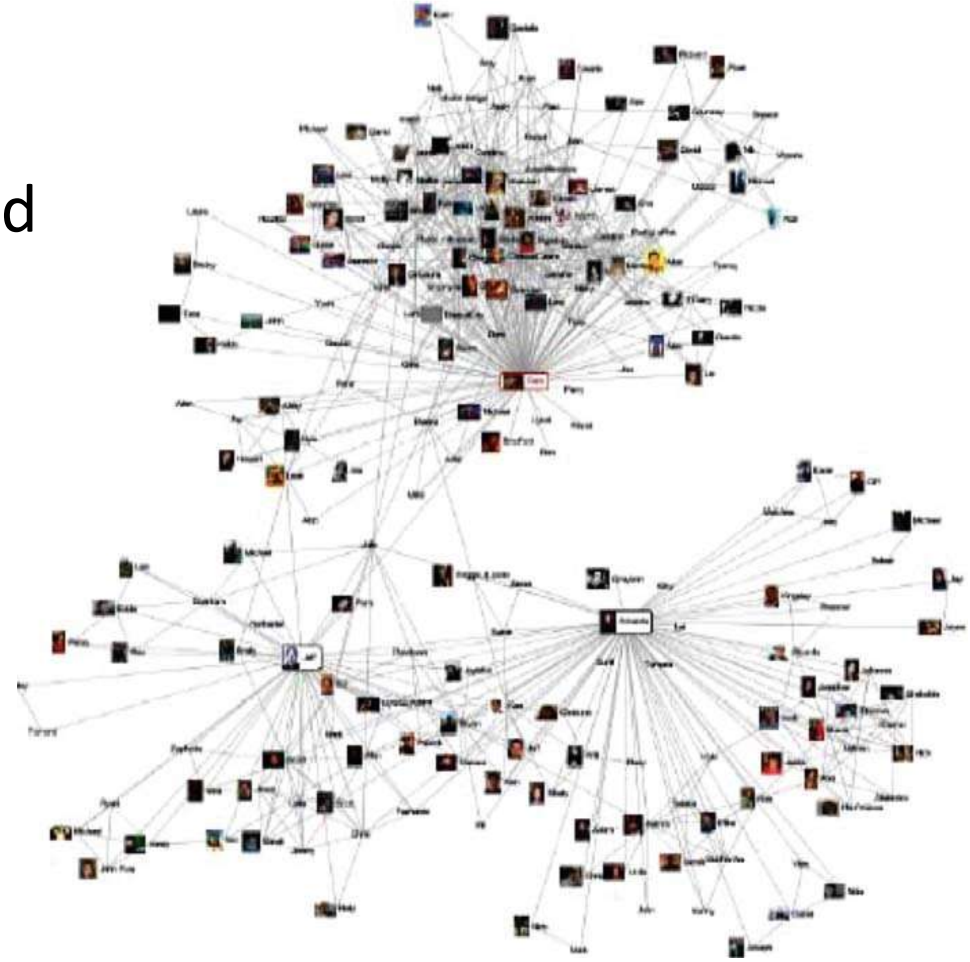


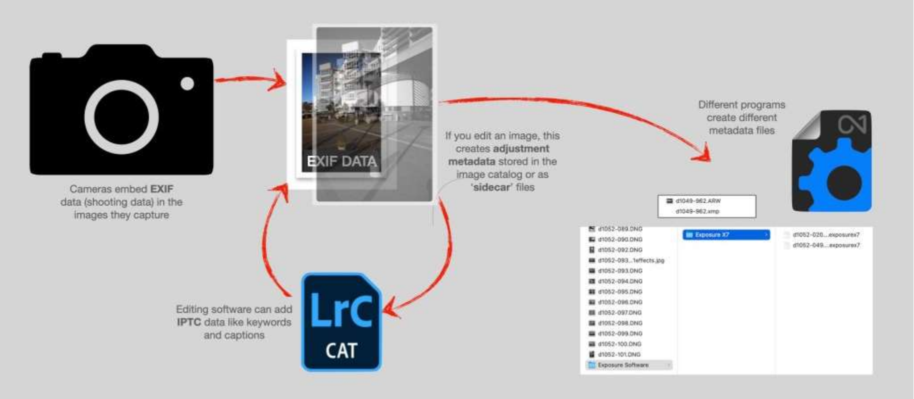


Biometric Privacy: Research Directions (5)

Social Networks

Sentiment analysis and personal sensible information can be extracted by analyzing and correlating data available in social networks





Cameras embed **EXIF** data (shooting data) in the images they capture

If you edit an image, this creates **adjustment metadata** stored in the image catalog or as '**sidecar**' files

Different programs create different metadata files

Editing software can add **IPTC** data like keywords and captions

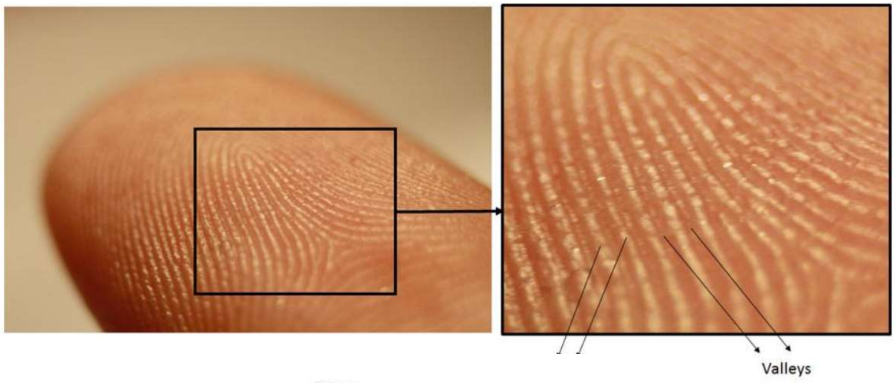
Biometric Privacy: Research Directions (6)

Personalized Interactions

- Social networks
- Sentiment analysis
- Virtual assistants
- e-commerce systems
- Market analysis
- AI-based approaches
- …

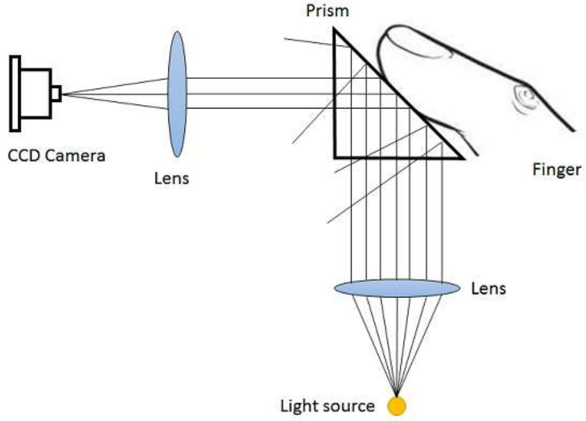
Biometric Traits and AI: Research Directions

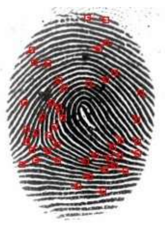
Fingerprint Recognition Methods



Capture methods

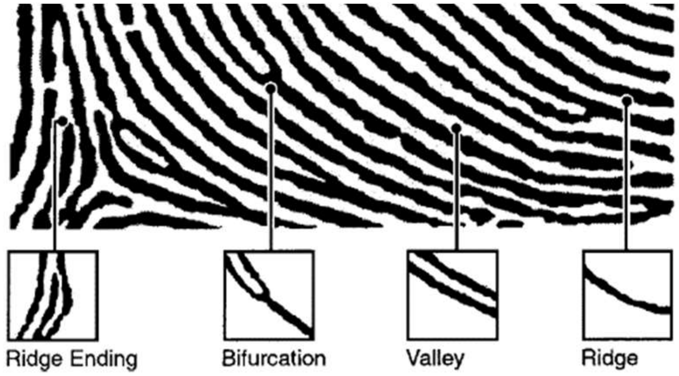
- Optical live-scan
- Solid-state live-scan
- Ultrasound live-scan





Matching algorithms

- Level 1: global ridge flow
- Level 2: minutiae points
- Level 3: fine details such as skin pores and inter-ridge information



Fingerprint Recognition: Research Directions (1)

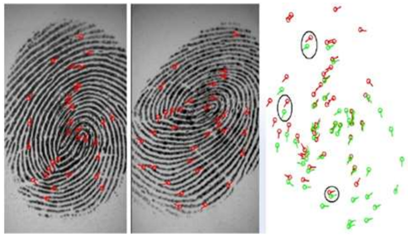
Current performance

FNMR=0.001 at FMR=0.001

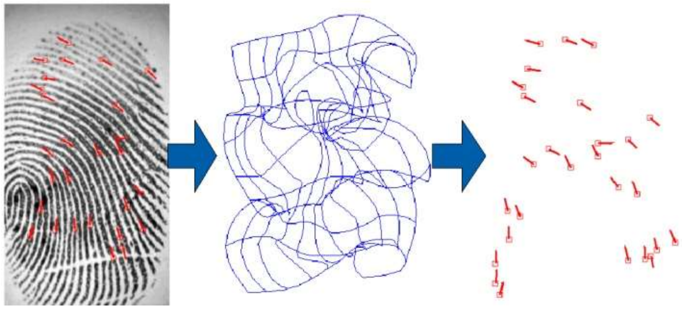
Current and future research areas

- Less-constrained acquisition
- High displacement/rotation
- Non-linear distortion
- Bad skin condition
- Feature extraction errors
- Matching millions of samples
- Exploiting extended features
- Robust orientation modeling
- Automated latent processing
- Learning based methods
- Template protection
- AI-based techniques

Non-linear distortion

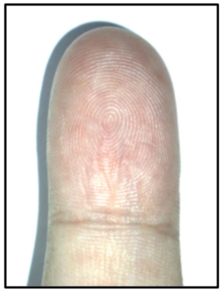


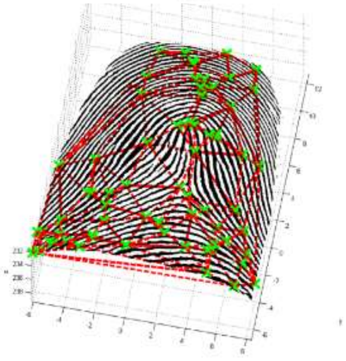
Bad skin condition



Template protection by applying gaussian transformation

Fingerprint Recognition: Research Directions (2)





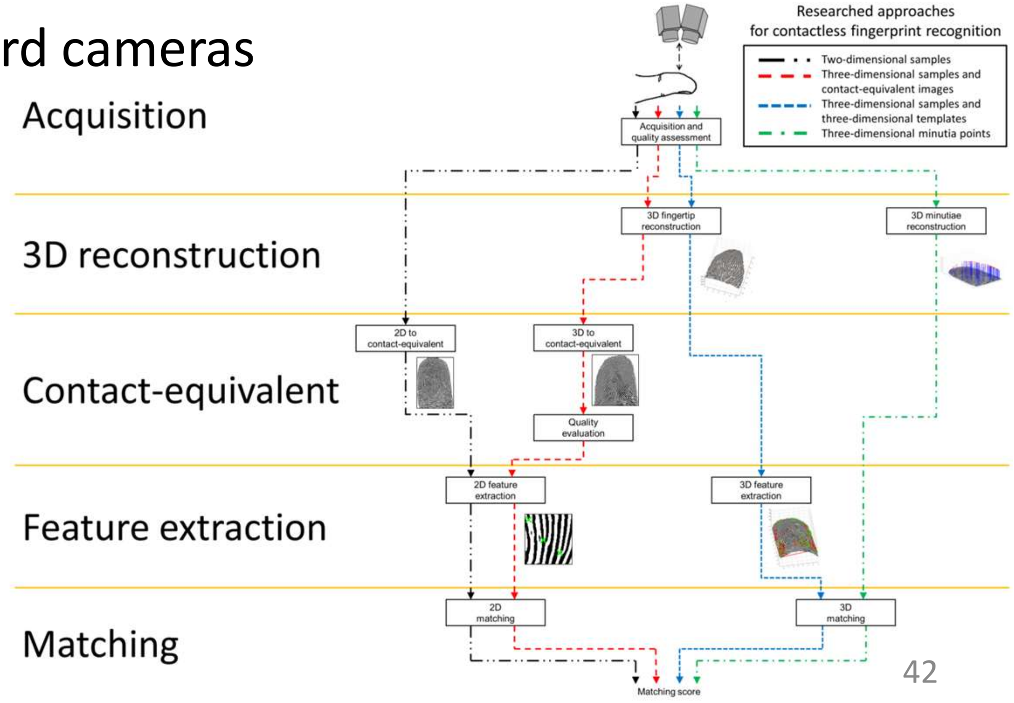
Contactless Fingerprint

Advantages

- Less-constrained
- No distortions due to pressure on sensor
- More robust to dust and dirt
- Higher user acceptance
- Use in mobile devices with standard cameras

Challenges

- Partially compatible with AFIS
- Complex background
- Sensible to lighting
- Sensible to position
- 2D systems can show distortions
- 3D systems
- Structured light
- Longer computational time



Acquisition

3D reconstruction

Contact-equivalent

Feature extraction

Matching

Researched approaches for contactless fingerprint recognition

Two-dimensional samples

Three-dimensional samples and contact-equivalent images

Three-dimensional samples and three-dimensional templates

Three-dimensional minutia points

Acquisition and quality assessment

3D fingertip reconstruction

3D minutiae reconstruction

2D to contact-equivalent

3D to contact-equivalent

Quality evaluation

2D feature extraction

3D feature extraction

2D matching

3D matching

Matching score

Face Recognition Methods

- Local or feature-based approaches

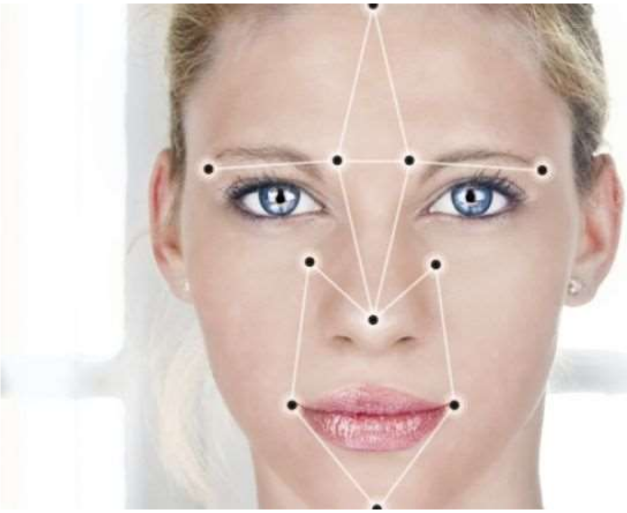
  Process the input image
  to identify and extract distinctive
  facial features such as the eyes,
  mouth, nose

- Holistic approaches

  Consider the whole face region
  for the recognition

- Hybrid approaches

  Comparable to
  the human visual
  perception



Face Recognition: Research Directions (1)

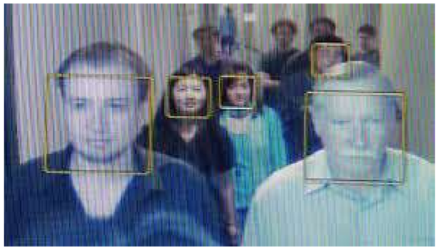
Current performance

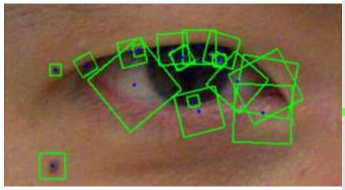
FNMR=0.003 @ FMR=0.001

outperform humans

Current and future research areas

- Less-constrained acquisition
- Face marks
- Periocular
- Age invariance
- Face at a distance
- Face individuality
- IR face recognition
- Sketch recognition
- AI-based techniques
- …





Face Recognition: Research Directions (2)

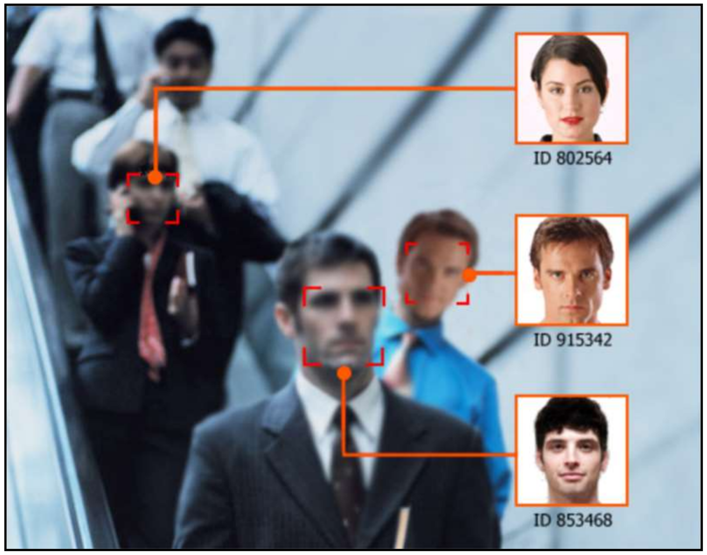
On-the-move Face

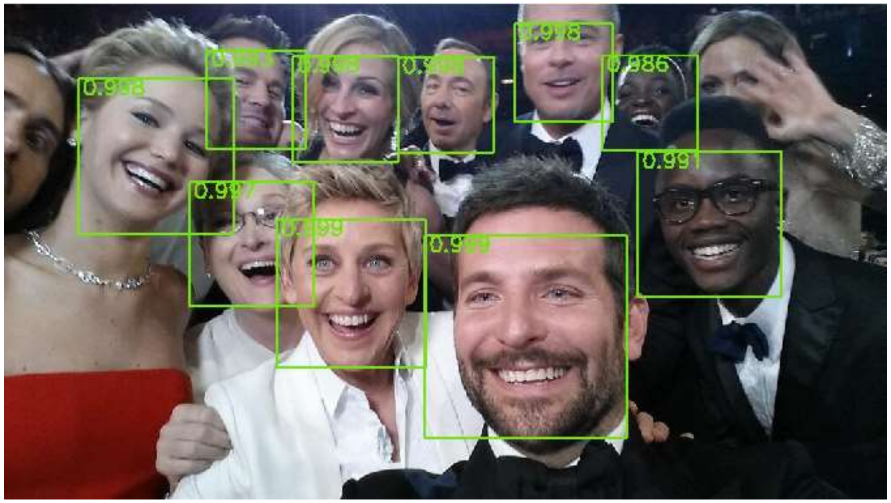
Advantages

- Less constrained
- More usability
- Increased user acceptability

Challenges

- Variability in face position
- Occlusions
- Distorsions





Iris Recognition Methods

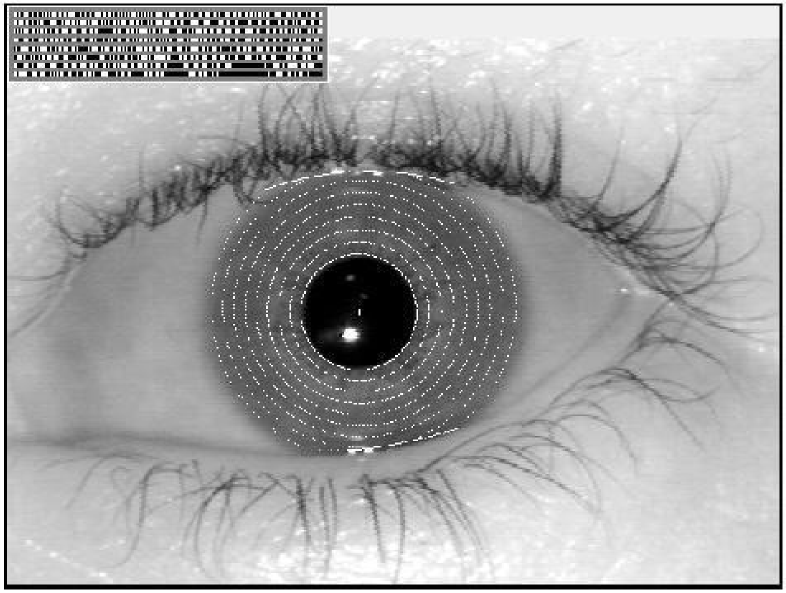
Iris acquisition

- Near infrared illumination
- Natural light

Iris segmentation

Iris coding and matching

- Daugman method
- “Eigen-Iris” approaches
- Texture filters
- Texture analysis
- Analyze the iris in parts



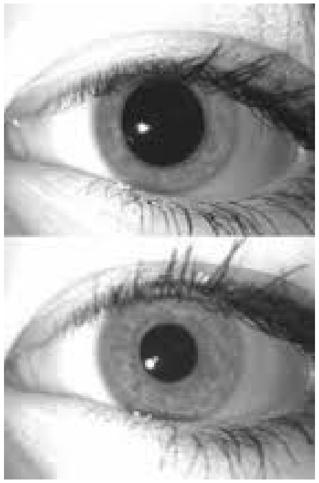
Iris Recognition: Research Directions (1)

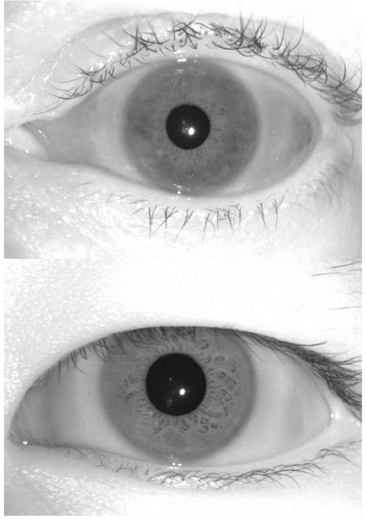
Current performance

FNMR=0.07 @ FMR=0.0001

Current and future research areas

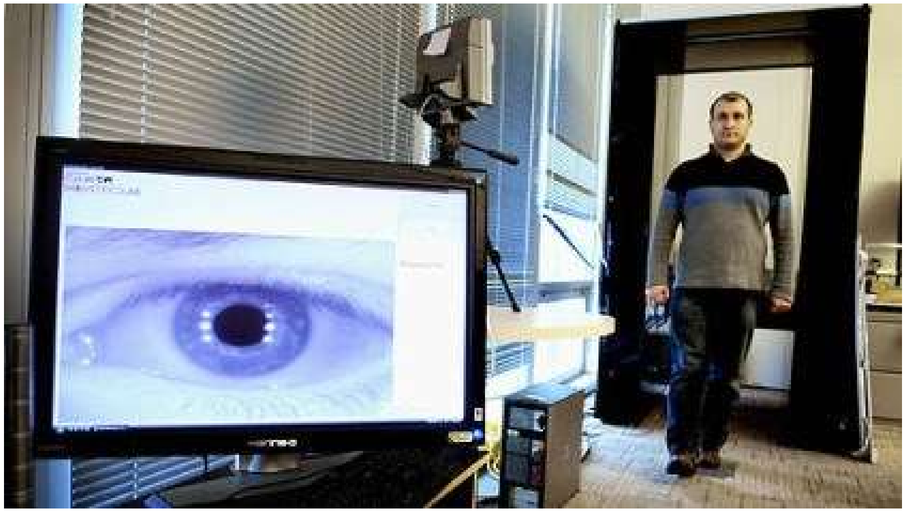
- Less constrained acquisition
- Improved segmentation
- Cancelable iris code
- Deal with pupil dilation
- Prediction of subject characteristics
- 3D retina representation
- AI-based techniques





Iris Recognition: Research Directions (2)

On-the-move Iris



Advantages

- Less constrained
- More usability
- Increased user acceptability

Challenges

- Variability in iris position
- Variability in eye position
- Occlusions
- Blur and out-of-focus

Biometrics and AI: Regulations and Research Directions

Biometric Privacy: Regulations

- European Union: General Data Protection Regulation (GDPR)
  - biometric data: special category of personal data
  - prohibit processing and storage by third parties without consent
  - prohibit processing for uniquely identifying a natural person, with exceptions (given consent, controller’s obligations, other laws, individual's vital interests, critical in legal claims, public health)
  - clear scope and capabilities of the system
  - ensure user control of personal data: right to be forgotten
  - disclosure and accountability: data breach must be notified within 72 hours
  - auditing
  - privacy by design and by default
- U.K.: UK GDPR – regulation compliant with GDPR
- California: California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- New York and Virginia follow California
- China: Personal Information Protection Law (PIPL)
- U.S.A. at federal level and India are considering regulations

AI: Regulations (1)

- European Union: EU AI Act
  - Unacceptable risk
    - Cognitive behavioral manipulation of people or specific vulnerable groups, social scoring, biometric identification and categorization of people, real-time and remote biometric identification systems (exceptions may be allowed for law enforcement purposes)
  - High risk
    - AI systems that negatively affect safety, AI systems that negatively affect fundamental rights.
  - Transparency requirements
    - Disclosing that the content was generated by AI, designing the model to prevent it from generating illegal content, publishing summaries of copyrighted data used for training
  - Supporting innovation
- USA: sector-specific AI-related agencies and organizations (e.g., Federal Trade Commission, National Highway Traffic Safety Administration, CCPA) address specific challenges.
- China: Chinese Cybersecurity Law and New Generation AI Development Plan provide measures for data protection and cybersecurity in AI.
- Canada: Pan-Canadian AI Strategy advocates for the responsible development of AI. Personal Information Protection and Electronic Documents Act regulates collection, use, and disclosure of individuals’ personal information using AI technologies.

AI: Regulations (2)

- Australia: National Artificial Intelligence Ethics Framework directs ethical principles in AI systems’ development and implementation process.
- International organizations:
  - Organization for Economic Co-operation and Development (OECD) and United Nations are involved in setting and outlining global guidelines on AI regulation (OECD’s AI Principles, United Nations Sustainable Development Goals).
- General principles of regulations:
  - *Ethical principles*: to uphold ethical principles, including transparency, fairness, and accountability, to guarantee responsible AI development and use.
  - *Data privacy*: to incorporate guidelines on how AI should collect, use, and protect personal data to eliminate privacy fears.
  - *Algorithmic bias*: measures to eliminate algorithmic bias and allow for fair and unbiased AI decision-making.
  - *Transparency and explainability*: AI systems should be transparent and easy to understand and enable users to understand how decisions are made and be accountable.
  - *International collaboration*: governments should cooperate with international bodies to ensure unified regulations that address global problems.

Ethics in AI for Biometrics

- *Do not harm*: avoid actions that harm people or the environment.
- *Collection*: explicit consensus and clarity in collection purpose.
- *Identity theft*: do not breach systems, steal biometric data that are ineffectively secured, and impersonate individuals.
- *Respect personal data*: when shared, stored, and processed, personal data must be respected and treated with care.
- *Misuse*: biometric data used only for collection-declared purpose.
- *Justice and accountability*: biometrics should be open, transparent, and accountable.
- *Technology quality*: biometric technology should benchmark quality, including accuracy, error detection, repair systems, and protection.
- *Human rights*: applications and use should align with human rights.
- *Equality*: biometric technology should not discriminate based on religion, age, gender, race, sexuality, or others.

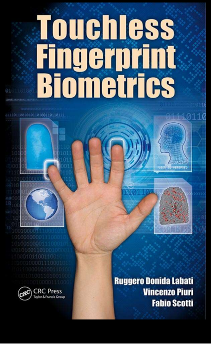
Artificial Intelligence for Biometrics

Vincenzo Piuri

Università degli Studi di Milano

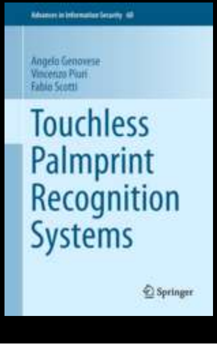
vincenzo.piuri@unimi.it

https://piuri.di.unimi.it


Touchless Fingerprint Biometrics

Ruggero Donida Labati
Vincenzo Piuri
Fabio Scotti

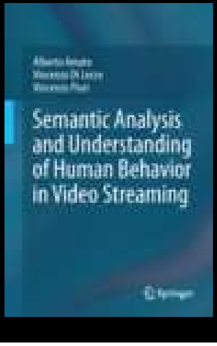
CRC Press
Taylor & Francis Group


Advances in Information Security 60

Angelo Genovese
Vincenzo Piuri
Fabio Scotti

Touchless Palmprint Recognition Systems

Springer


Alberto Amato
Vincenzo Di Lecce
Vincenzo Piuri

Semantic Analysis and Understanding of Human Behavior in Video Streaming

Springer

Francesco Bellocchio · N. Alberto Borghese
Stefano Ferrari · Vincenzo Piuri

3D Surface Reconstruction

Multi-Scale Hierarchical Approaches

Springer

EdgeAI GLACIATION SERICS SECURITY AND RIGHTS IN THE CYBERSPACE