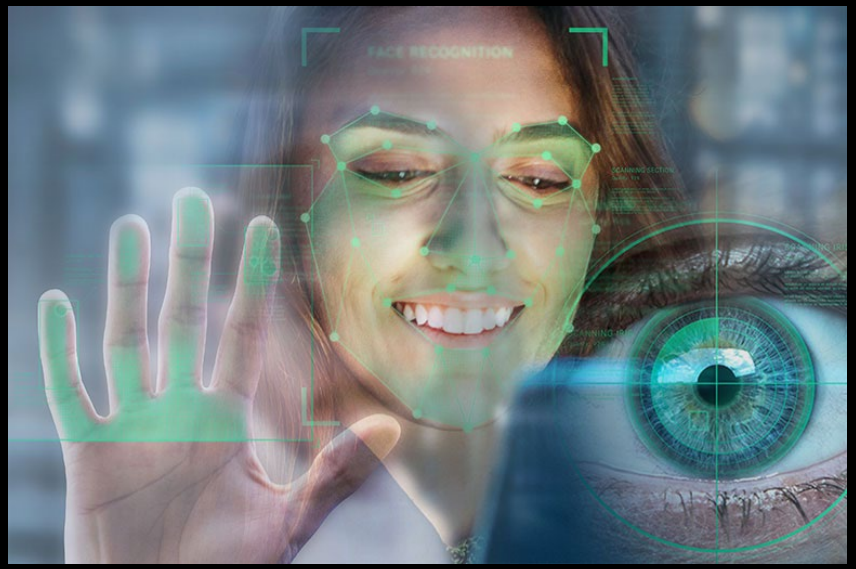


Biometrics: technologies, challenges, and research directions

Vincenzo Piuri

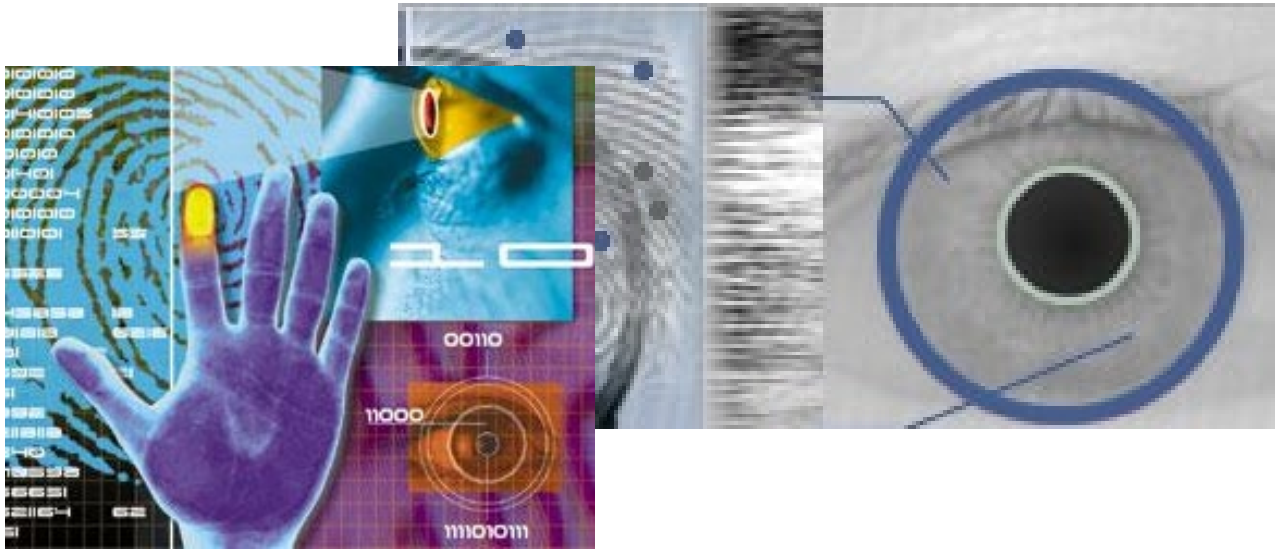
Università degli Studi di Milano

vincenzo.piuri@unimi.it

https://piuri.di.unimi.it

EdgeAI GLACIATION SERICS

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**"

Autenthication Techniques

Verification vs Identification

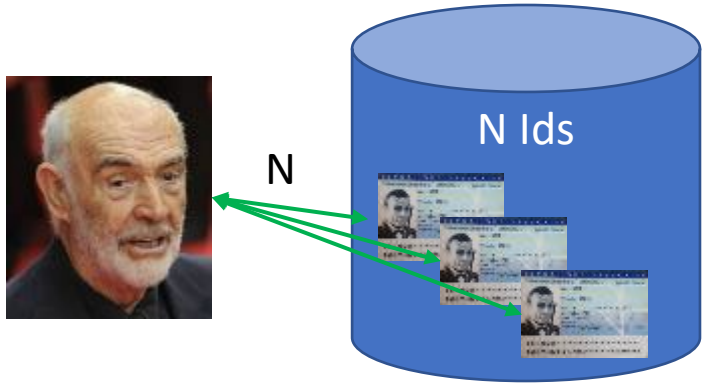
Verification (Autentication):
Am I who I say to be?

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

Identification: *Who am I?*

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

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



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

Biometrics Offers Positive and Negative Recognition

POSITIVE Verification or Identification
Determine with high accuracy that the user is who he says she/he is.

- Preventing the use of a **single** identity by *multiple* people

NEGATIVE Verification or Identification
Determine with high accuracy that user is NOT who he says she/he is.

- Preventing the use of *multiple* identities by a **single** person
- The **black/watch list** case: "You are not in the list" = Negative Identification

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

Surveillance

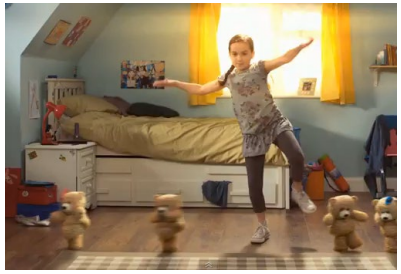
- Buildings
- Public areas
- …

Logical Access Control to Services

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

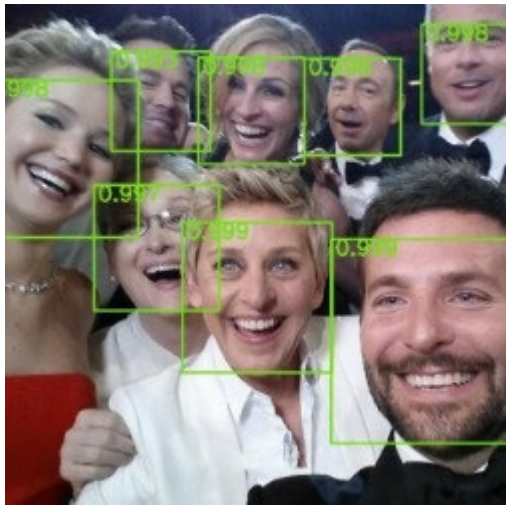
Smart Environments

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



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
- …



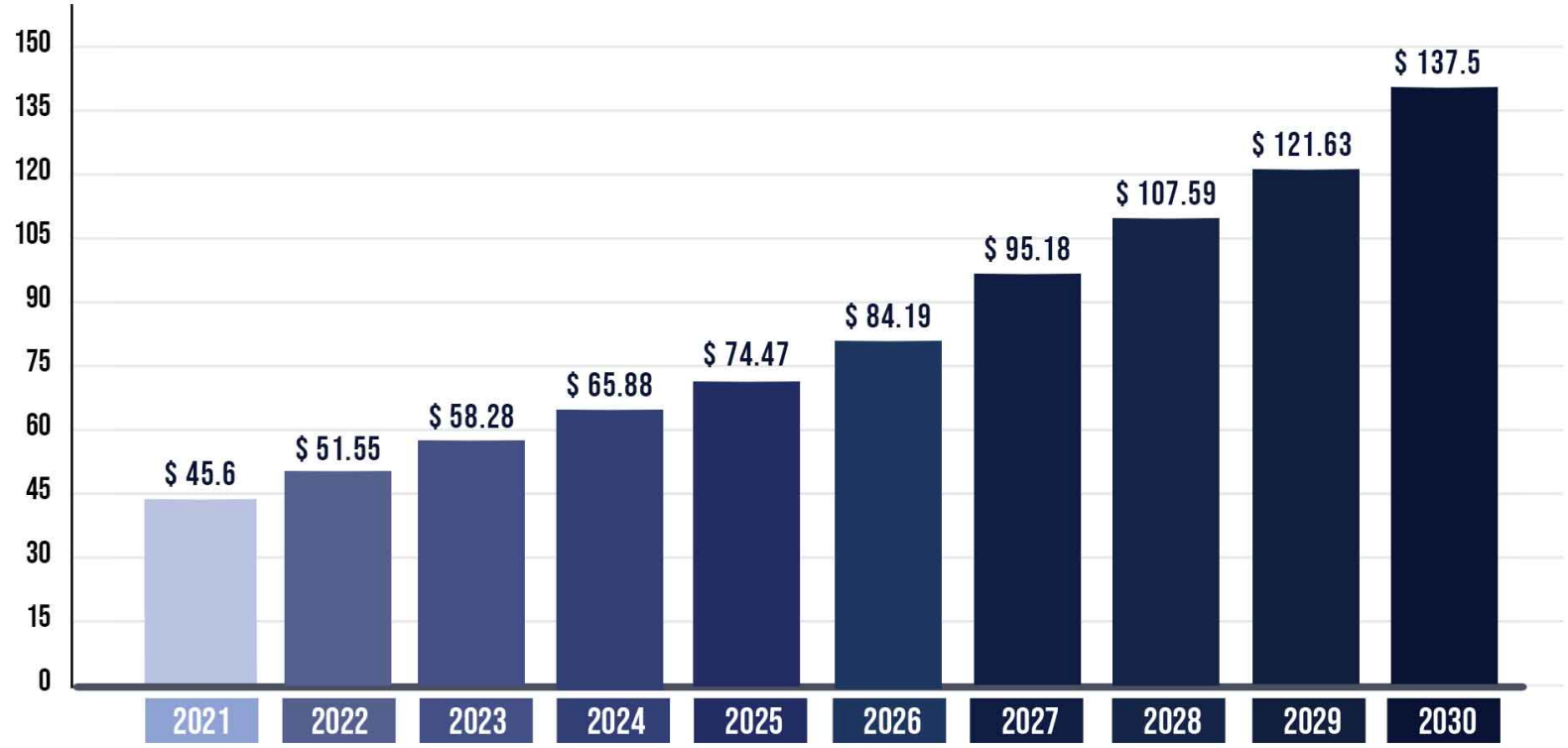
Humanitarian and Forensics Applications

- Recognition of victims
- Refugee protection
- Welfare and food distribution
- Prevention of human trafficking
- Prevention of terrorism
- …

Market Trend (1)

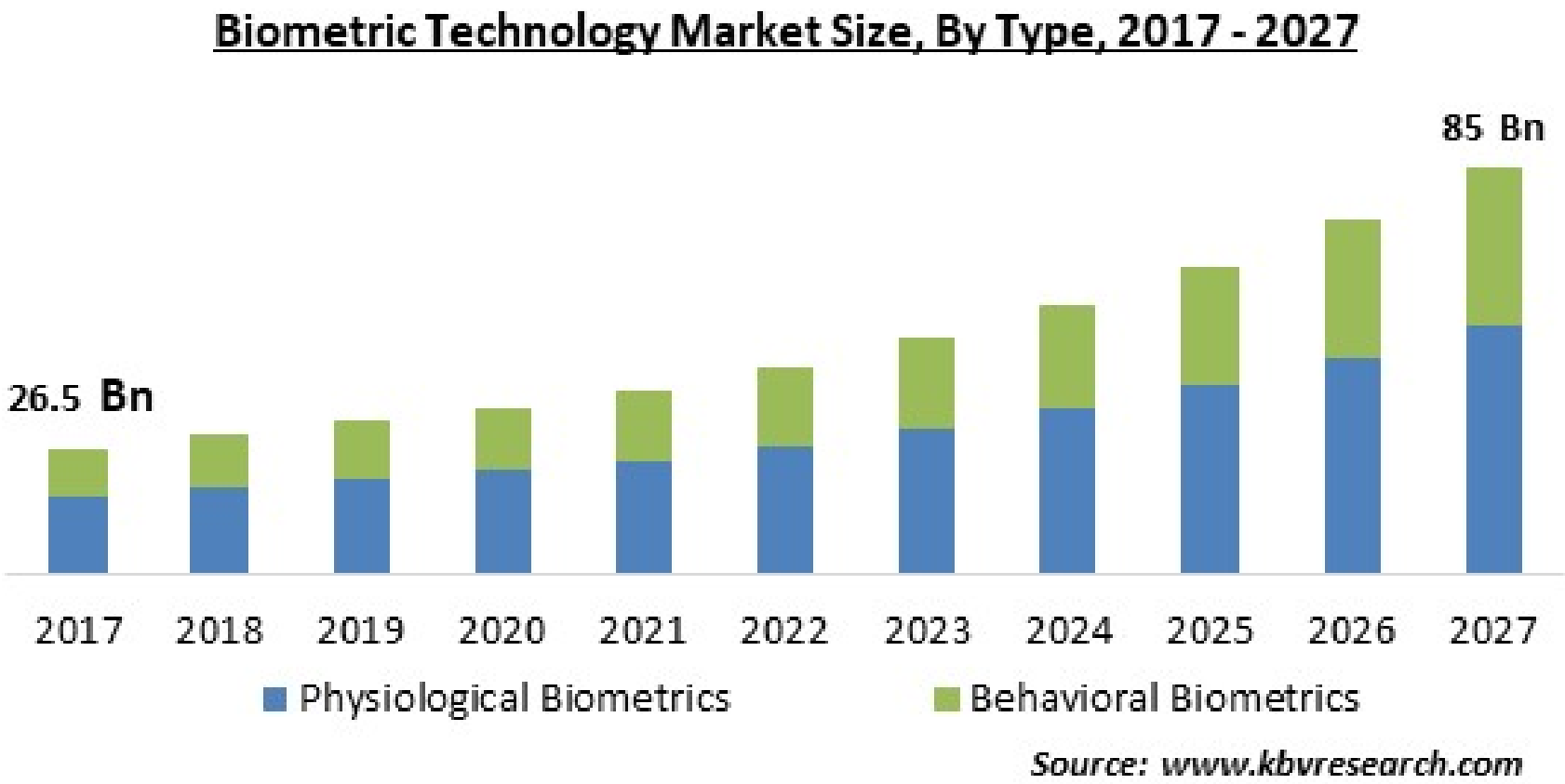
PRECEDENCE RESEARCH

BIOMETRIC TECHNOLOGY MARKET SIZE, 2021 TO 2030 (USD BILLION)



Source: www.precedenceresearch.com

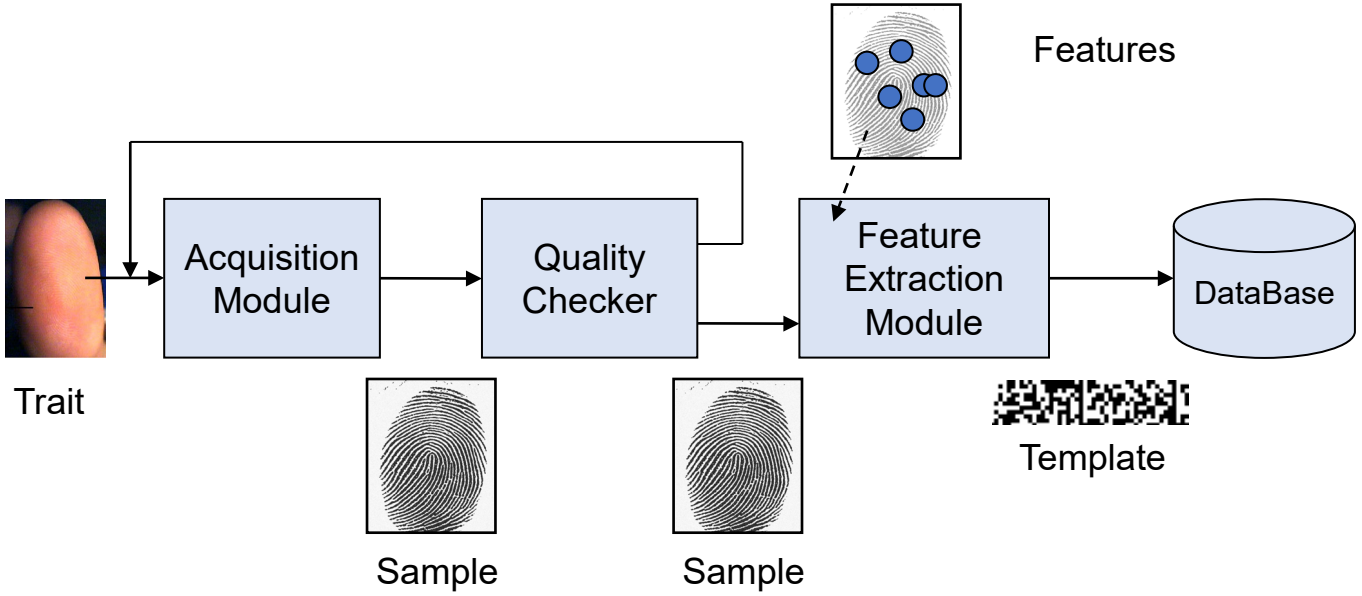
Market Trend (2)



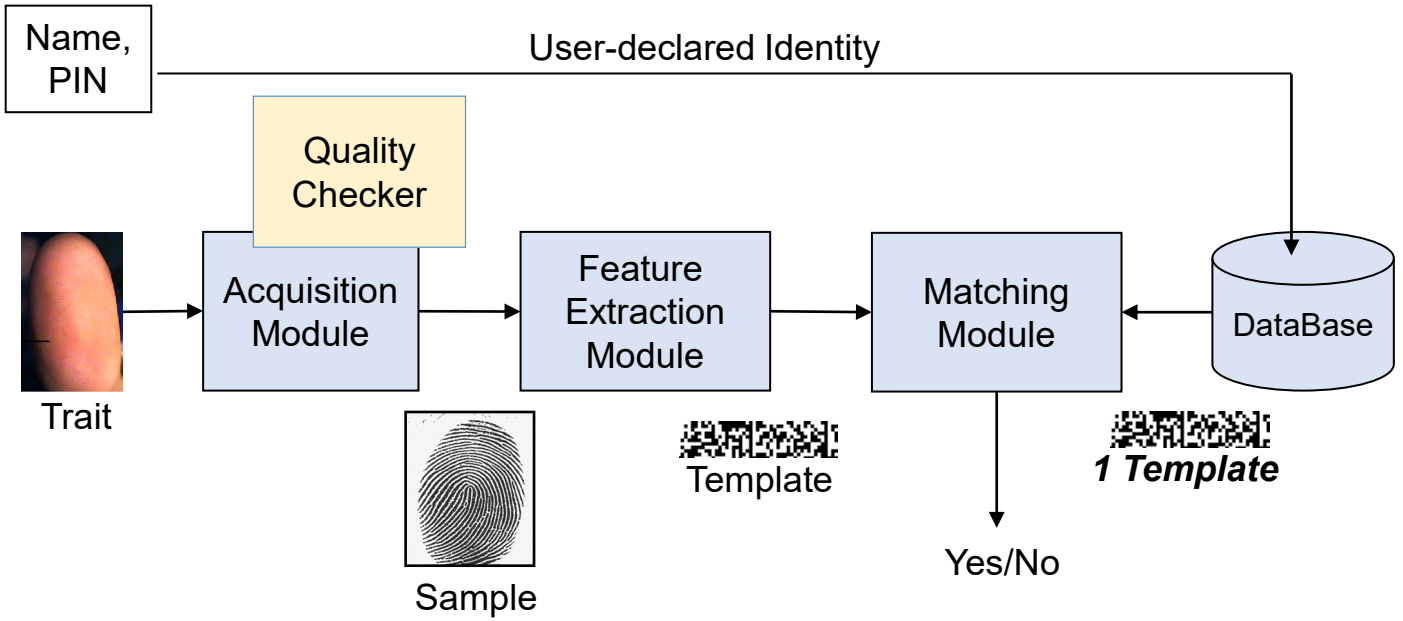
Biometric Systems Operation

Enrollment

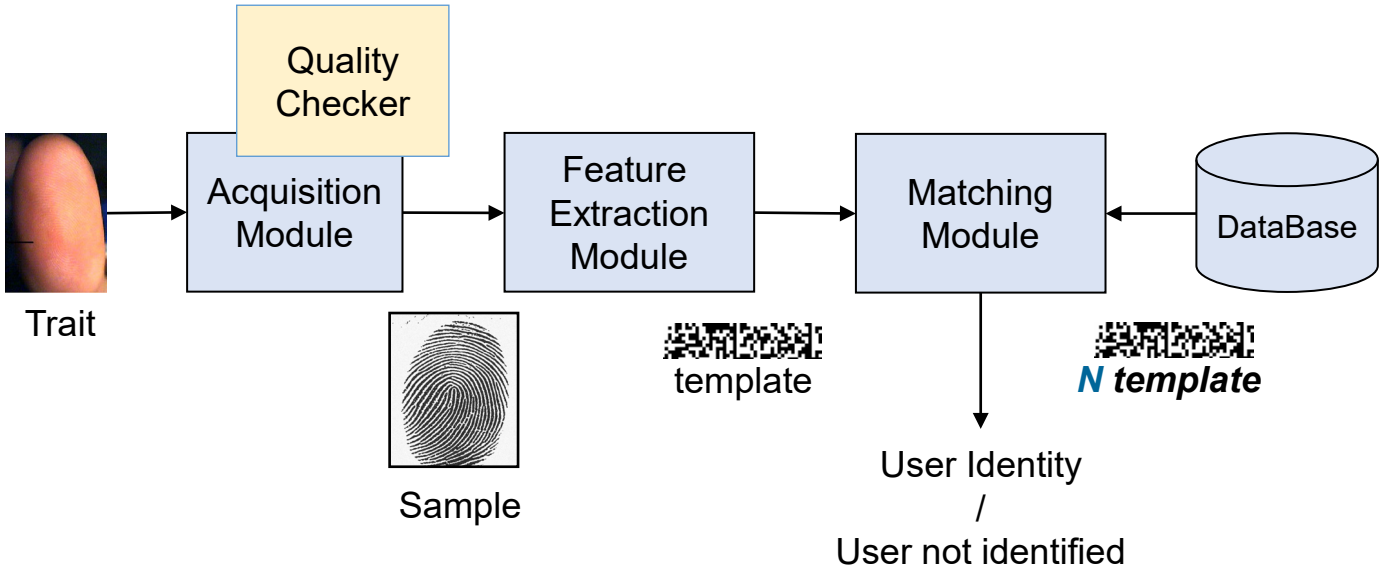
Biometric trait → Template → DataBase



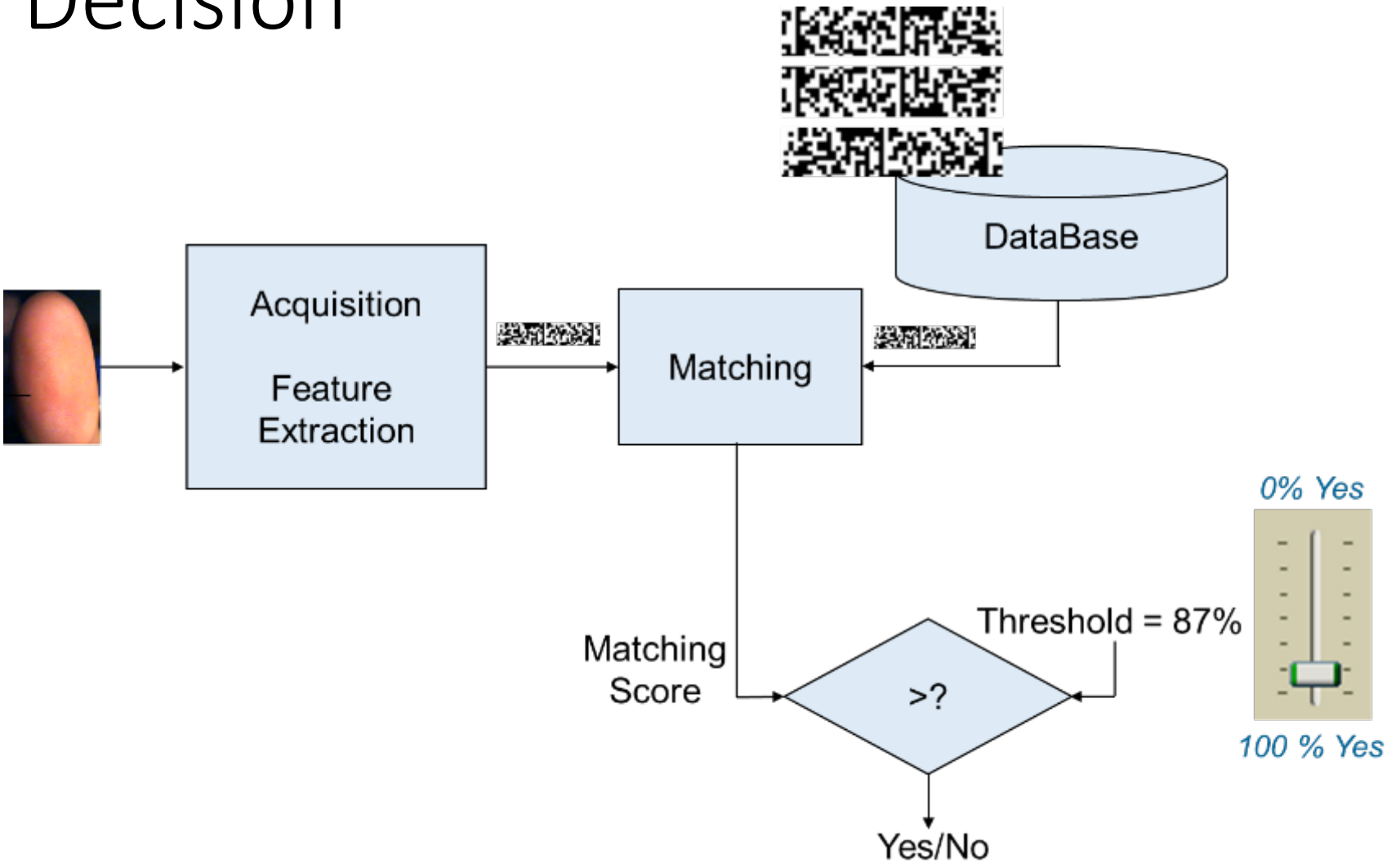
Verification



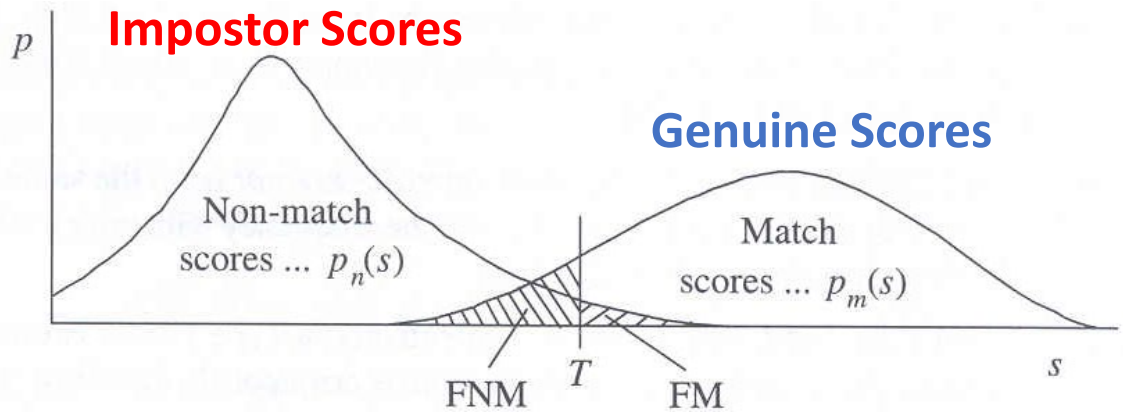
Identification

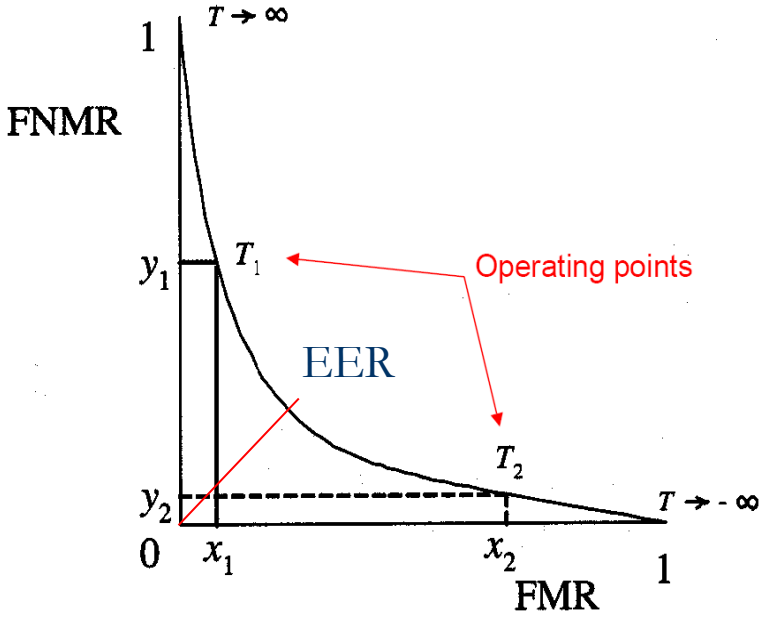


Decision


DataBase
Acquisition
Feature
Extraction
Matching
Matching
Score
>?
Threshold = 87%
0% Yes
100 % Yes
Yes/No

Impostor and Genuine Recognition



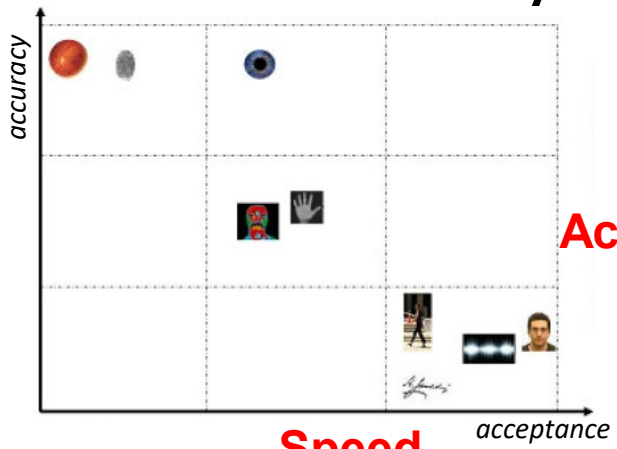


False Match Rate (***FMR***)

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

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

Biometric Systems Evaluation

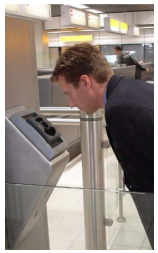


Social Acceptance

High
Medium
Zero

Accuracy

99.9999
99.99
99.0

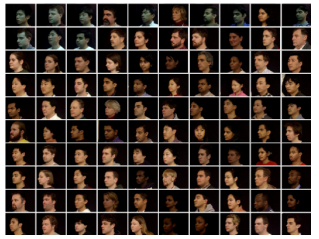


Speed

10000
100
1

Scalability

10000
100
20

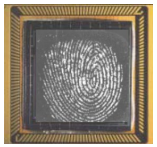


Interoperability

1 type
6 types

Usability

Simple
Complex



Cost

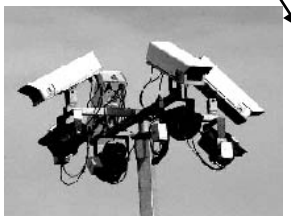
100
10000

Security

Medium
High

Privacy

Medium
High

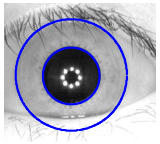


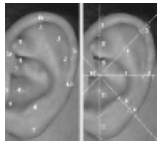
Biometric Traits and Biometric Research Directions

Biometric Traits

Physiological

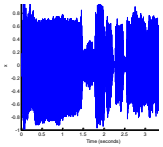
- Fingerprint
- Face
- Iris
- Palm
- Retina
- Hand geometry
- Hand veins
- Ear
- DNA
- ECG
- EEG
- …





Behavioral

- Voice
- Signature
- Keystroke
- Gait
- Gesture
- Emotion
- …

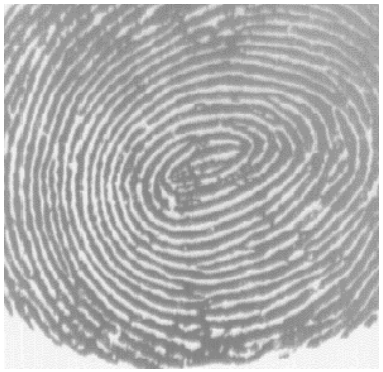


Fingerprint

- Oldest and most widespread used trait
- Fingerprint is a pattern of ridges and valleys that develops from a causal configuration already present from embryo
- Can be found on the fingers, palms and underfoot
- They are believed to be unique (based on current knowledge)
- The pattern does not change in time

Two fingerprints of the same person

Fingerprints of two different persons!



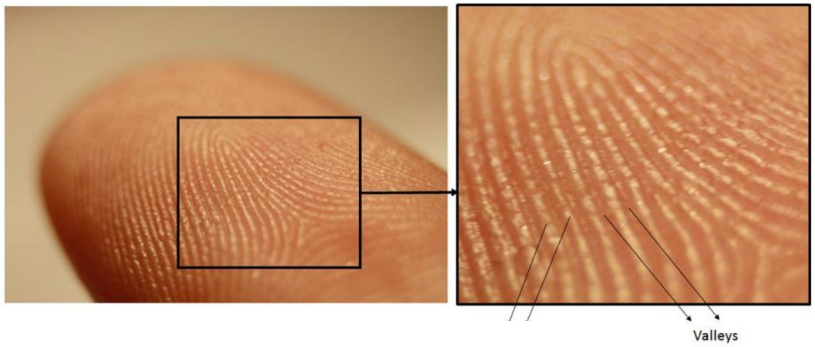
Fingerprint Recognition Methods

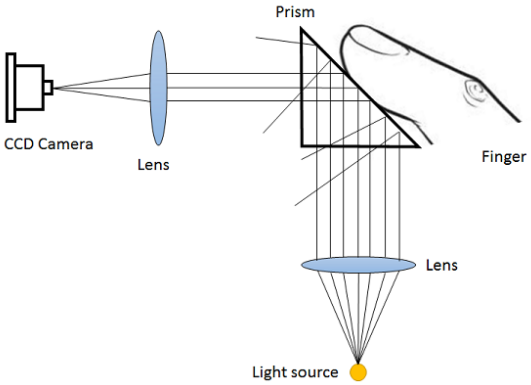
Capture methods

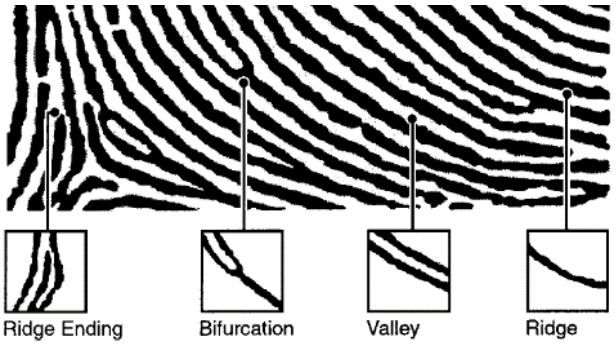
- Optical live-scan
- Solid-state live-scan
- Ultrasound live-scan

Matching algorithms

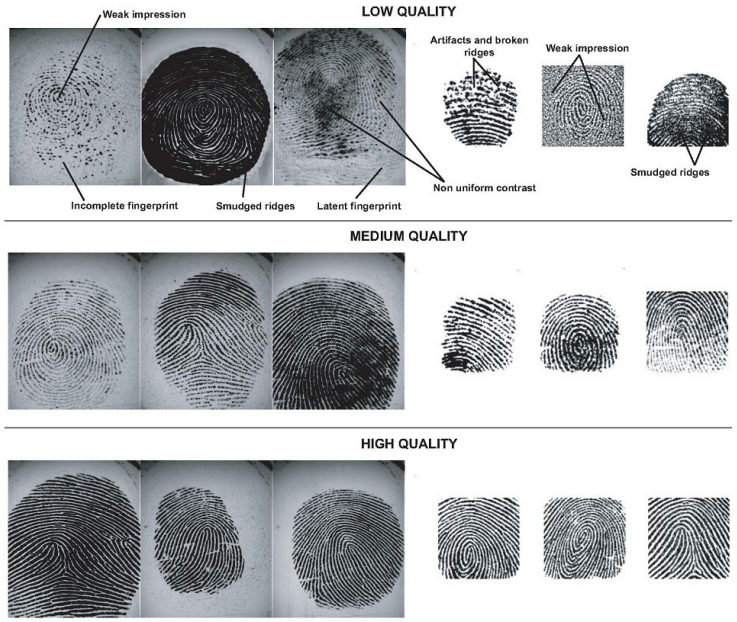
- Level 1: global ridge flow
- Level 2: minutiae points
- Level 3: fine details such as skin pores and inter-ridge information







Fingerprint Image Quality

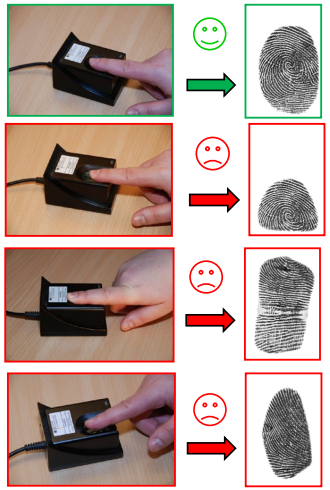


Local image defects

- Partially merging ridges
- Low contrast
- Few visible minutiae
- Artifacts caused by image compression
- Latent fingerprints
- Big “gaps” between the ridges
- “Linked” ridges

Factors that influence quality

- Physical factors: age, skin condition
- Behavioral factors: applied pressure, willingness to cooperate
- Environmental factors: temperature, moisture
- Operational factors: user familiarity, feedback, sensor cleaning, ergonomics



Fingerprint Recognition: Research Directions (1)

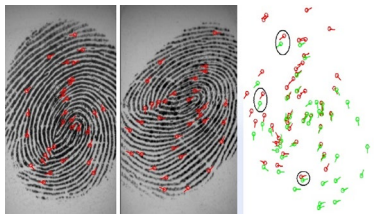
Current performance

FNMR=0.001 at FMR=0.001

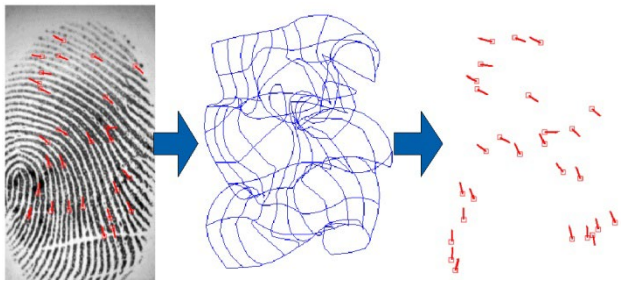
Current and future research areas

- Less-constrainted 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
- …

Non-linear distortion

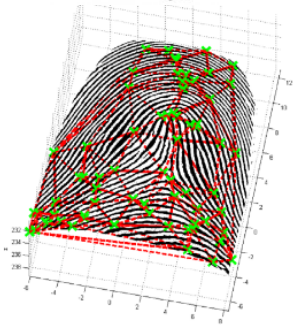


Bad skin condition



Template protection by applying gaussian transformation

Fingerprint Recognition: Research Directions (2)



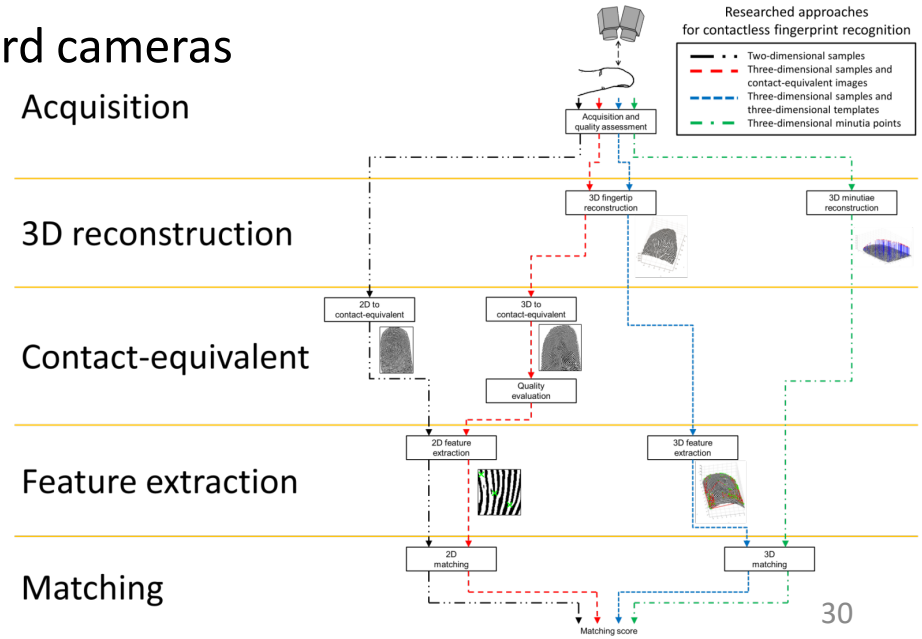
Contactless Fingerprint

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

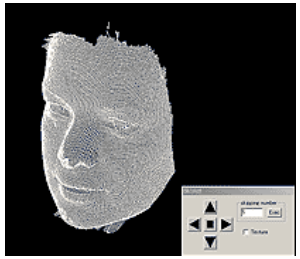
Challenges

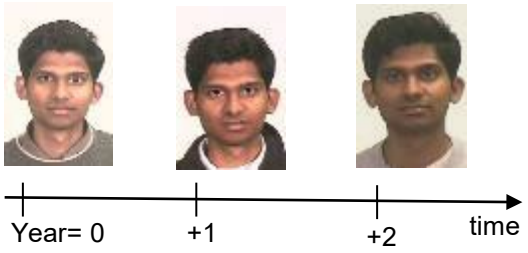
- Partially compatible with AFIS
- Complex background
- Sensible to lighting
- Sensible to position
- 2D systems can show distortions
- 3D systems
- Structured light
- Longer computational time



Face

- Among the least intrusive biometric trait
- Normally used by people to recognize each other
- Sensors: cameras, video / webcam, smartphones, PC, 3D scanner
- Challenges
  - Change in time (aging)
  - Lights and backgrounds change
  - Facial expression
  - Different poses
  - Occlusions





Face Recognition Methods

- Local or feature-based approaches

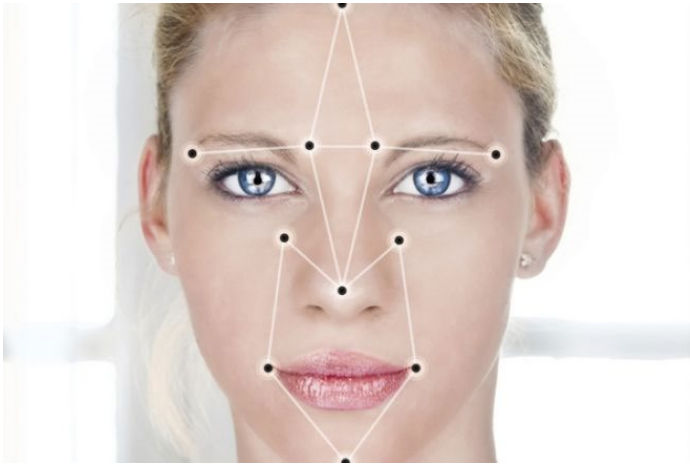
  Process the input image to identify and extract distinctive facial features such as the eyes, mouth, nose

- Holistic approaches

  Consider the whole face region for the recognition

- Hybrid approaches

  Comparable to the human visual perception



Face Image Quality

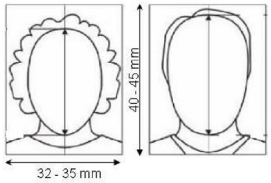


Image dimensions

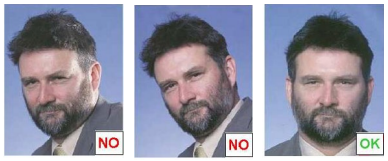
Too close Too far

Damaged or stained

Faded Pointed

Shadow in background Shadow in face

Other subject Objects



Artistic pose Tilted face

Not centered

Out of focus

Too dark Too bright

Unnatural color

Red eyes

Covered face

Wearing a hat

Eyes covered by hair

Heavy frame Frame covering eyes

Dark glasses Glare on glasses

Face Recognition: Research Directions (1)

Current performance

FNMR=0.003 @ FMR=0.001

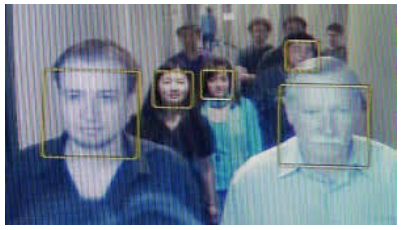
outperform humans

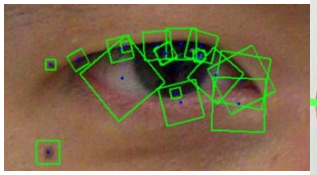
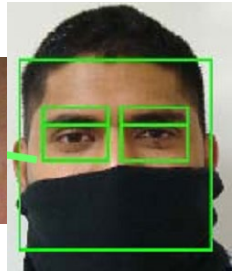
Current and future research areas

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



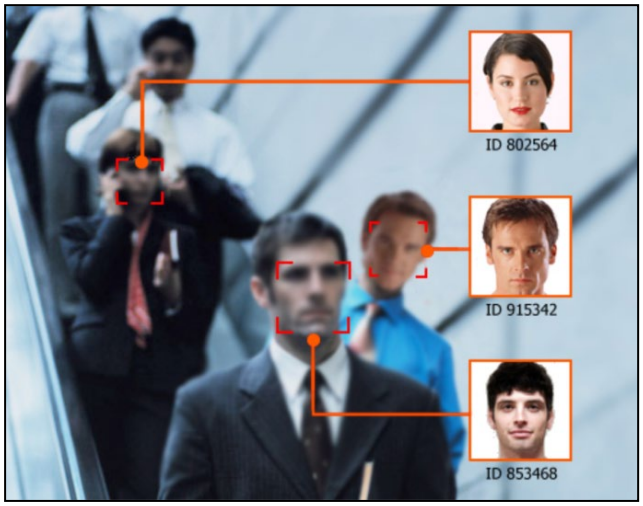




Face Recognition: Research Directions (2)

On-the-move Face

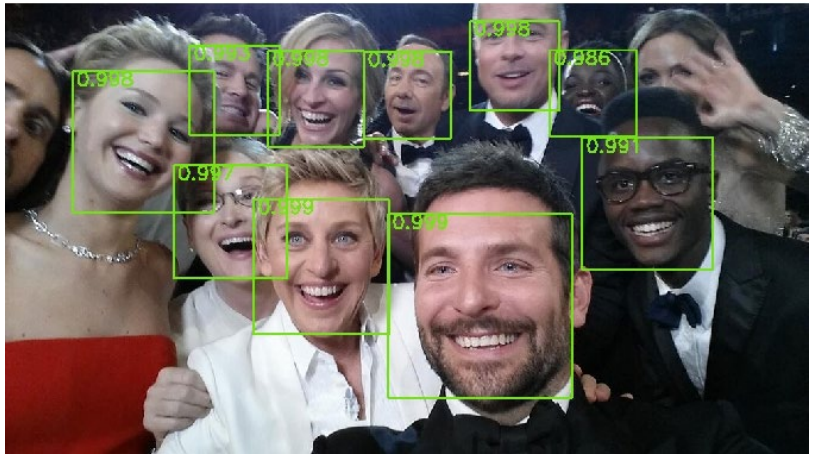


Advantages

- Less constrained
- More usability
- Increased user acceptability

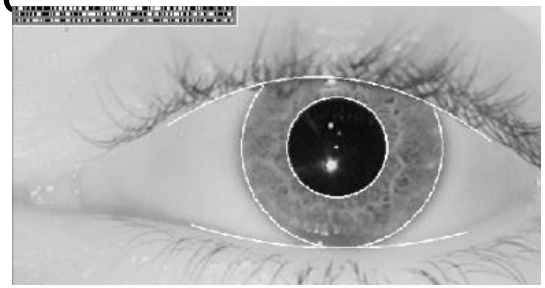
Challenges

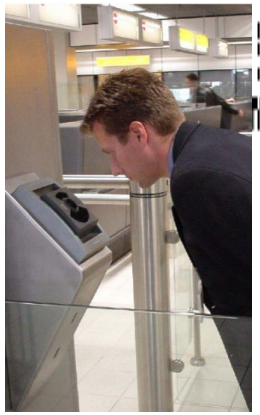
- Variability in face position
- Occlusions
- Distorsions

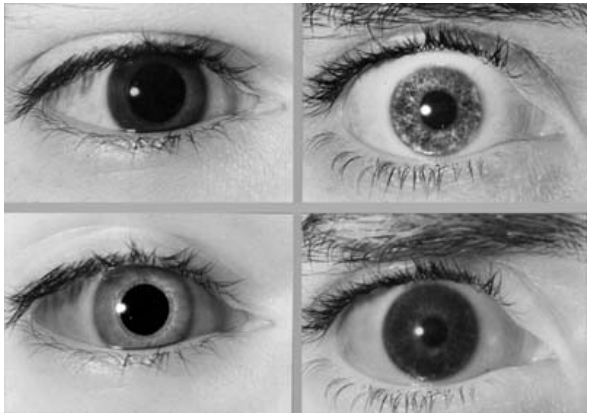


Iris

- Regarded as the most accurate biometric trait
- Numerous and stable in-time characteristics
- Stable (on average) from eight month of life
- Systems are rather complex and expensive, but hard to fraud
- Can be acquired in social media images





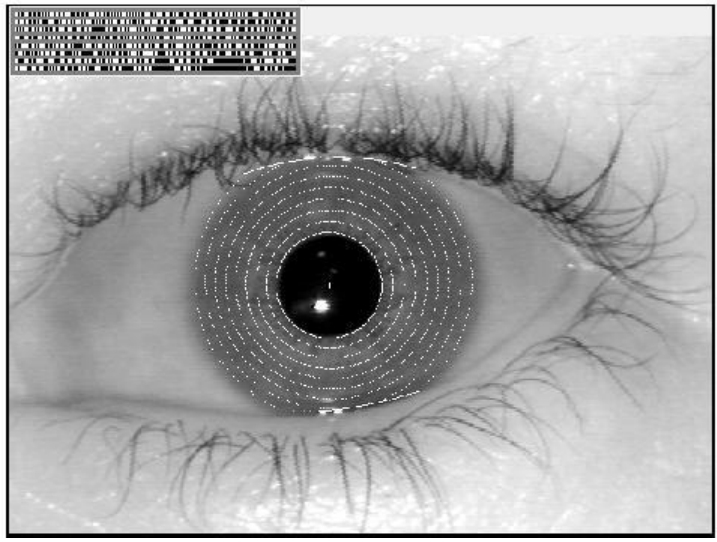


Iris Recognition Methods

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 Image Quality

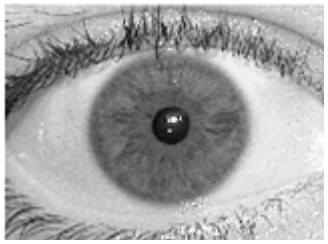
Quality factors

- Environmental
- User behavior

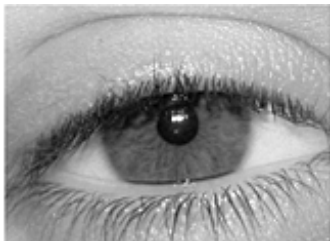
Assessment methods

- Iris Segmentation Scores
- Interlacing
- Blur
- Illumination
- Lighting
- Occlusion
- Pixel Count
- Dilation
- Off-angle

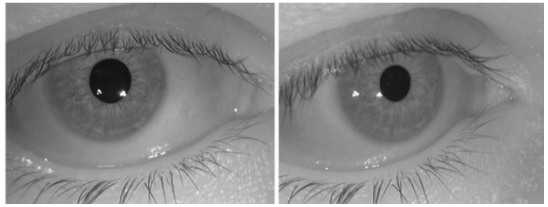
High quality



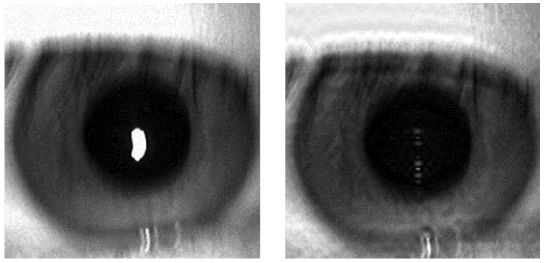
Occluded



Off-angle



Blur



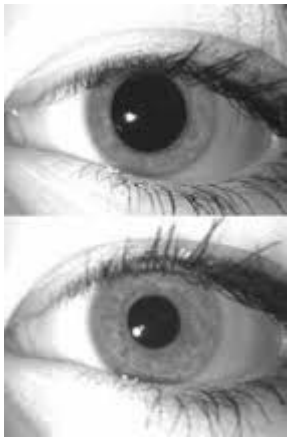
Iris Recognition: Research Directions (1)

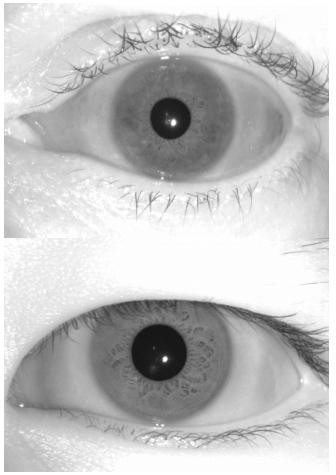
Current performance

FNMR=0.07 @ FMR=0.0001

Current and future research areas

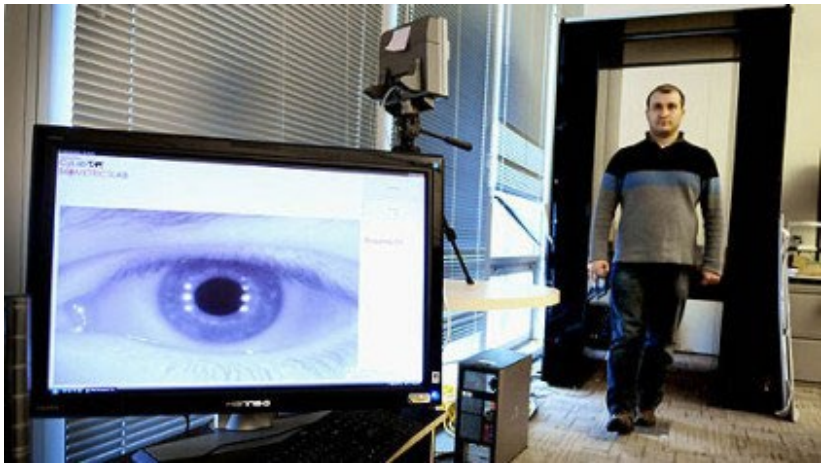
- Less constrained acquisition
- Improved segmentation
- Cancelable iris code
- Deal with pupil dilation
- Prediction of subject characteristics
- 3D retina representation





Iris Recognition: Research Directions (2)

On-the-move Iris



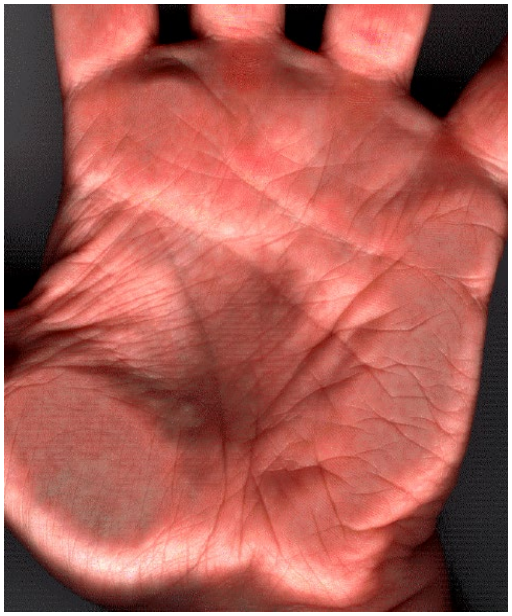
Advantages

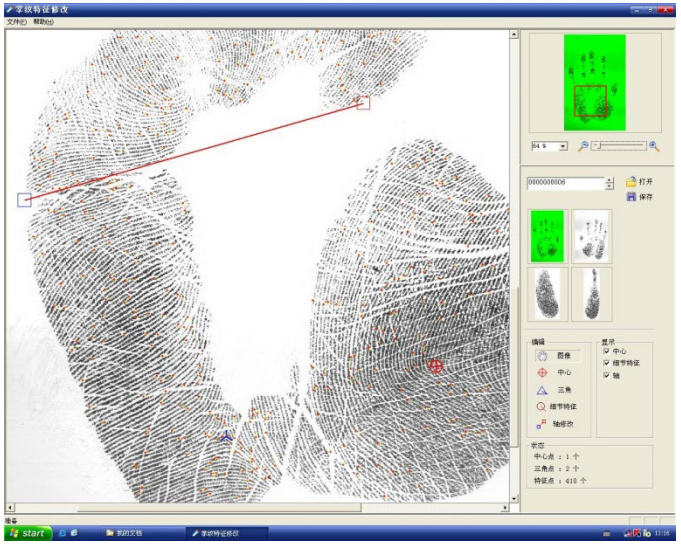
- Less constrained
- More usability
- Increased user acceptability

Challenges

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

Palm Print





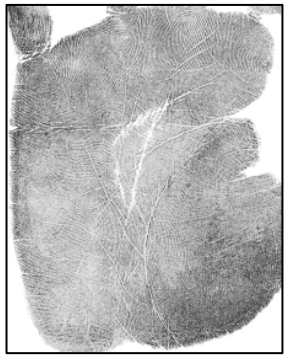
Contactless Palmprint

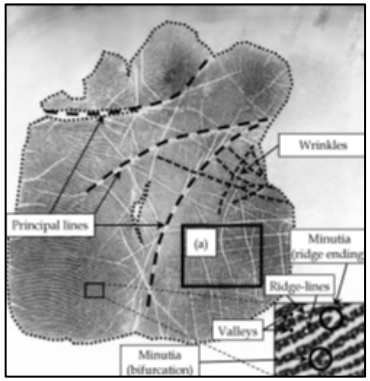
Advantages

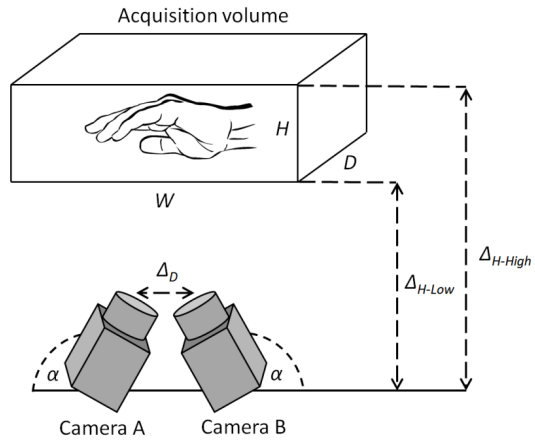
- Less-constrained
- Low resolutions (< 200 dpi)
- Increased user acceptability
- More robust: distortion, dirt

Challenges

- High accuracy features not always usable
- Low contrast
- Complex background
- Sensible to lighting
- Sensible to position



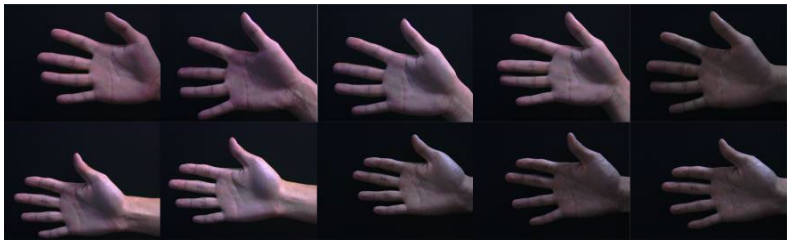




Recognition algorithms

- Ridge based
- Line based
- Subspace based
- Statistical
- Coding based

Contactless Palmprint: Research Directions



Single view systems: 2D systems
- Cameras, Webcams
- Enhancement + traditional recognition methods

Multiple view systems: 3D systems
- Multiple cameras
- Laser scanners
- Mosaicking of three different views
- Illuminator shaped as a ring-mirror

Systems based on structured light
- Able to estimate the height of the ridge pattern
- Long acquisition time

Unwrapping methods
- Parametric models (e.g. cylinder, sphere, set of rings)
- Non-parametric models based on minimization functions

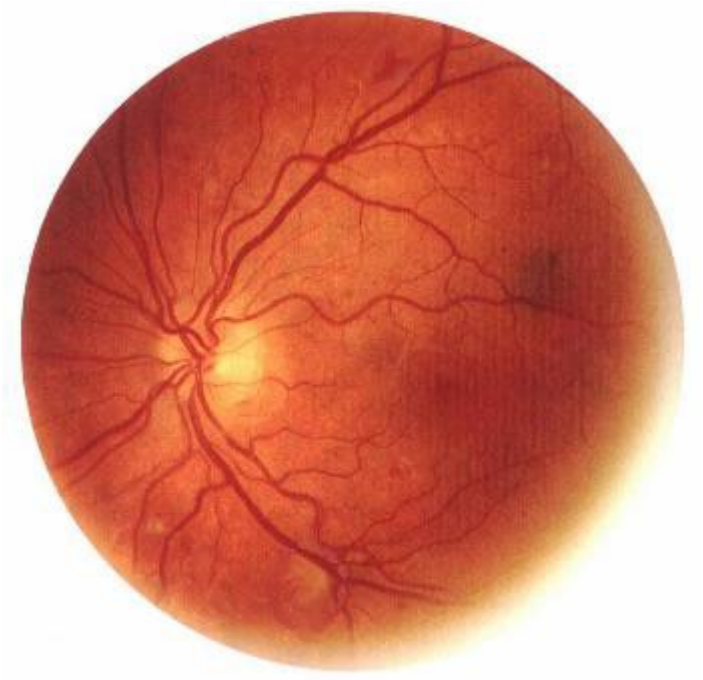
Quality estimation of acquisition

Improving 3D models
- More robust 3D matching methods
- Robust 3D alignment methods

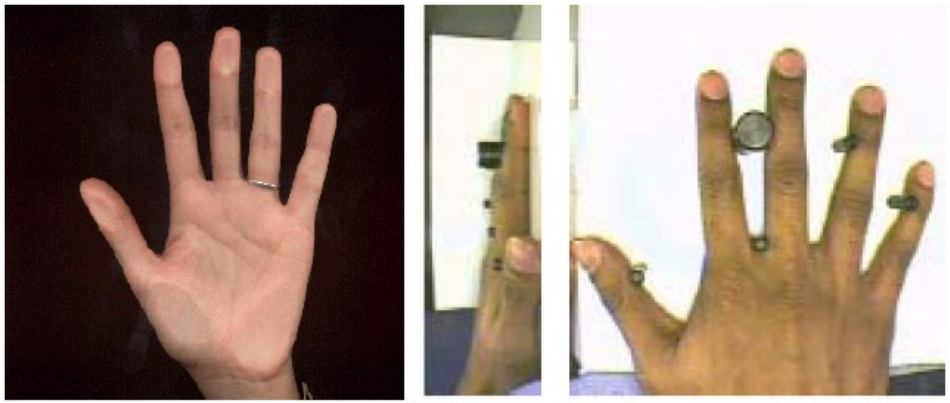
Simultaneous acquisition with multiple illuminations

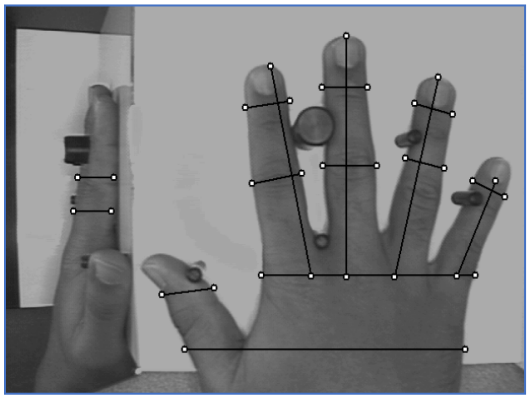
Faster acquisition

Retina

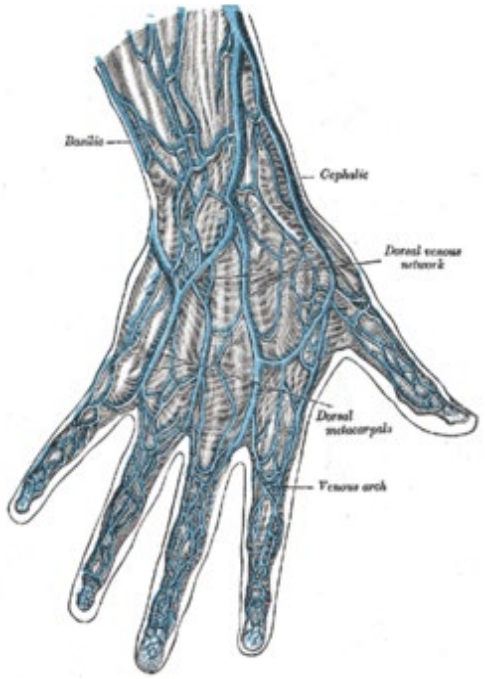


Hand Geometry



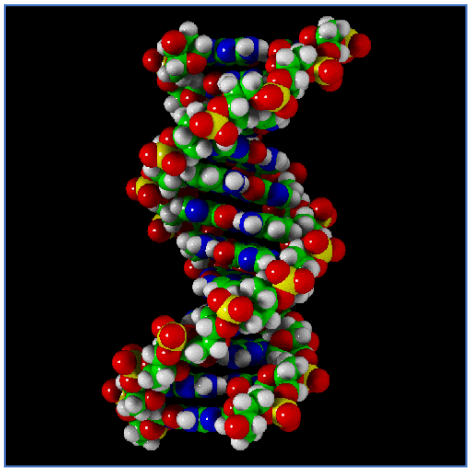


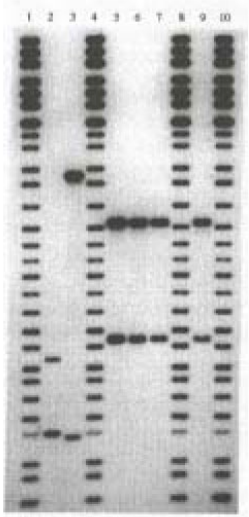
Hand Veins


Basilic
Cephalic
Dorsal venous network
Dorsal metacarpals
Venous arch

Ear Shape

DNA





Physiological Signals for Biometric Recognition

- Difficult to counterfeit
- Only from living people
- Continuous authentication

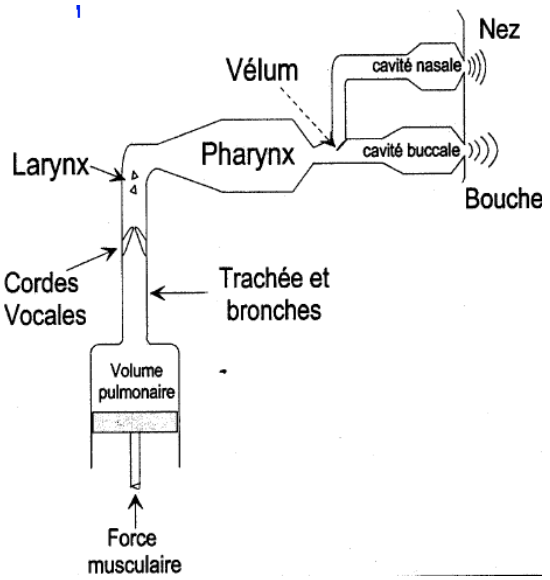
Electrocardiogram

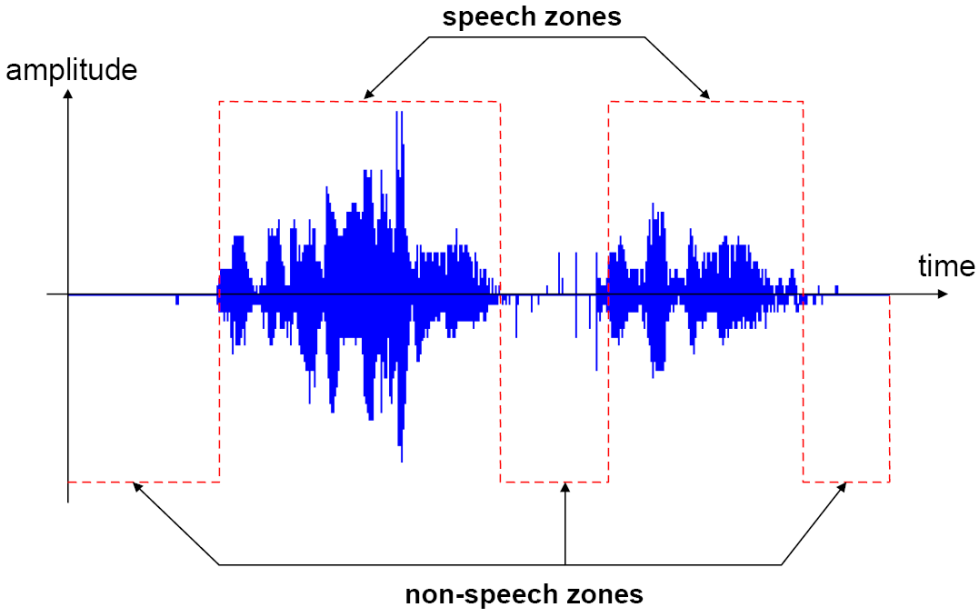
Electroencephalogram

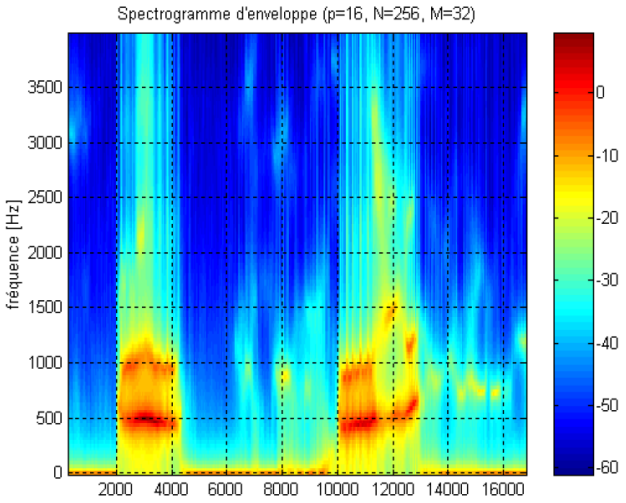
Photoplethysmogram

Voice

- Easily accepted by users
- Low cost
- Low accuracy
- Easy to forge



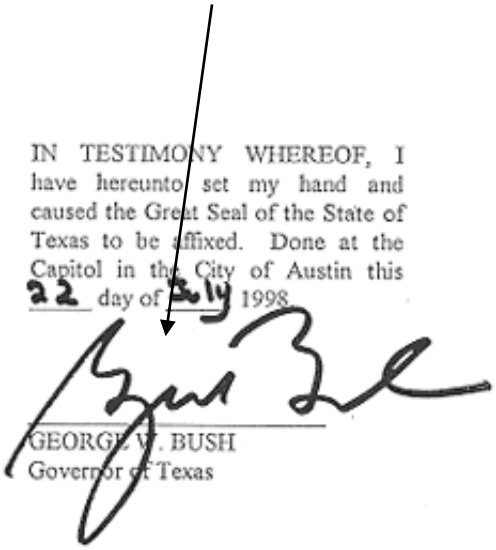




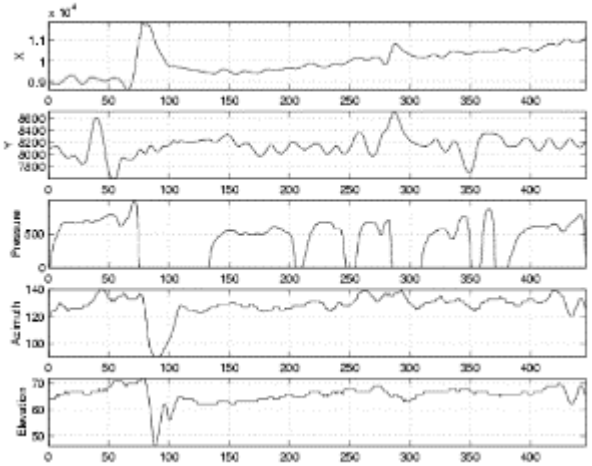
Signature

- Easy
- Cheap but not accurate

STATIC

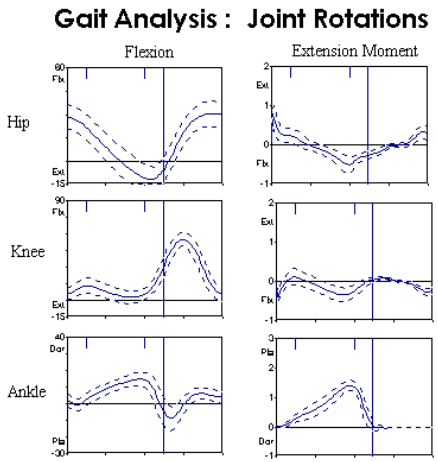


DYNAMIC



Keystroke

Gait


Gait Analysis : Joint Rotations
Flexion
Extension Moment
Hip
Knee
Ankle

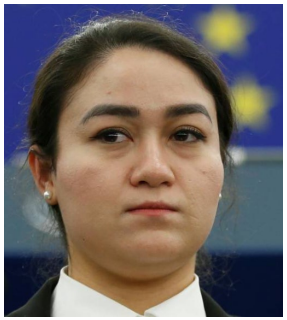
Gesture

Emotion


Happy
Sad
Petulant
Lonely
Amused
Skeptical
Furious
Wistful
Confused
Bored
Sarcastic
Regretful
Aroused
Terrified
Proud
Mischievous

Soft Biometrics

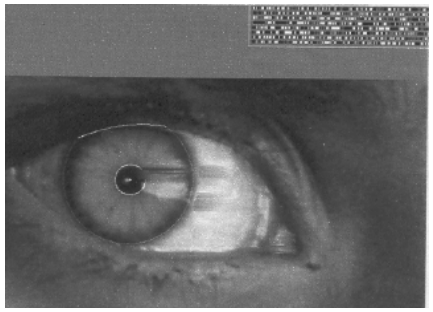
- Gender
- Age
- Skin color
- Ethnicity
- Hair color
- Eye color
- Weight
- Height
- …



Which Trait for an Application?

Each trait has different properties and usability

THERE IS NO SINGLE TRAIT
WHCH IS GOOD FOR ALL APPICATIONS



Properties of Biometric Traits

Human characteristic

1. Universality
   each person should have the characteristic
2. Distinctiveness
   any two persons should be sufficiently different in characteristic
3. Permanence (in time)
   the characteristic should be sufficiently invariant over a period of time
4. Collectability
   the characteristic can be measured quantitatively

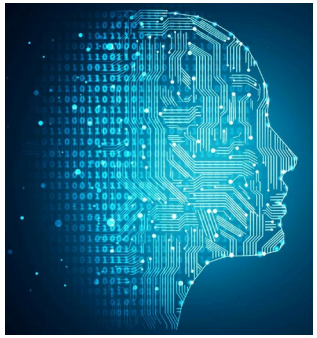
Technology

5. Performance
   accuracy and computational time should be adequate
6. Acceptability
   extent to which people are willing to accept its use in their daily lives
7. Resistance to Circumvention
   how easily the system can be fooled using fraud

Properties of Biometric Traits

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F.Thermograms	High	High	Low	High	Medium	high	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear	Medium	medium	High	medium	Medium	High	Medium

Biometric Systems: Research Directions



Contactless and on-the-move

Artificial Intelligence

Interoperable distributed systems

Mobile and embedded

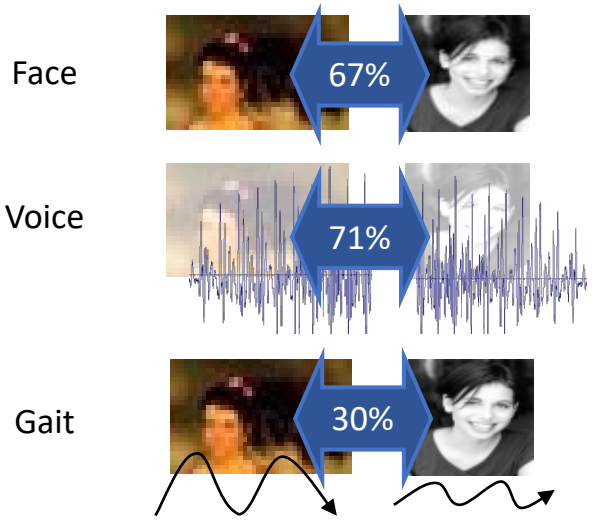
Ethics and privacy

Multimodal and higher resolution

Human Beings are Multimodal

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

→ The brain performs a multimodal matching



Soft biometrics

- 57Kg
- 175cm
- Brunette

7%

- 79Kg
- 155cm
- Brown hair

67%+71%+30%+7%

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

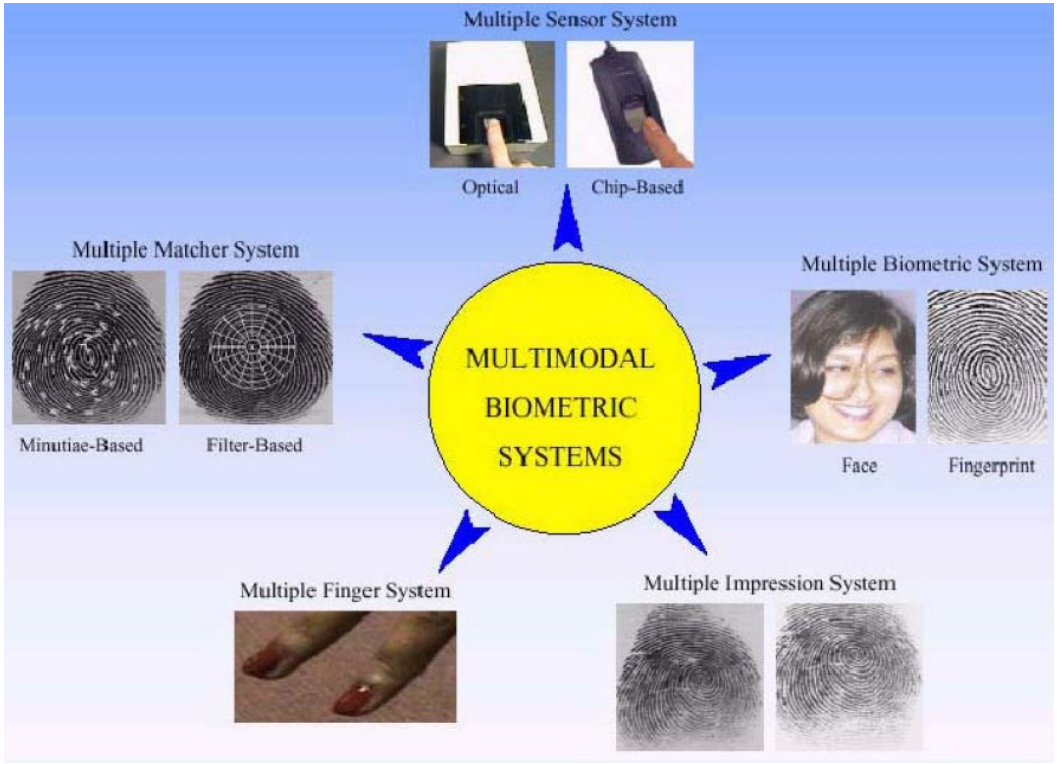
Multibiometrics

Data gathering

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

Fusion logics

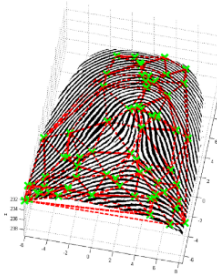
- Sensor level
- Feature set level
- Matching score level
- Decision level

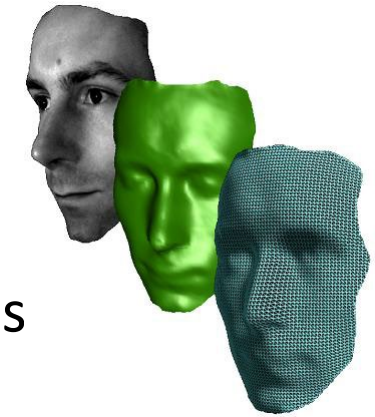


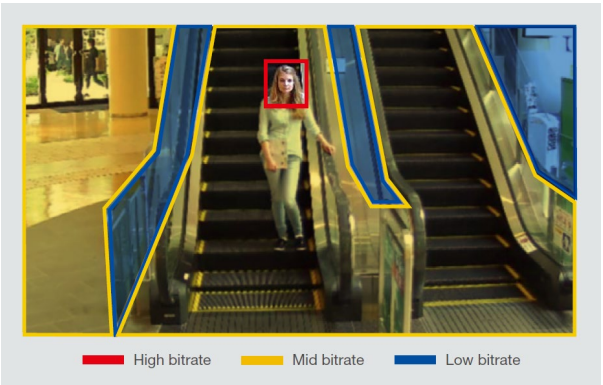
Voice, Face
Voice, Lip Movement
Voice, Face, Lip Movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand geometry
Fingerprint, Voice, Hand geometry
Fingerprint, Hand geometry
Facial thermogram, Face
Iris, Face
Palmprint, Hand geometry
Ear, Voice

Multibiometrics: Research Directions

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







Continuous / Periodic Authentication: Research Directions

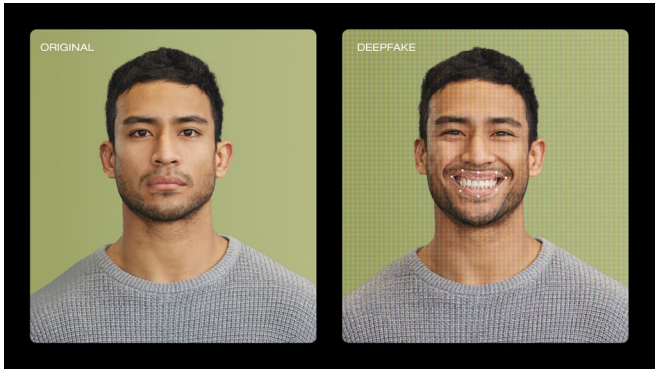
- Keystroke dynamics, mouse movements
- Face, iris
- Gesture
- Voice
- Gait for mobile devices
- Research directions:
  - user-friendly biometrics
  - soft biometrics
  - behavior prediction
  - IoT integration
  - …

Forgery / Spoofing: Research Directions

- From physical objects
- At a distance
- From social networks
- New anti-spoofing techniques based on liveness (termic, 3D, motion, heart beats, breath, …)

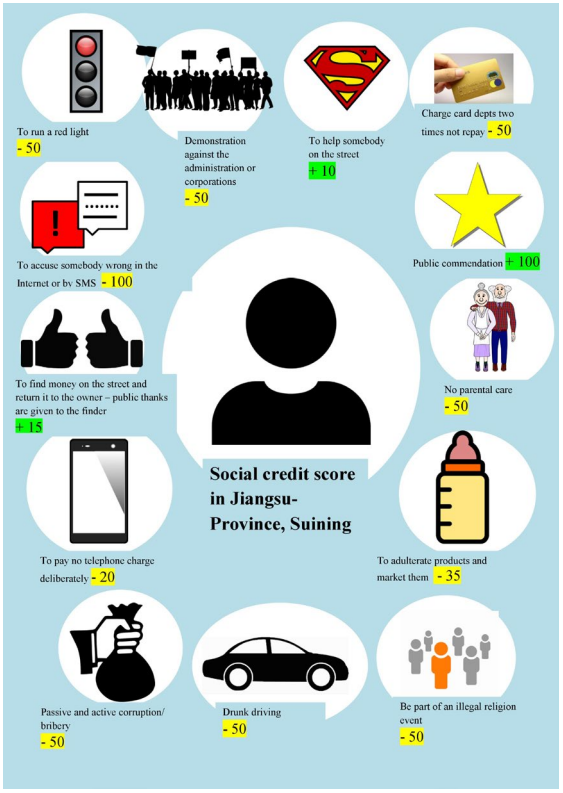
Deepfake: Research Directions

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



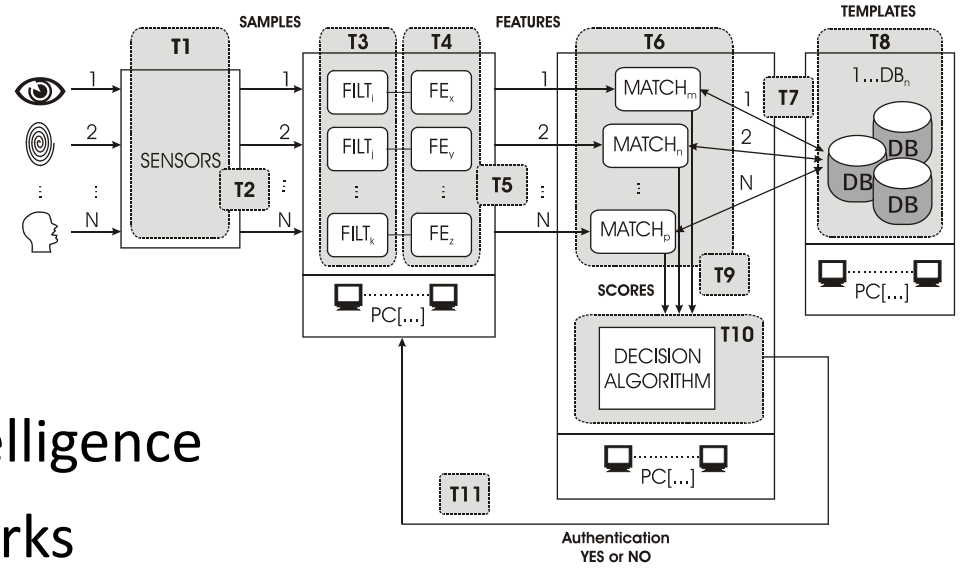
Unauthorized / Unintended Use: Research Directions

- Biometric information sent to a biometric-based system should be used only for the intended purpose
- Inclusion in proscription lists without individual is informed
- Evaluation of social credits

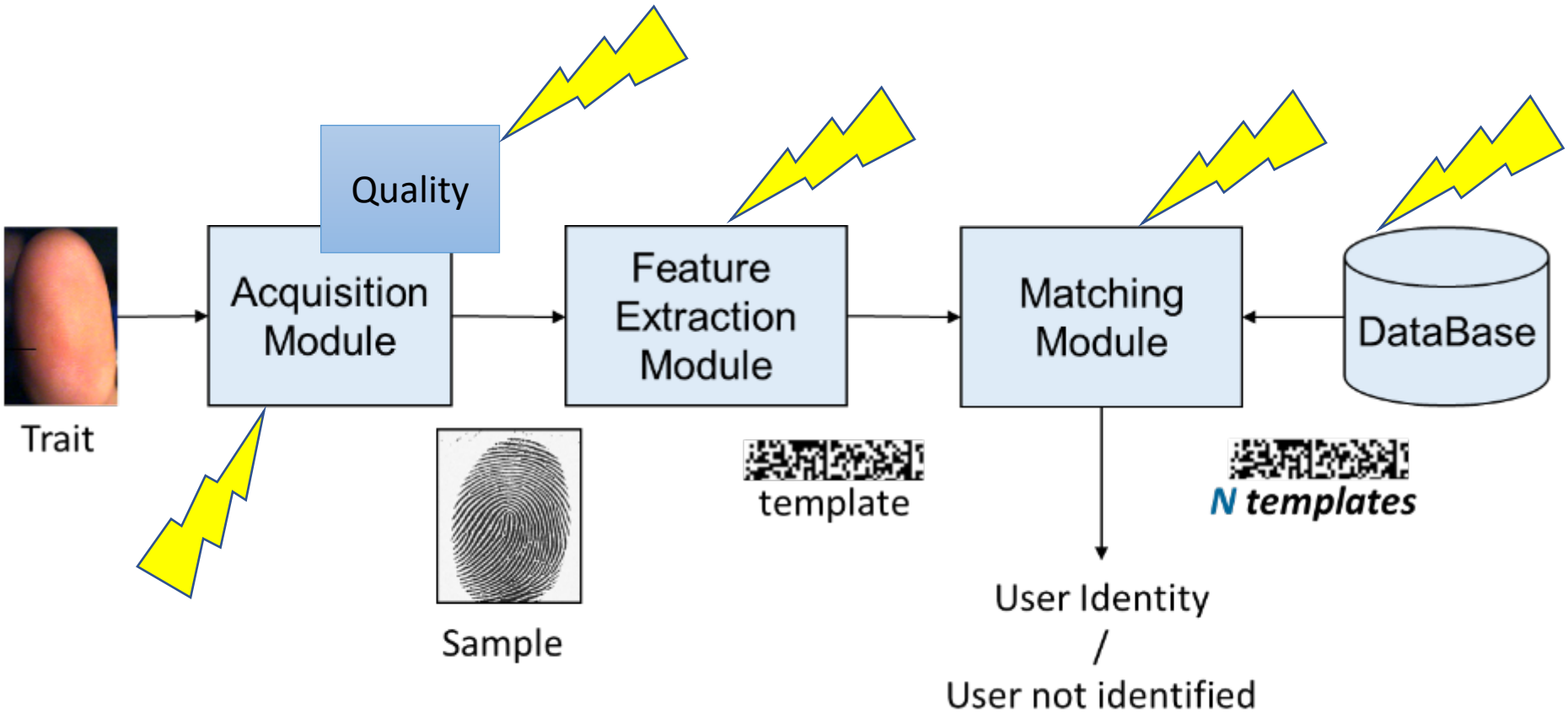


Distributed Biometric Systems: Research Directions

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



Artificial Intelligence: Research Directions (1)

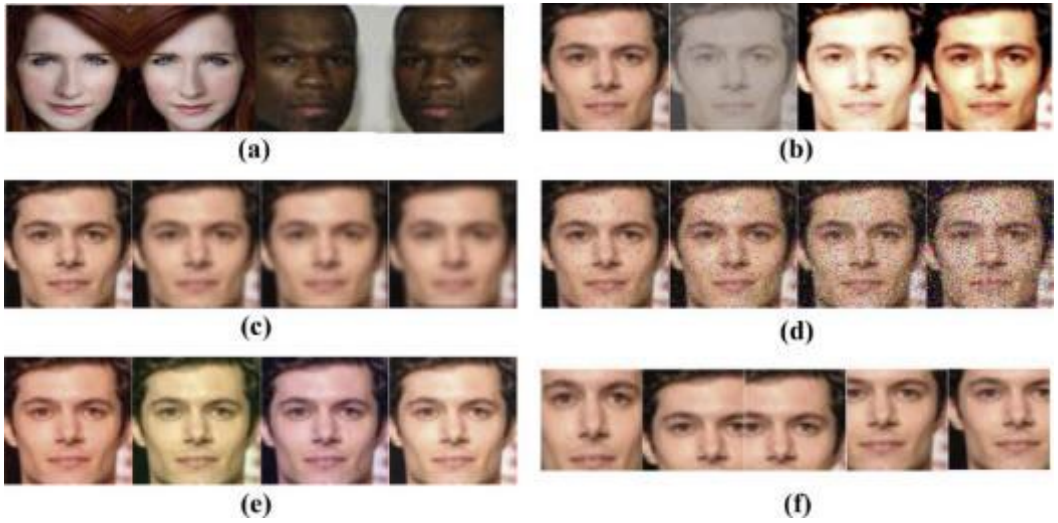


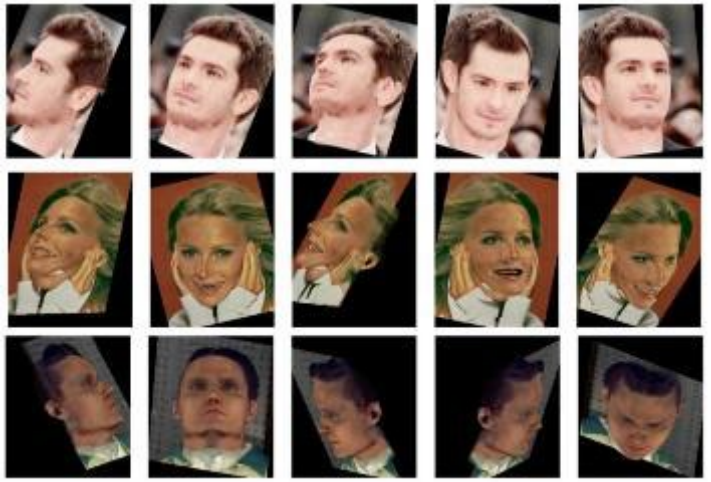
Artificial Intelligence: Research Directions (2)

AI for Data Augmentation

Landmark perturbation for face alignment.

Flipping
patches (clipping)
color casting
blurring

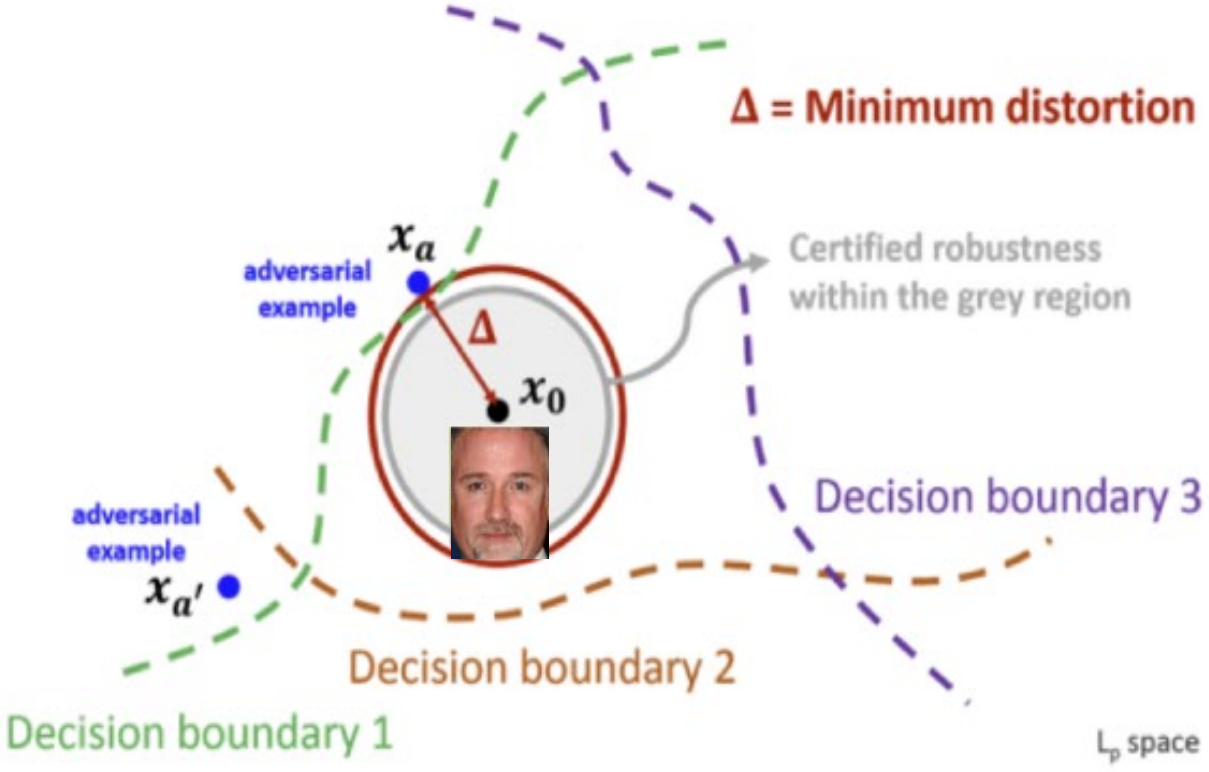




Artificial Intelligence: Research Directions (3)

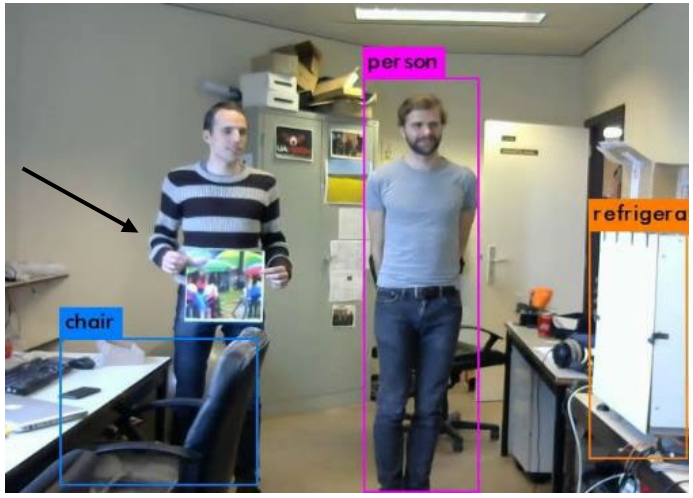
AI for Recognition Robustness

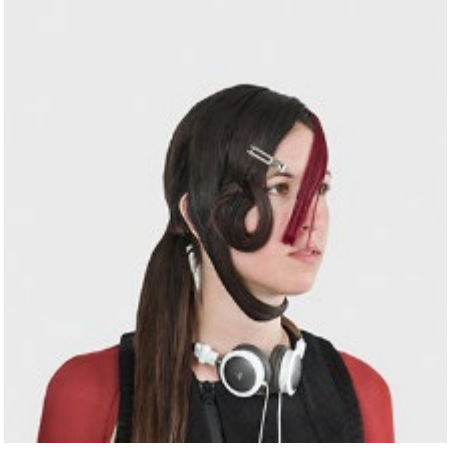
Generative Adversarial Networks

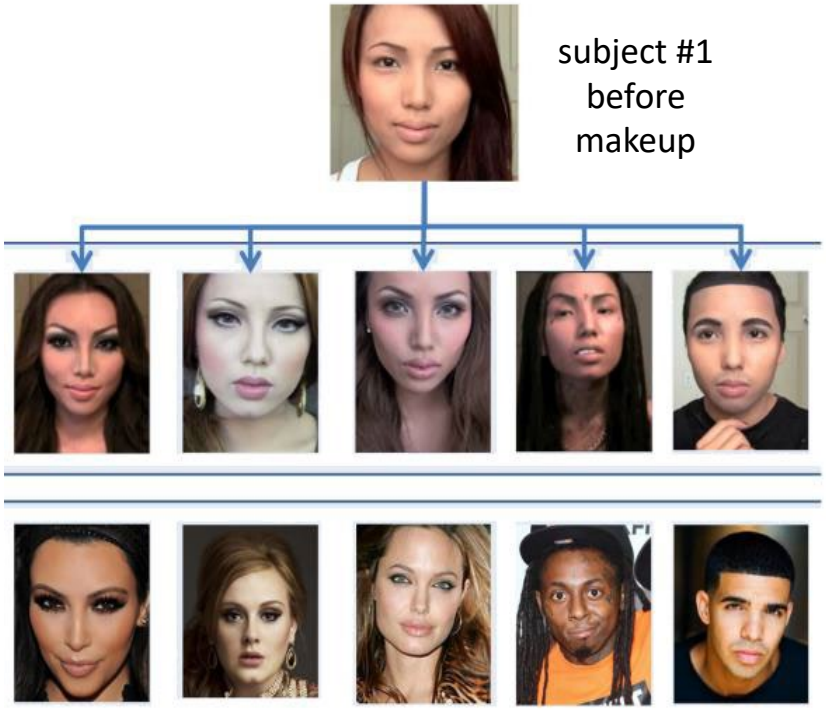


Artificial Intelligence: Research Directions (4)

AI for Identity Concealing Detection



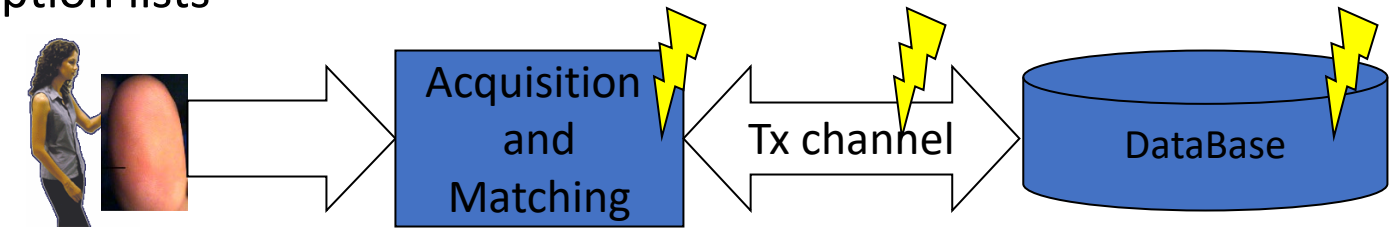




Biometric Privacy: Research Directions (1)

- 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

… using cards and documents



… using real time systems

Biometric Privacy: Research Directions (2)

Privacy in Biometric Applications

1. Privacy-protective applications

   Biometrics protects personal information that might otherwise be compromised like enterprise security,…

2. Privacy-sympathetic applications

   Designed considering privacy protection techniques, most of the current applications

3. Privacy-neutral applications

   Authentication systems for electronic devices

4. Privacy-invasive applications

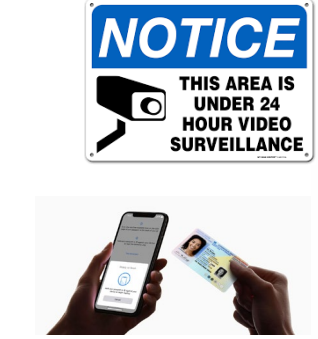
   Surveillance applications and some national ID services

Biometric Privacy: Research Directions (3)

Risk Analysis

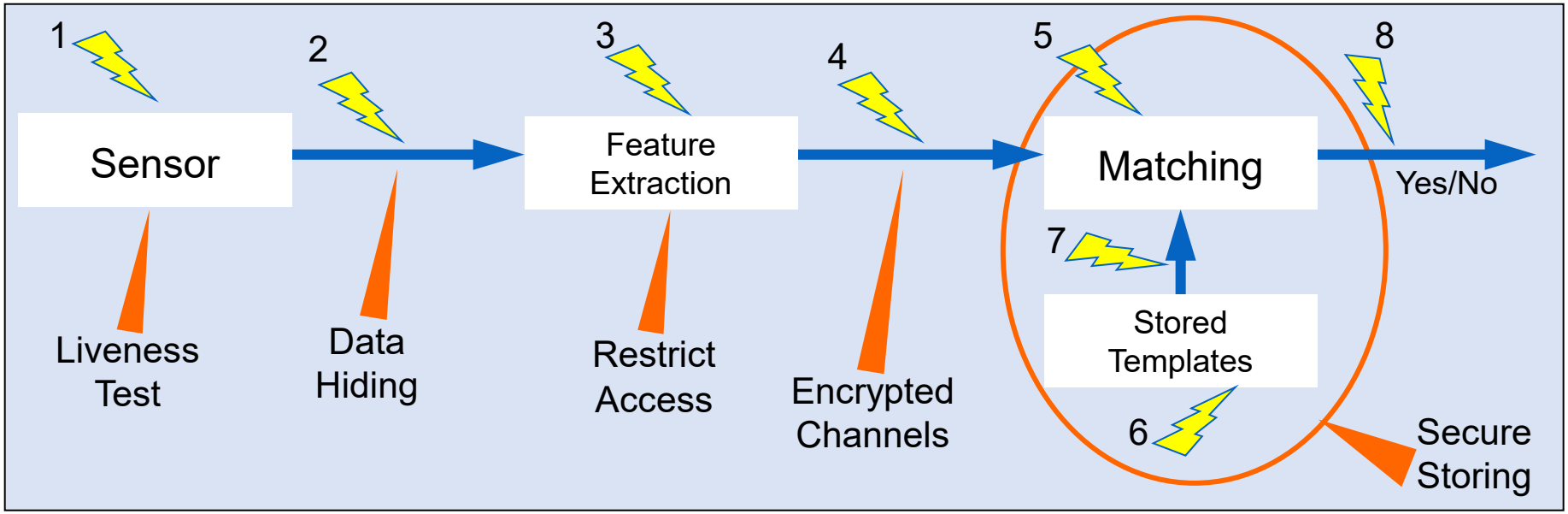
Privacy++

Lower Risk Of Privacy Invasiveness		Greater Risk Of Privacy Invasiveness
Overt	1. Is the system deployed overtly or covertly?	Covert
Optional	2. Is the system optional or mandatory?	Mandatory
Verification	3. Is the system used for identification or verification?	Identification
Fixed Period	4. Is the system deployed for a fixed period of time?	Indefinite
Private Sector	5. Is the system deployed in the public or the private sector?	Public Sector
Individual, Customer	6. In what capacity is the user interacting with the system?	Employee, Citizen
Enrollee	7. Who owns the biometric information?	Institution
Personal Storage	8. Where is the biometric data stored?	Database Storage
Behavioral	9. What type of biometric technology is being deployed?	Physiological
Templates	10. Does the system utilize biometric templates, biometric images, or both?	Images



Biometric Privacy: Research Directions (4)

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 (5)

Biometric Privacy Protection: Approaches

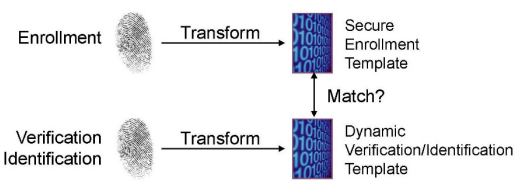
- Central Repository
  - Centralized protection
- Distributed Repository
  - Anonymization by distribution
- Smart Hardware
  - Privacy rules embedded in hardware
- Smart Data
  - Encapsulate access methods inside the data

Biometric Privacy: Research Directions (6)

Biometric Privacy Protection: Techniques

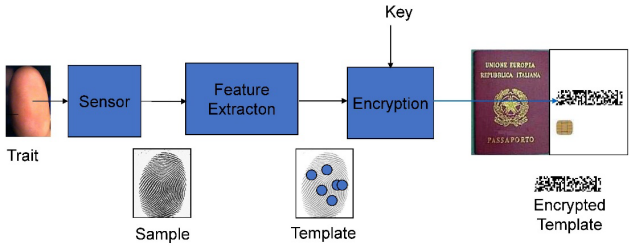
Techniques

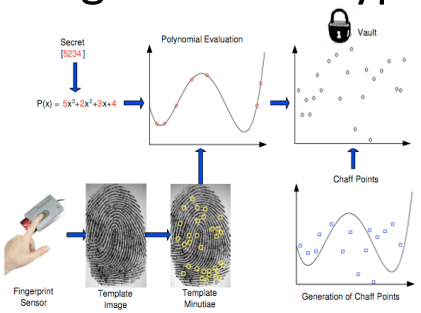
- Key-generating, Key-binding, Biometric encryption
- Feature Transformation, Helper Data Approach
- Fuzzy Commitment, Fuzzy Vault, Fuzzy Extractor
- Secure Sketch, Bio-Hashing, Revocable Bio-Token, Biotope
- Bio-Encryptor , …



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, …

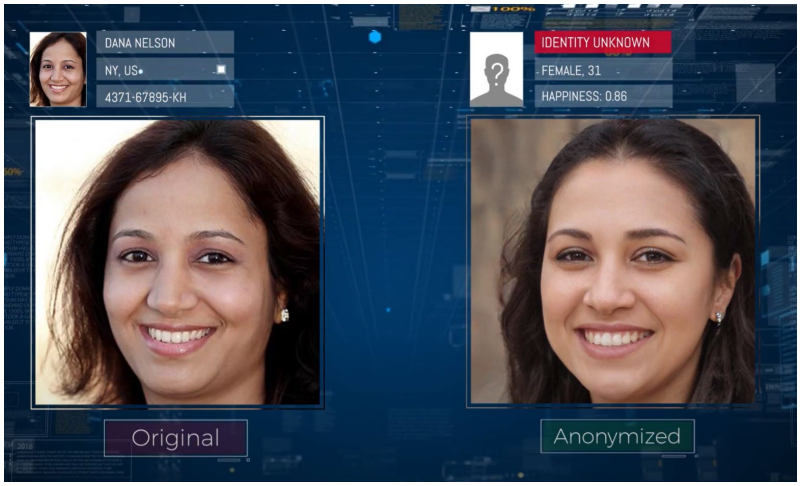




Biometric Privacy: Research Directions (7)

Image and Video Anonymization

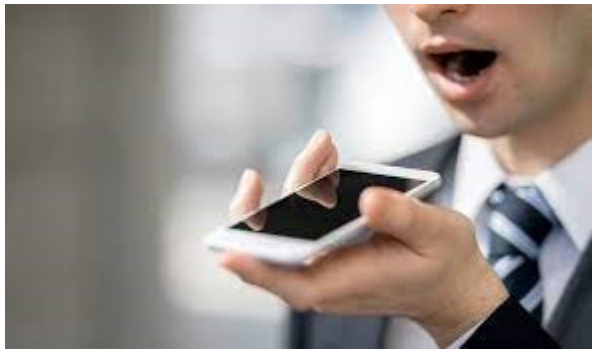
Personally Identifiable Information can be removed by advanced computer vision, AI and deep learning, while preserving key biometric attributes



Biometric Privacy: Research Directions (8)

Personalized Interactions

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



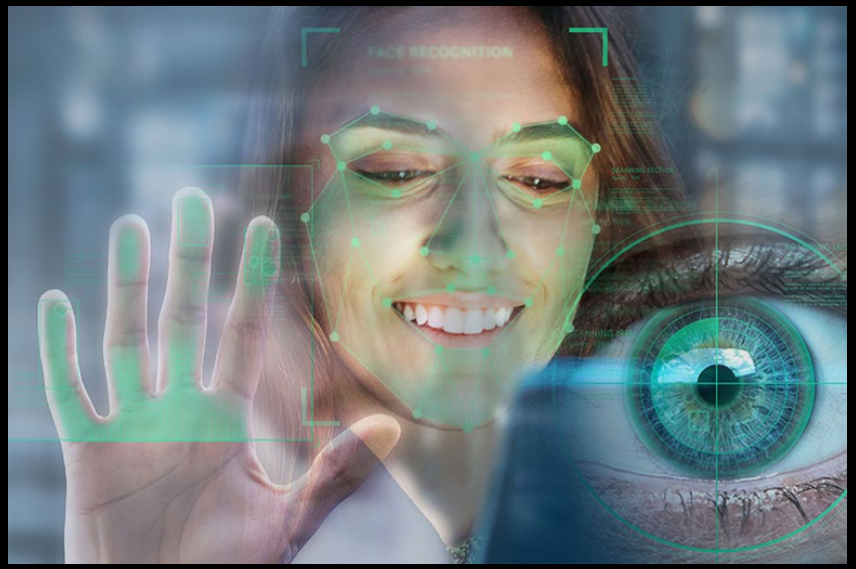
Biometric Privacy: Regulations

- 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

Ethics in 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.

Biometrics: technologies, challenges, and research directions

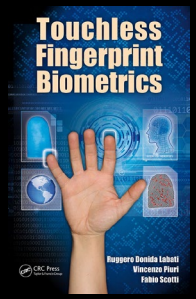


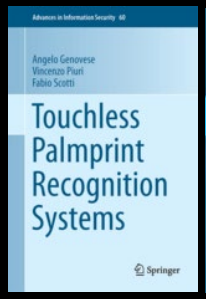
Vincenzo Piuri

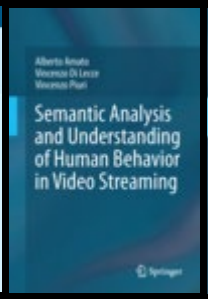
Università degli Studi di Milano

vincenzo.piuri@unimi.it

https://piuri.di.unimi.it







EdgeAI GLACIATION SERICS