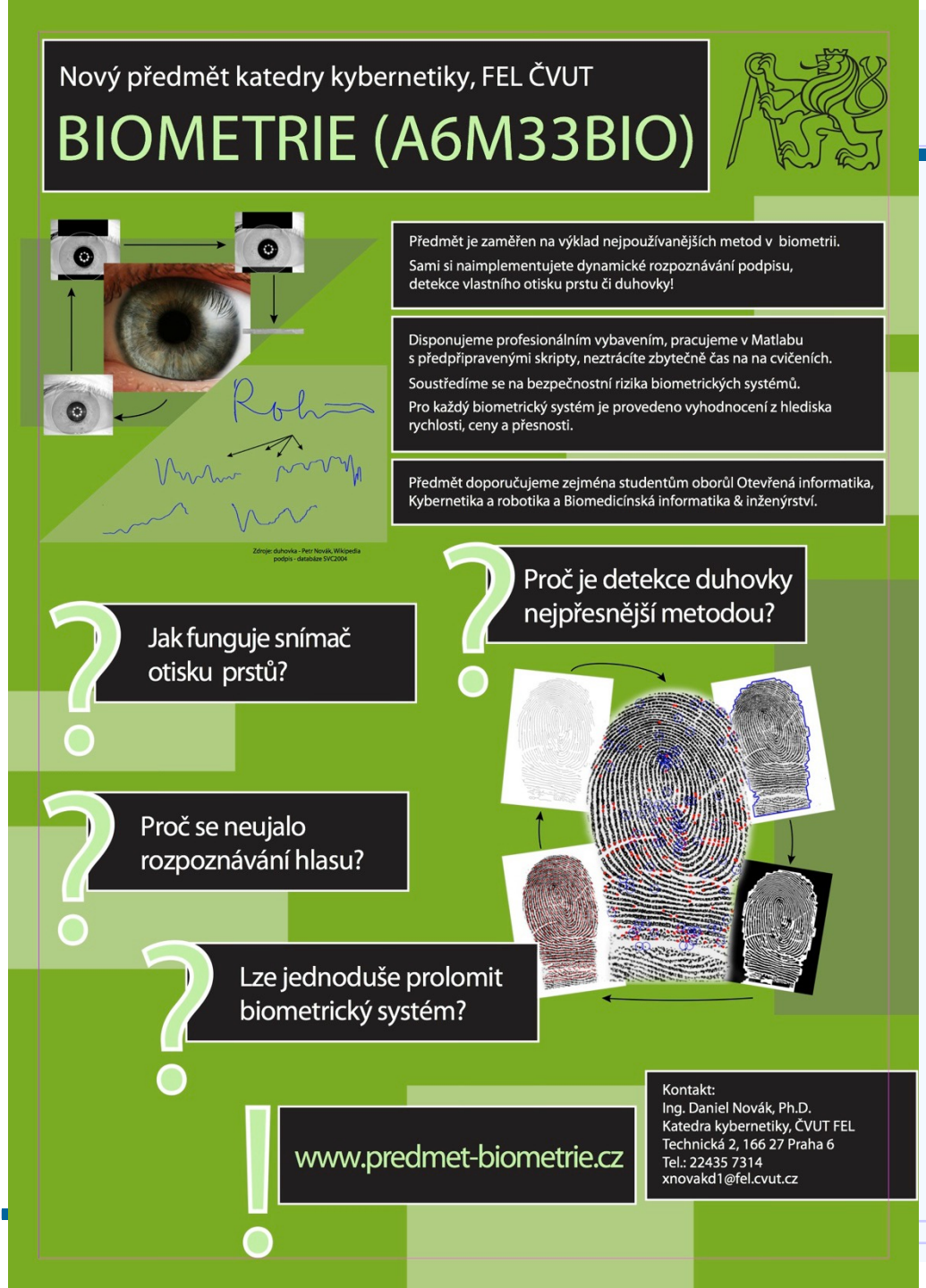


Biometrics Introduction

Daniel Novák

26.9.2024, Prague

Acknowledgments: Chang Jia, Andrzej Drygajlo

laboratory Gerstner

Podmínky předmětu

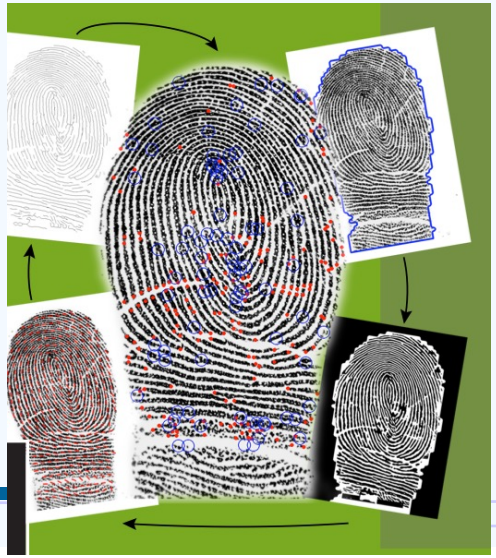
- Garant předmětu: Daniel Novák, místnost G202, xnovakd1@fel.cvut.cz
- Stránky předmětu
  - https://cw.felk.cvut.cz/doku.php/courses/a6m33bio/start
  - 3. laboratorní úlohy – každá za 20 bodů, celkem 60 bodů
  - Klasifikovaný zápočet – 20 otázek, každá za 2 body
- Podmínky předmětu
  - https://cw.felk.cvut.cz/doku.php/courses/a6m33bio/podminky

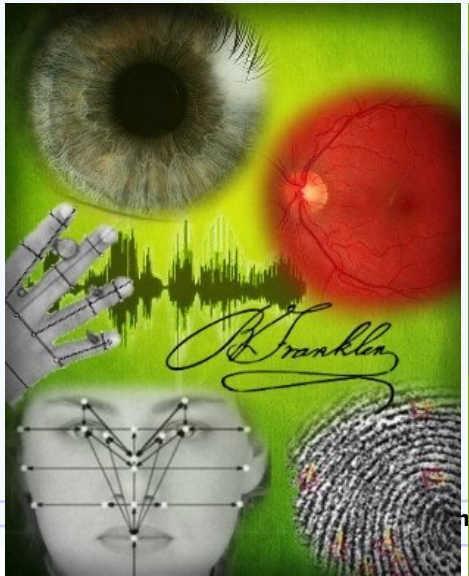
Body z předmětu	Stupeň ECTS	Známka
100–90	A	výborně
89–80	B	velmi dobře
79–70	C	dobře
69–60	D	uspokojivě
59–50	E	dostatečně
49 a méně	F	nedostatečně

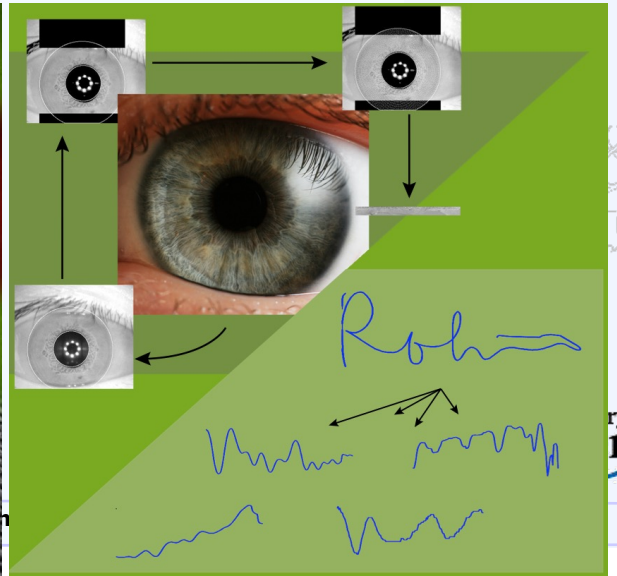
laboratory Gerstner

Facebook, Web

- **Prispivejte zejmena vy!!!!**
- Facebook (zalikujte, pokud se vam predmet bude libit:)
  - http://www.facebook.com/biometrieCVUT
- Webove stranky
  - http://www.predmet-biometrie.cz/
- Novinky
- https://www.biometricupdate.com/, https://www.wired.com/tag/biometrics/





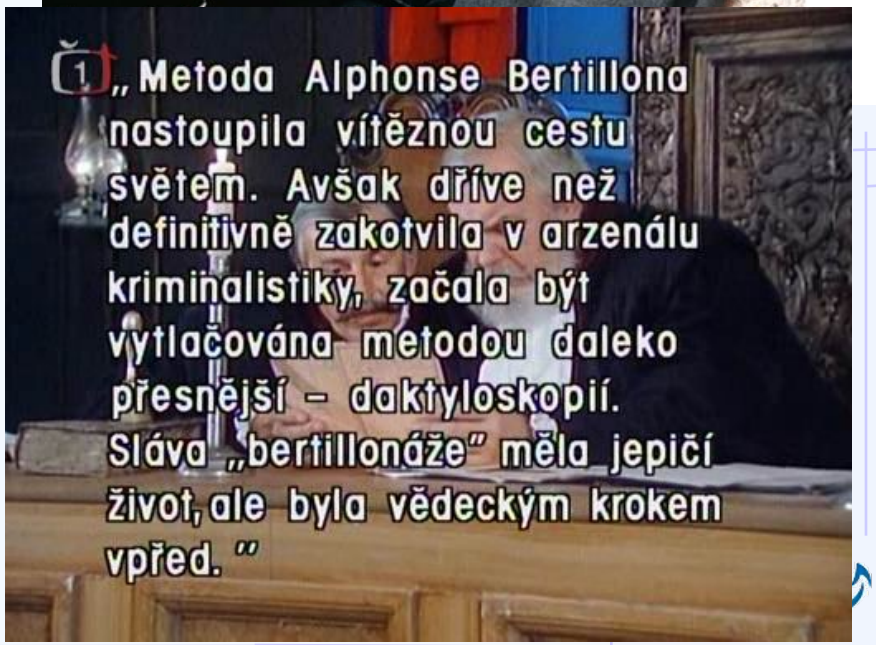


Najdete něco zajimaveho

Proč Biometrie ?

Alternativní úvod

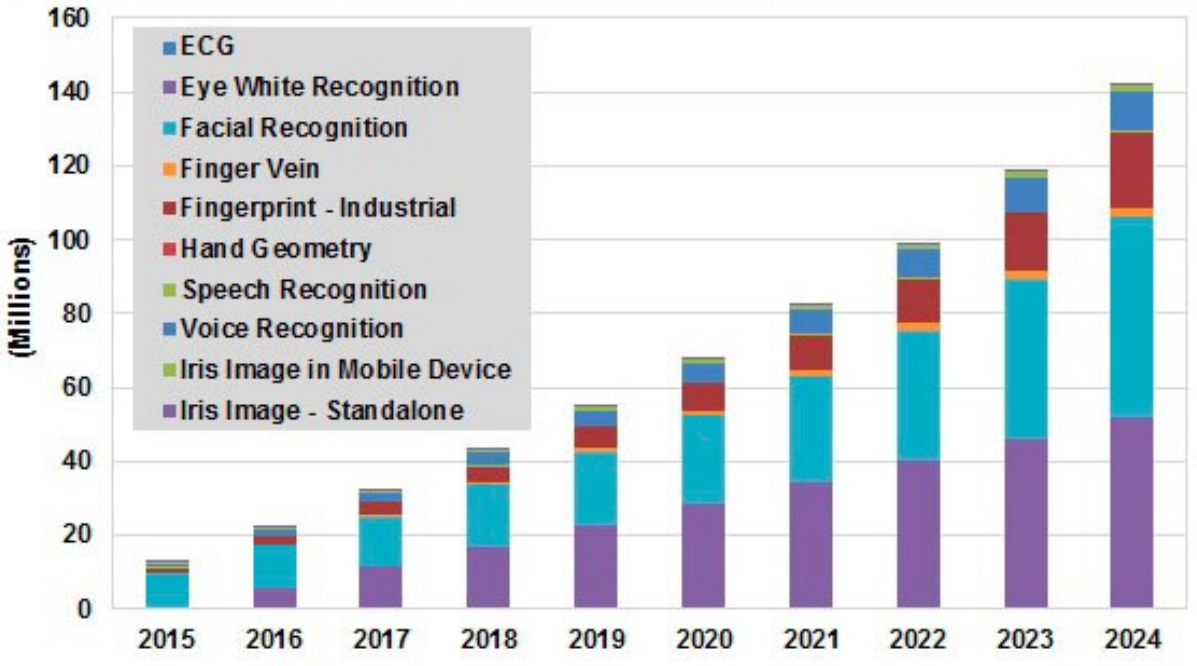
- Dobrodužství kriminalistiky na csfd
- Dobrodužství kriminalistiky na CT



Alphonse Bertillon: Forensic Anthropometry

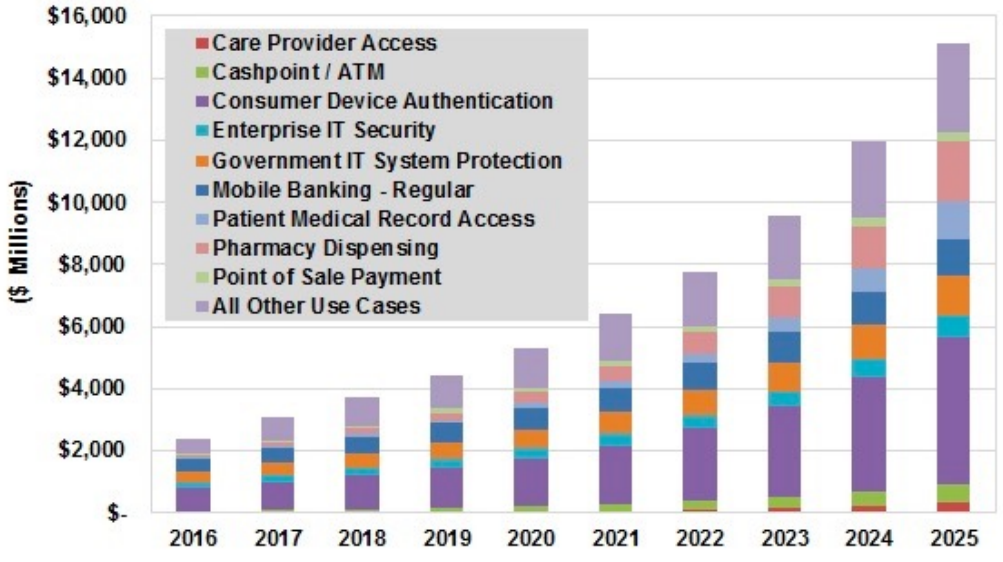
- Alphonse_Bertillon
- Dreyfusova aféra

Trend



Tractica

Annual Biometrics Revenue by Selected Use Cases, World Markets: 2016-2025



Source: Tractica

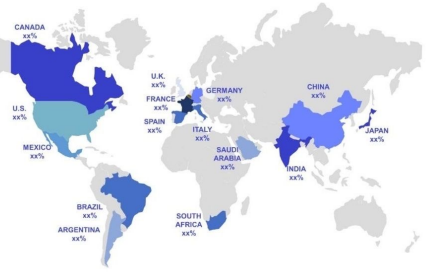
U.S. biometrics technology market size, by end-use, 2014 - 2025 (USD Billio

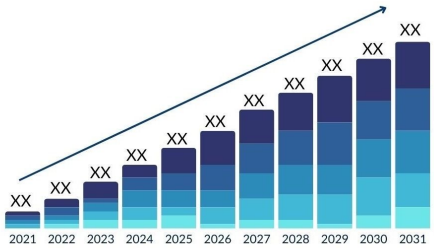
Source: www.grandviewresearch.com

laboratory Gerstner

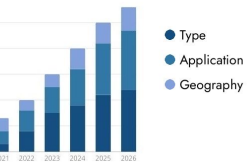
Market Share

ontactless Biometrics Technology Market Size and Scope

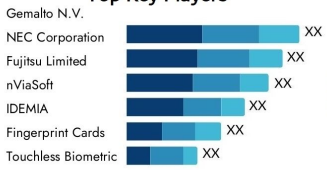




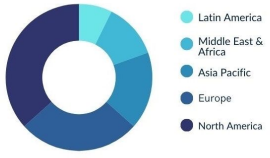
larket Segmentation



Top Key Players

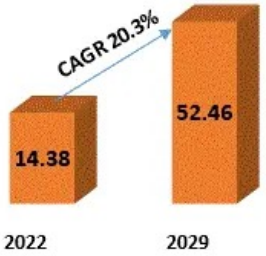


Regional Analysis



Source : www.marketresearchintellect.com

Contactless Biometrics Technology Market

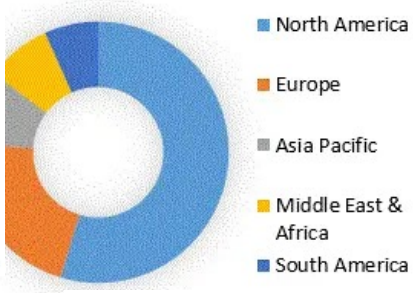


Market Size in US$ Billion

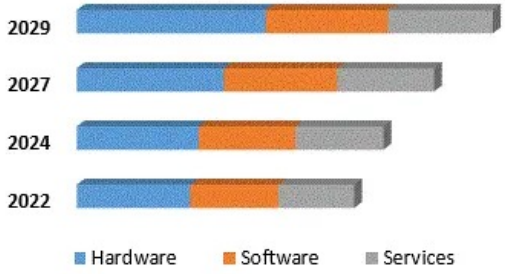
Key Players

3M	Assa Abloy AB
Fujitsu Limited	Aware, Inc.
Touchless Biometric Systems AG	Griaule Biometrics
Aware Inc.	Lumidigm Inc.
NEC Corporation	Privaris
Fingerprint Cards AB	Gemalto N.V.
IDEMIA	RCG Holdings Limited
Neurotechnology	Siemens AG
HID Global	Thales SA
	Other Key Players

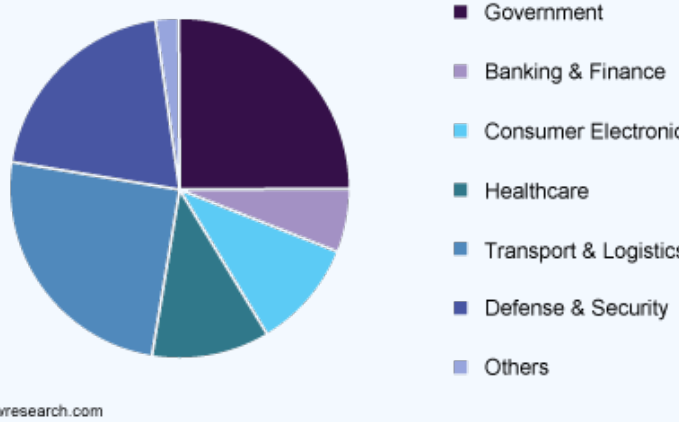
Regional Analysis in 2022 (%)



Offering Segment Overview



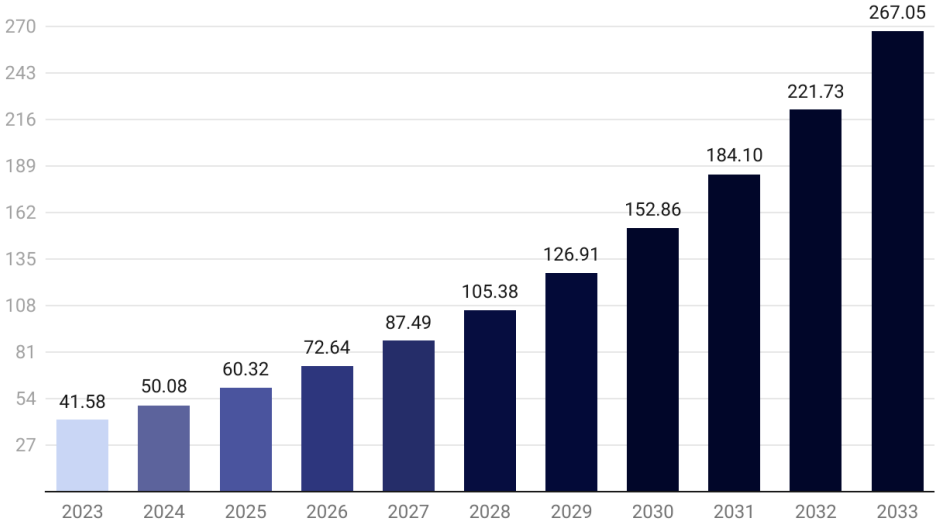
Europe contactless biometrics technology market shar



Source: www.grandviewresearch.com

BIOMETRIC MARKET SIZE 2023 TO 2033

(USD BILLION)



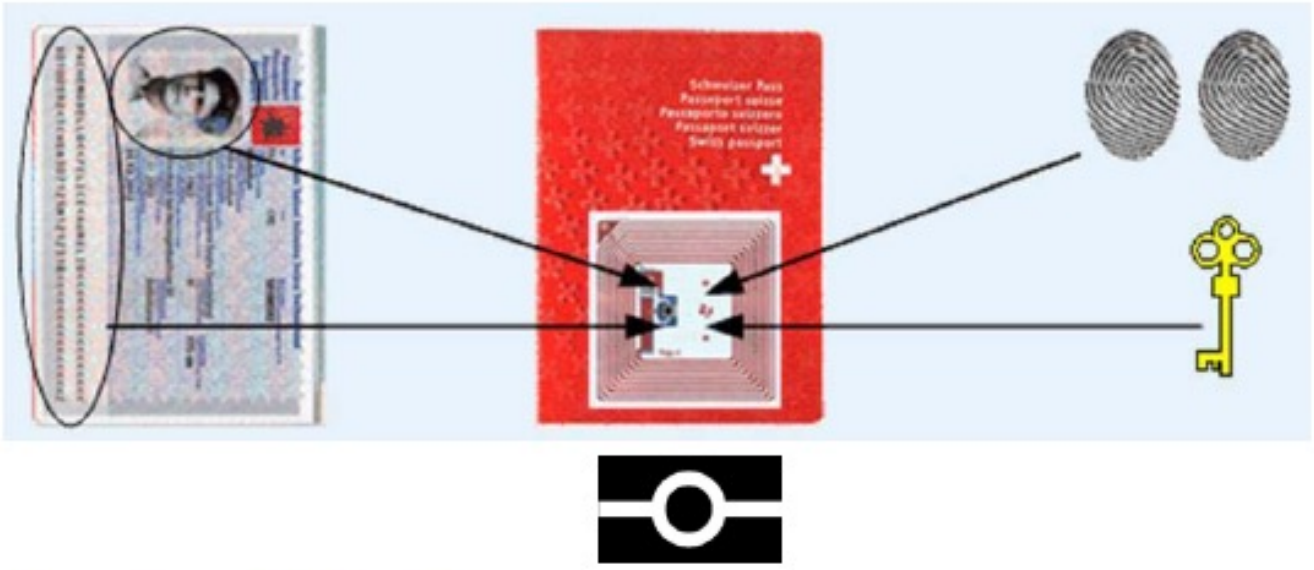
ePassport – Biometricky pas

Nutná podmínka pro výjezd do USA+ESTA, v ČR od roku 2006, od dubna 2009 s 2 otisky prstů, 140 statu, Epassport (mobile app)

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

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

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



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

Today: eBorders in the United Arab Emirates (UAE)

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

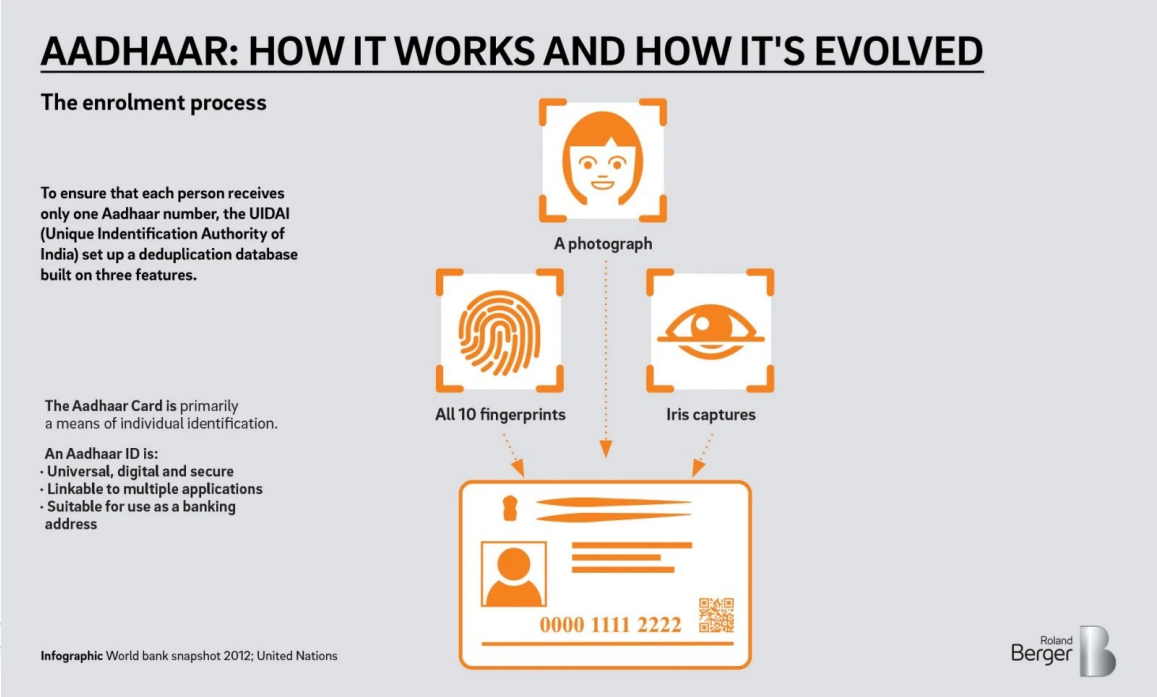
- 1 central database
  - Watchlist application
  - Fully networked
  - Enrolment centres: prisons and deportation centres
  - More than 1 million enrolments (150+ nationalities)
  - Exhaustive search takes <2 seconds

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

IrisGuard incorporated

India's Aadhaar project

- The Aadhaar number is a 12-digit unique identity number issued to all Indian residents
- biographic and biometric data (a photograph, ten fingerprints, and two iris scans).
- 1,370,020,912 Aadhaar IDs have been issued as of 20 May 2023, covering more than 99,9% of the Indian adult population.
- world's most extensive biometric identification system



Ukradená identita

Článek v NY times a v Telegraph, zodpovědný byl MOSAD

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

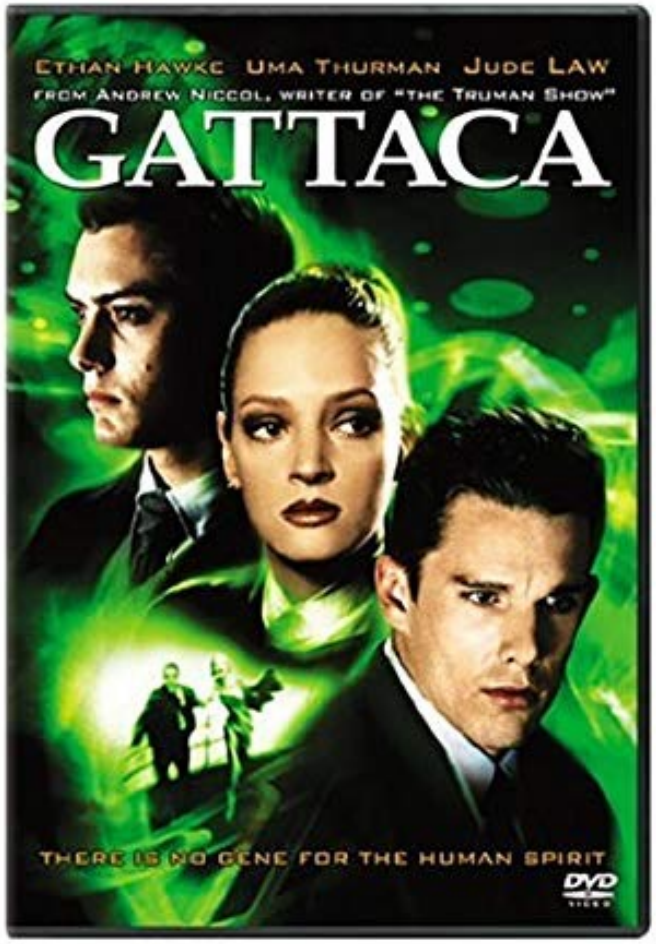
- One of the victims of the identity theft was British-Israeli Paul John Keeley (picture right). The passport used by one of the suspected assassins bore his name, but featured a photograph of another man (pictured left)

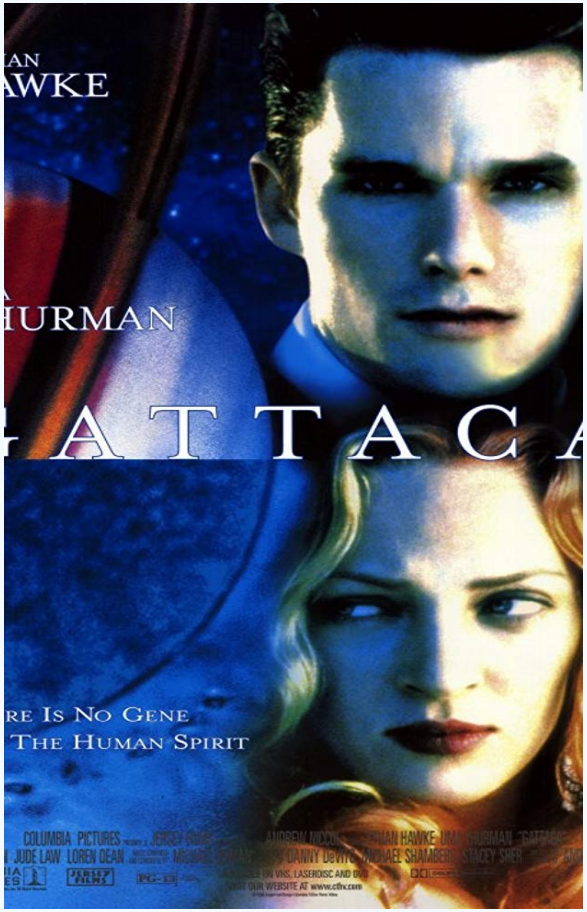
Další krádež identity

- DU – Unknown podívat se a ohodnotit na CSFD

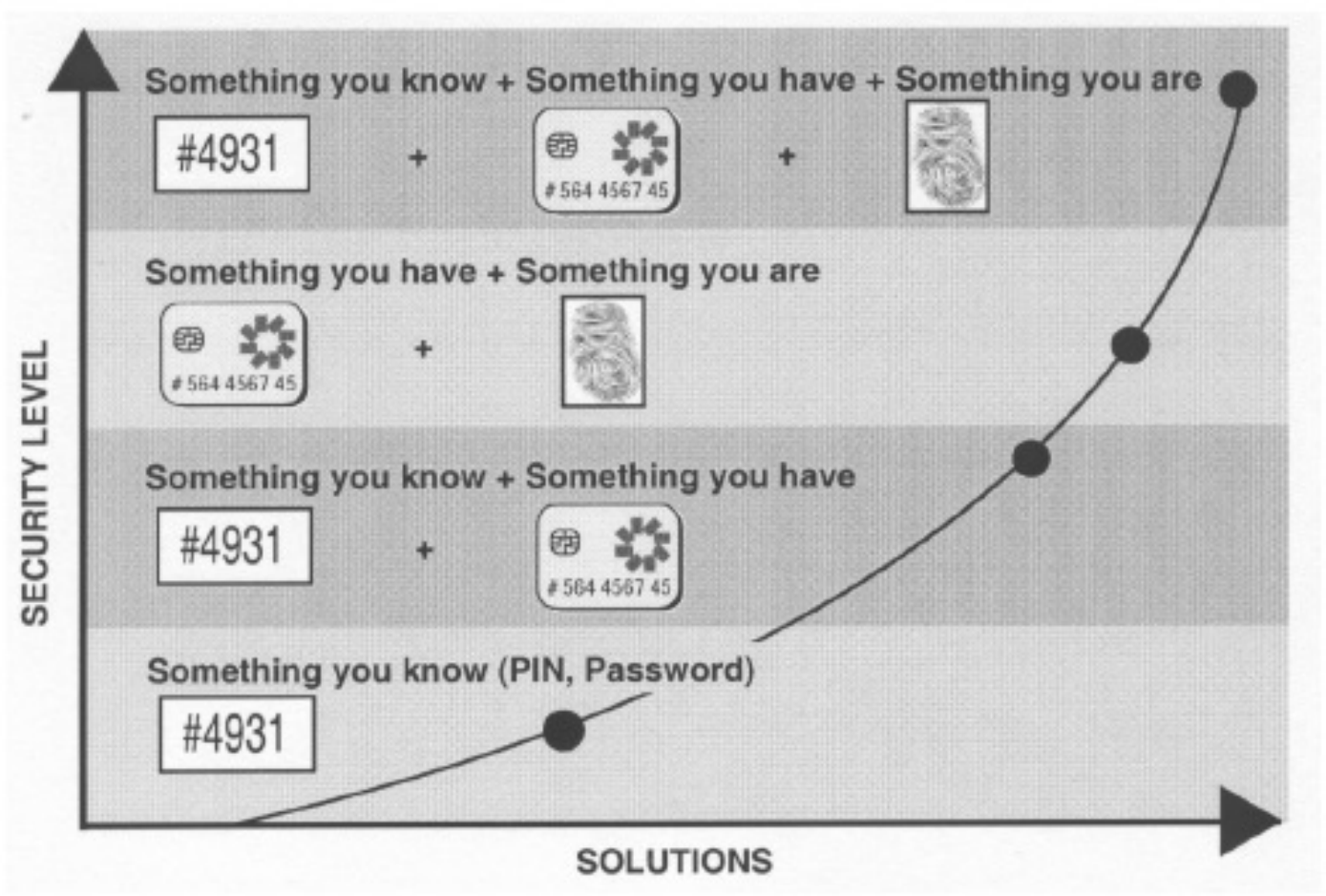
Další krádež identity

– DU – Gattaca podívat se a ohodnotit na CSFD (83%)

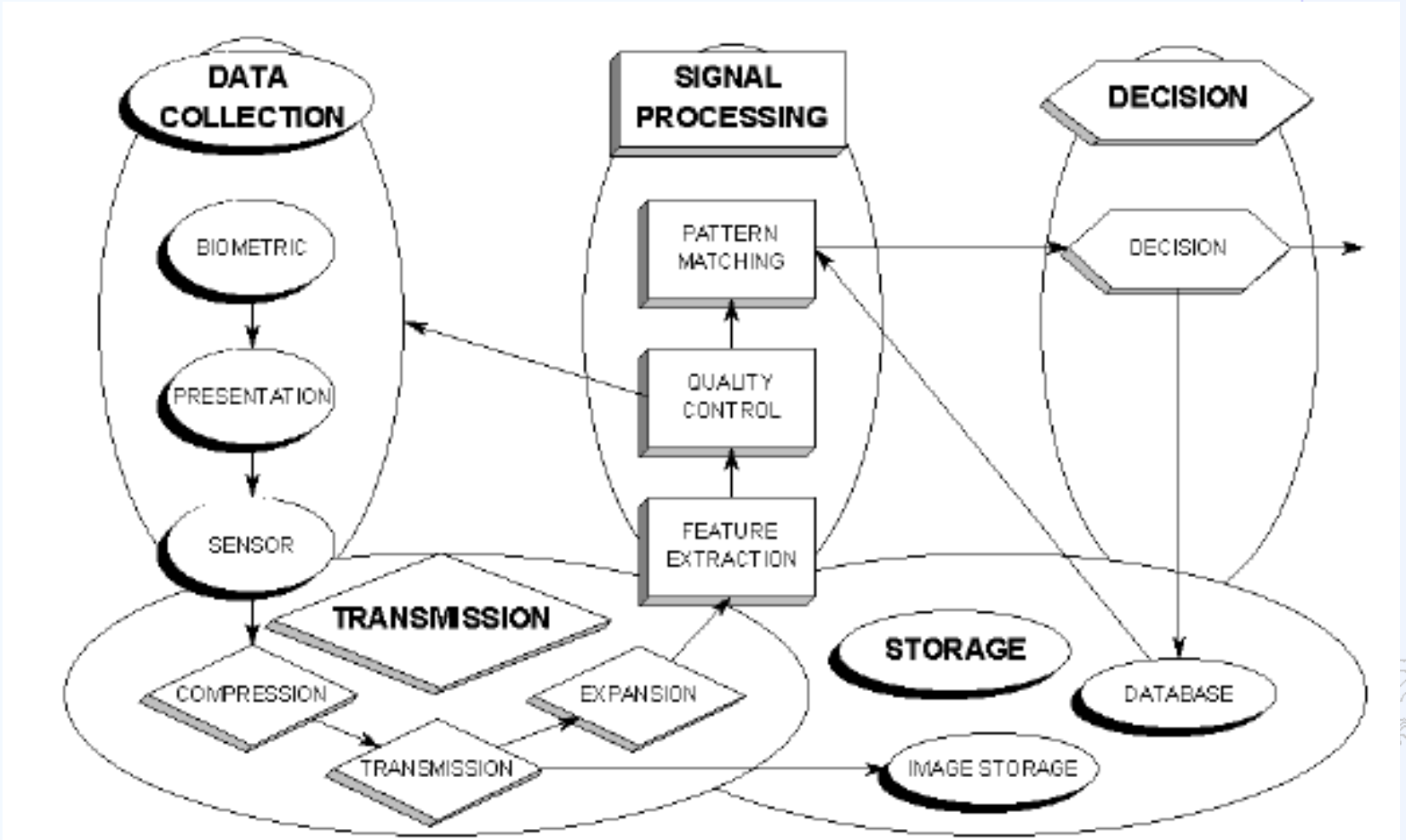




Three basic means



Generic Biometric System

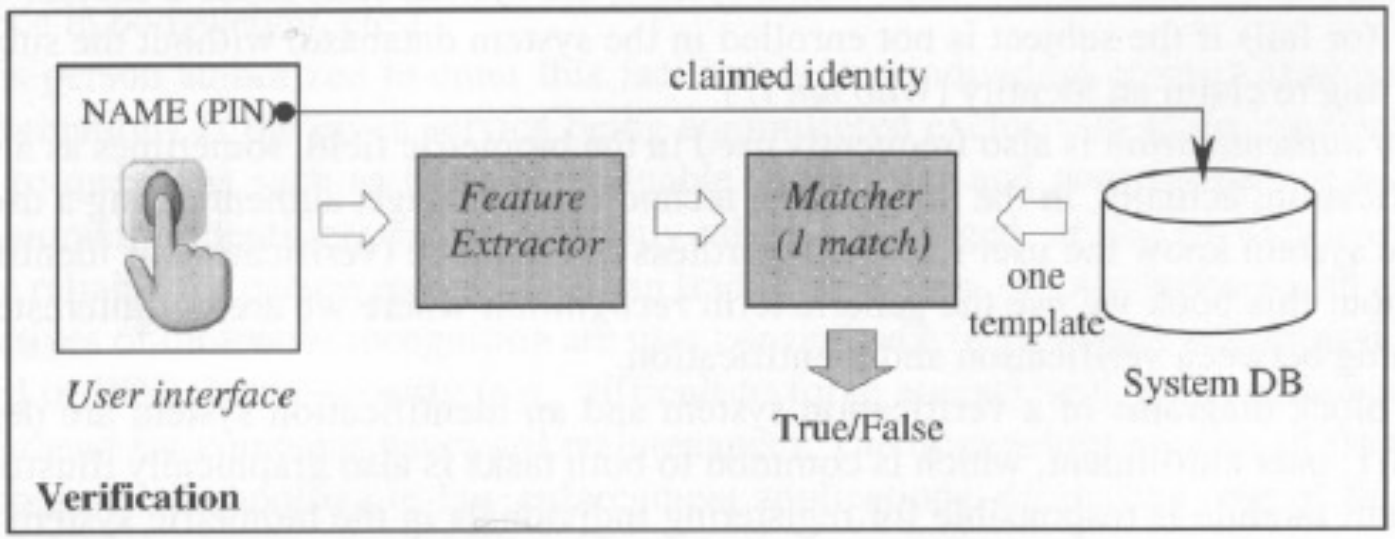


Pattern Recognition System

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

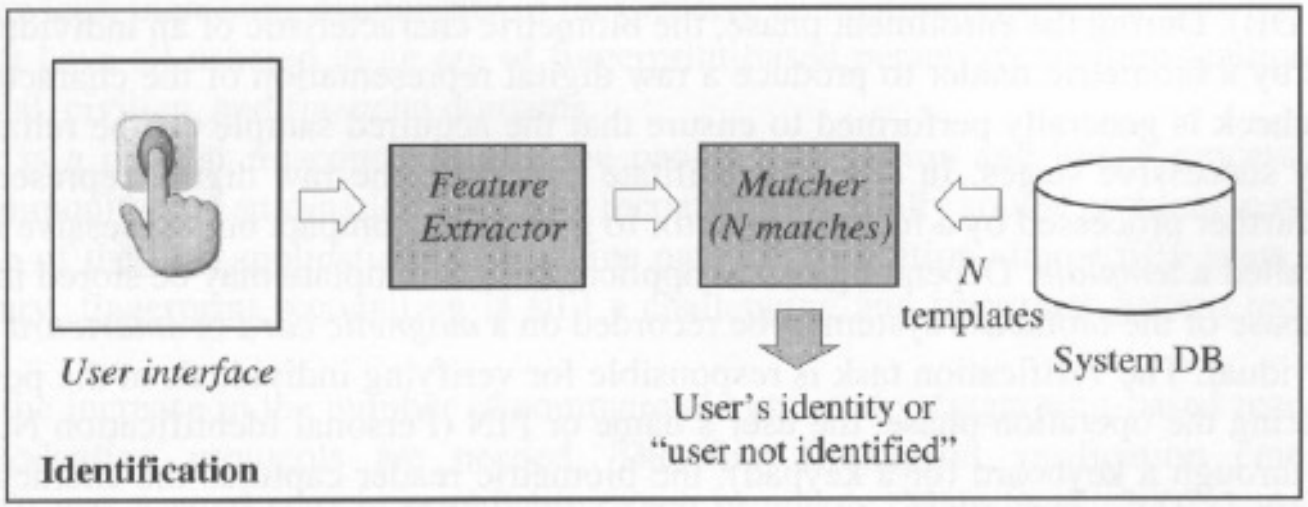
Person recognition

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



Identification

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



Example Iris & Speech

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

Main Sorting

Biometrics can be sorted into two classes:

- Physiological

  Examples: face, fingerprint, hand geometry and iris recognition

- Behavioral

  Examples: signature and voice

Biometric Identifiers

Common:

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

Others:

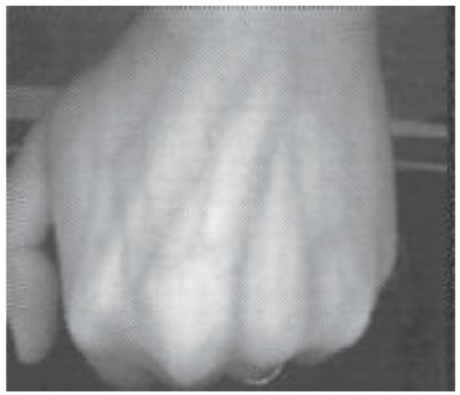
- DNA
- Retina recognition
- Thermograms
- Gait
- Keystroke
- Ear recognition
- Skin reflection
- Lip motion
- Body odor

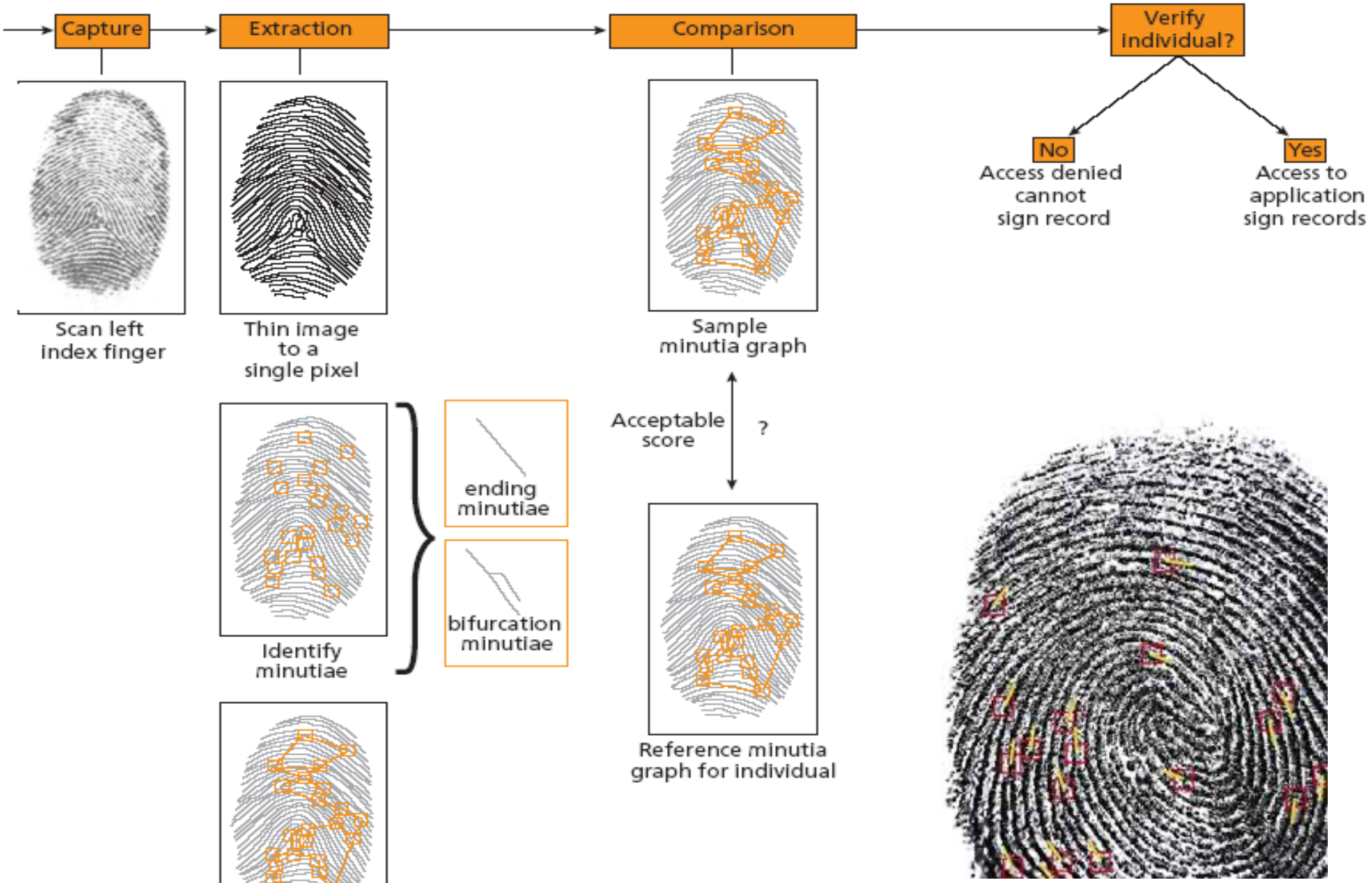
laboratory Gerstner

Some More* …

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

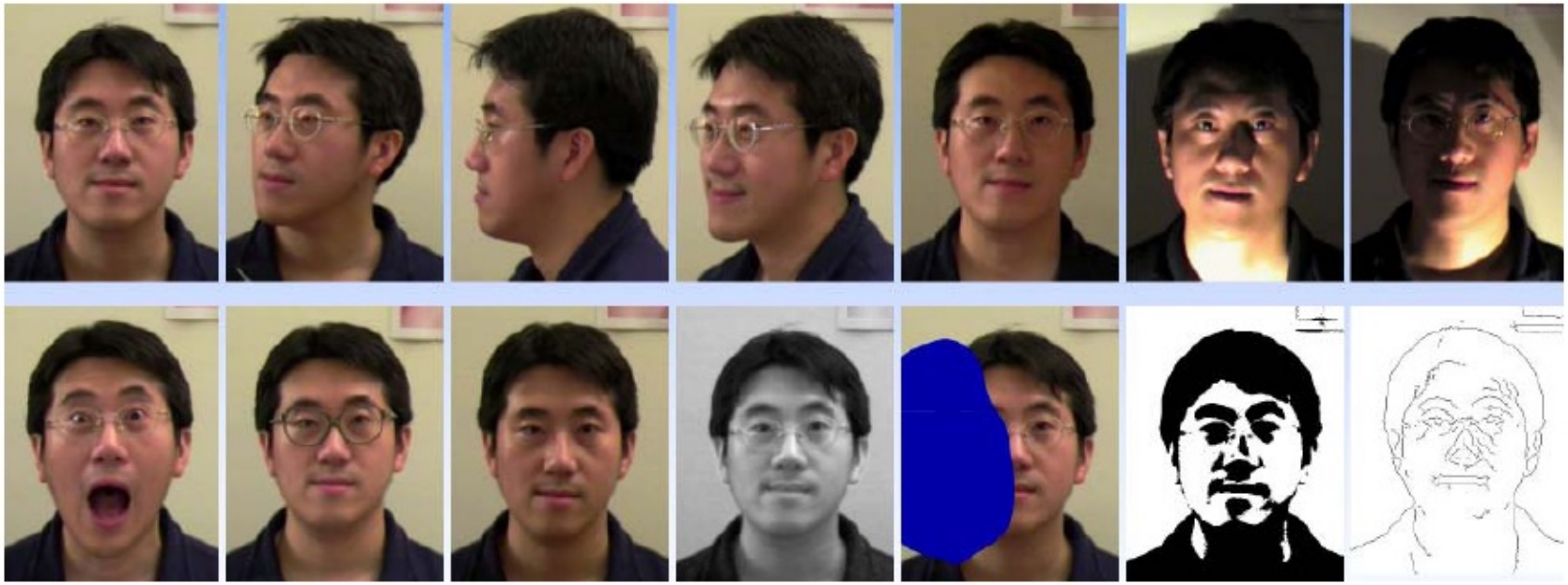
•*See details in ***Chapter 7 Esoteric Biometrics*** of ***Biometrics*** by John D. Woodward, Nicholas M. Orlans, Peter T. Higgins, New York : McGraw-Hill/Osborne, c2003




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

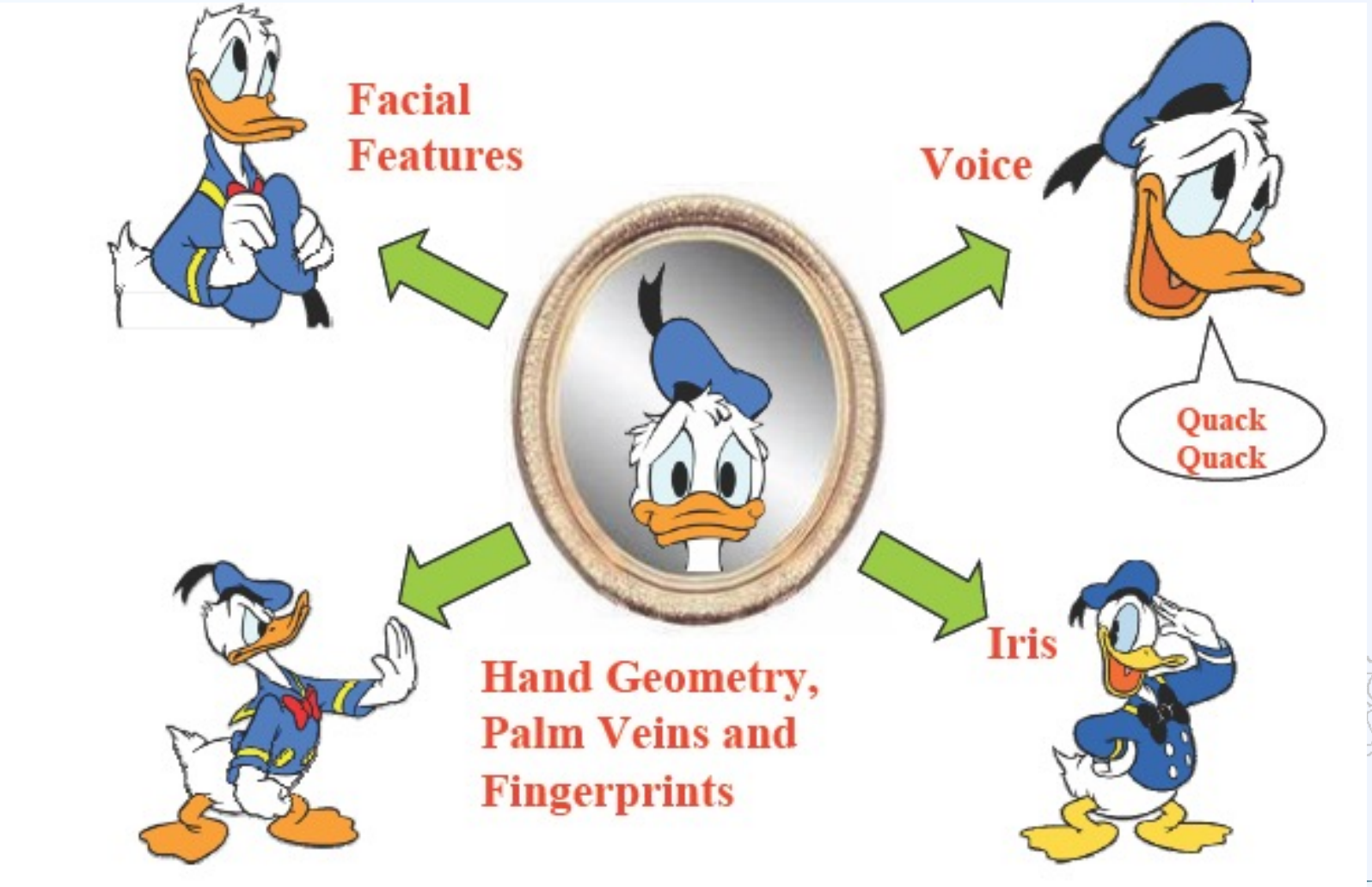
Intra-class variability

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

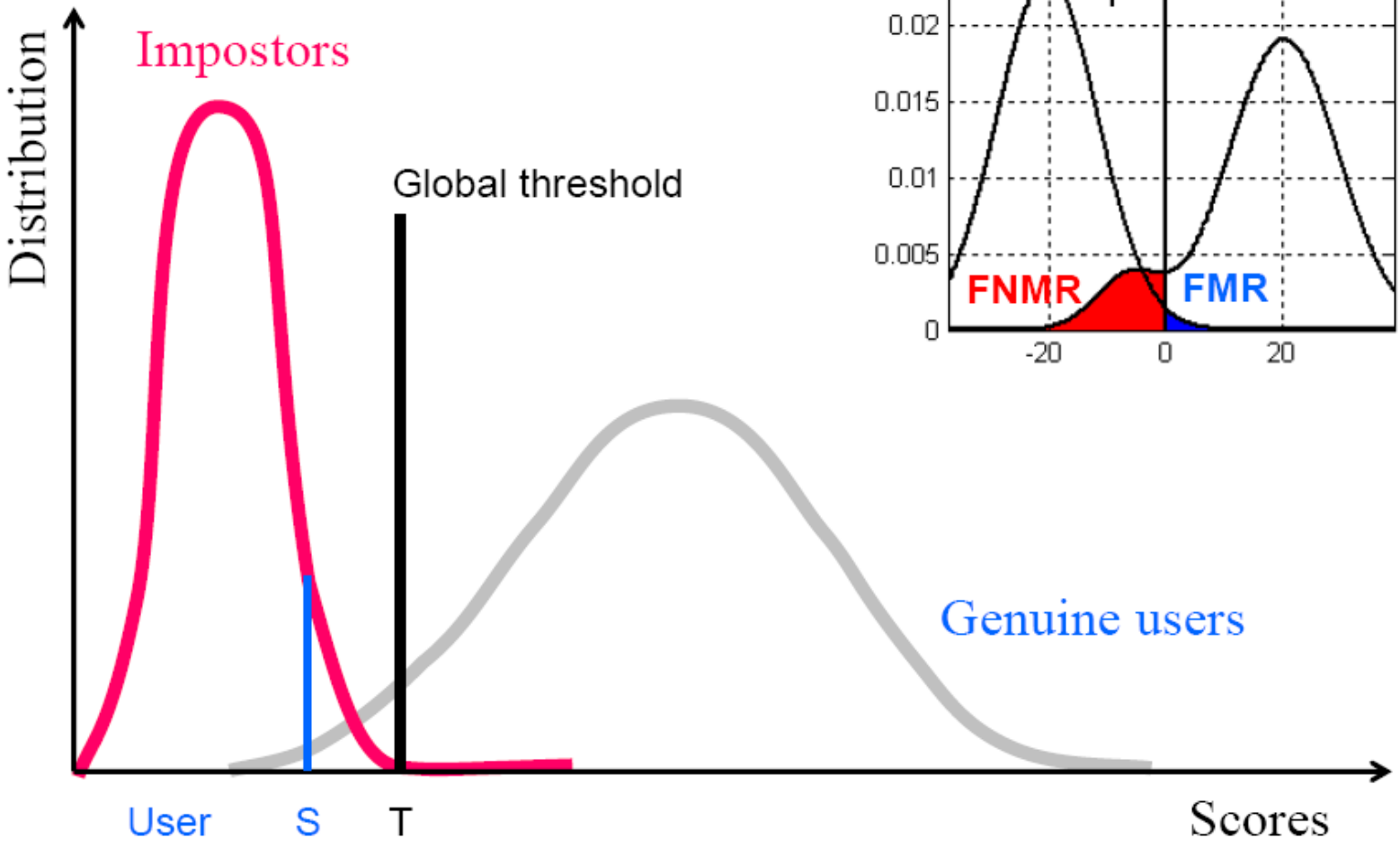


The power of make up

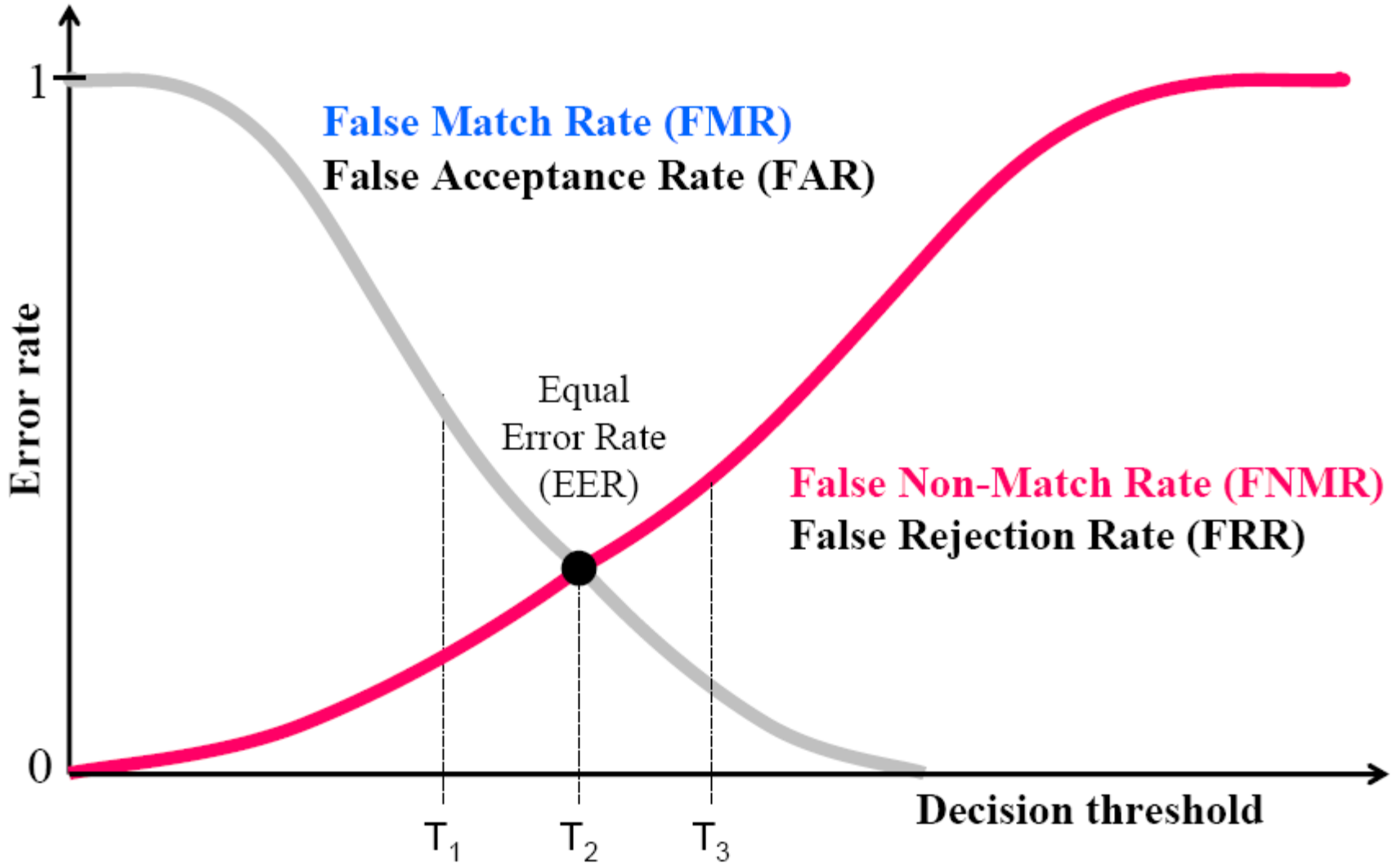
Multimodal Biometrics



Performance evaluation



FMR and FNMR

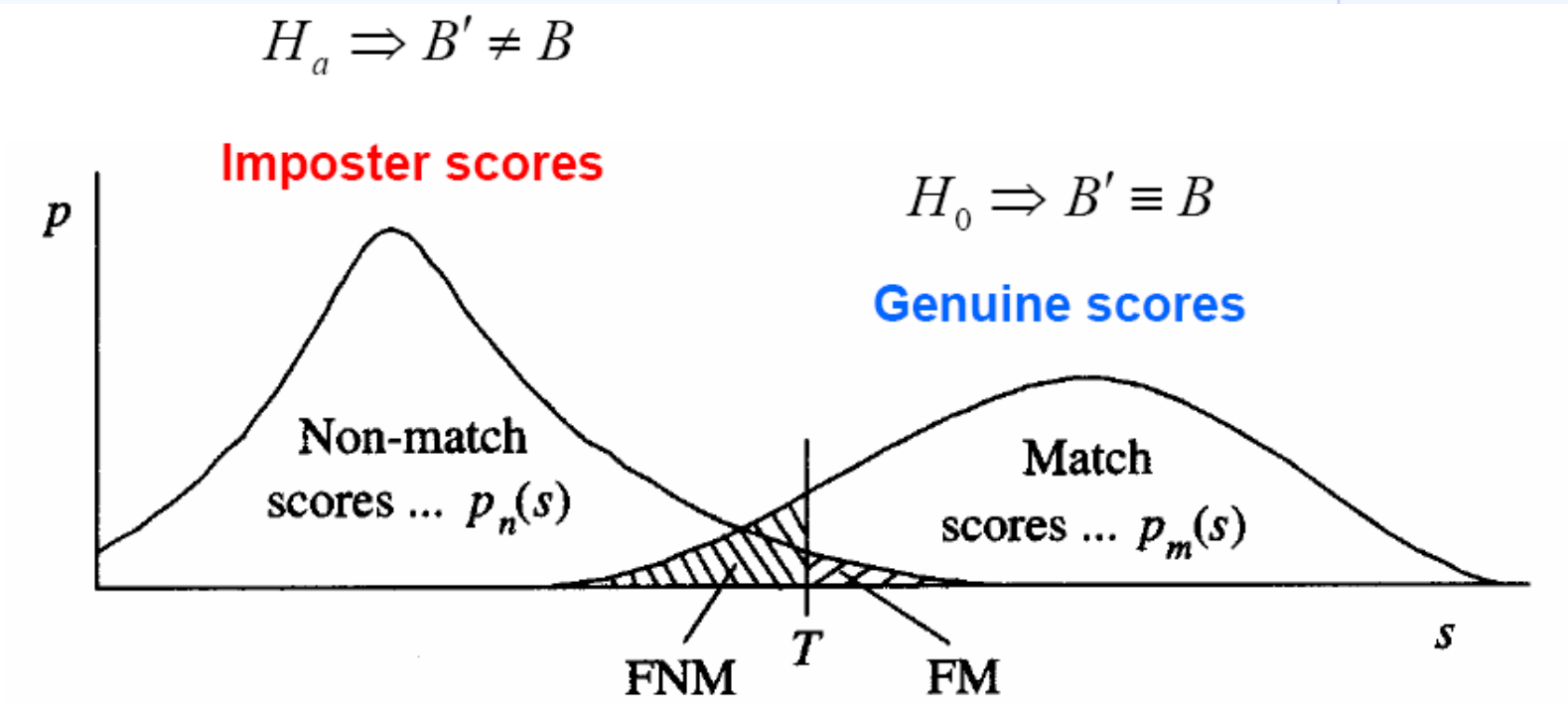

1
0
Error rate
False Match Rate (FMR)
False Acceptance Rate (FAR)
Equal
Error Rate
(EER)
False Non-Match Rate (FNMR)
False Rejection Rate (FRR)
T1
T2
T3
Decision threshold

FA & FR

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

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

Scores distribution



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

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

Two kinds of error

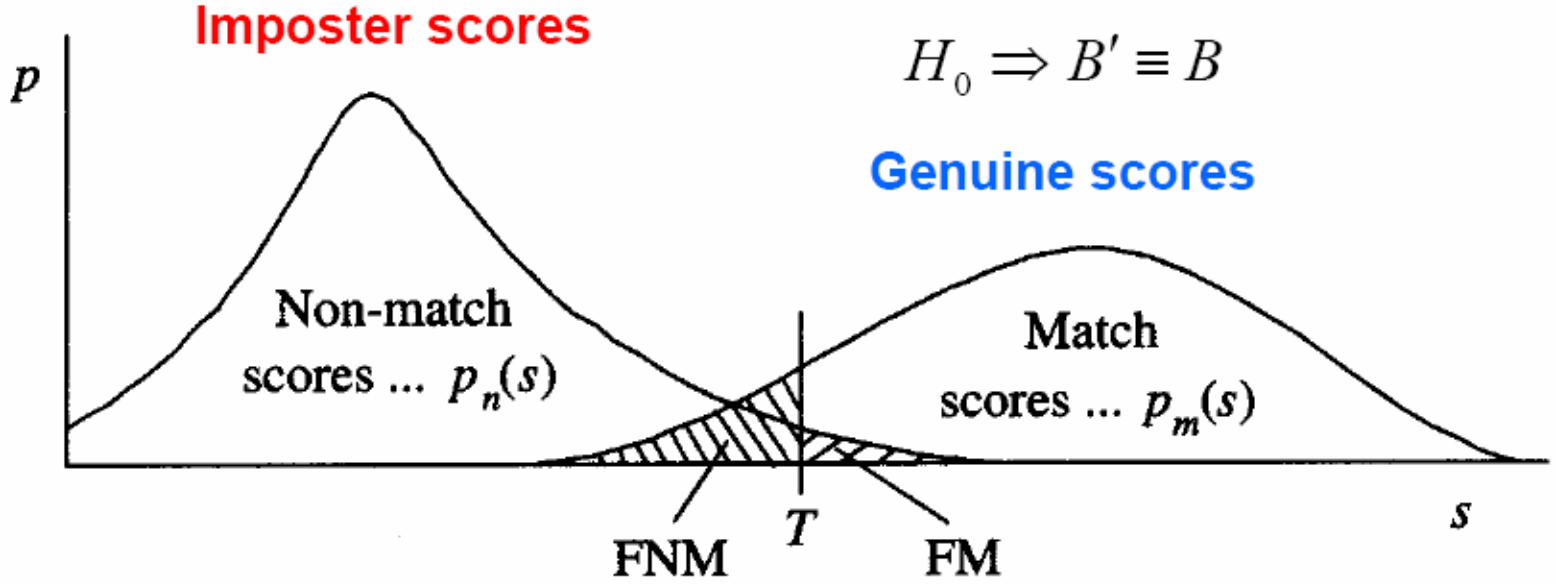
- Verification:

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

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

Two kinds of error

$$H_a \Rightarrow B' \neq B$$



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

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

Errors & Accuracy

- There are about 30 minutiae: the U.S. Federal Bureau of Investigation (FBI) has evidenced that no two individuals can have more than **eight minutiae** in common

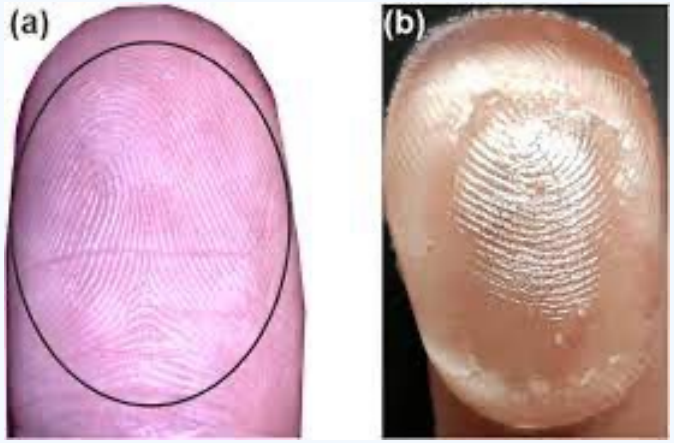
- NIST found that 0.2% of searches in a database of 26.6 photos failed to match the correct image, compared with a 4% failure rate in 2014.
- In NIST'S 2020 tests, the best algorithm had a failure rate of 0,08%.

- 50x improvement over six years

- In July 2018, Newsweek reported that Amazon's facial recognition technology falsely identified **28 US Congress members as people arrested for crimes.**

laboratory Gerstner

Liveness in biometrics



gelatin fingerprints, fake irises, and special glasses

Privacy - camera towers

Privacy – Hong Kong

Privacy – Hong Kong

Privacy – Hacking

Camouflaged Fashion

This design combines unconventional hairstyling and makeup to create an anti-face, an attempt to block facial recognition software.

USE TONAL INVERSE

Some algorithms will analyze gradations in skin tone and texture. This process helps locate the facial region, but it relies on assumptions about what typical facial features look like. To confuse this process, use hair or makeup that contrasts with your skin tone and apply makeup in unusual tones and directions: light colors on dark skin, dark colors on light skin.

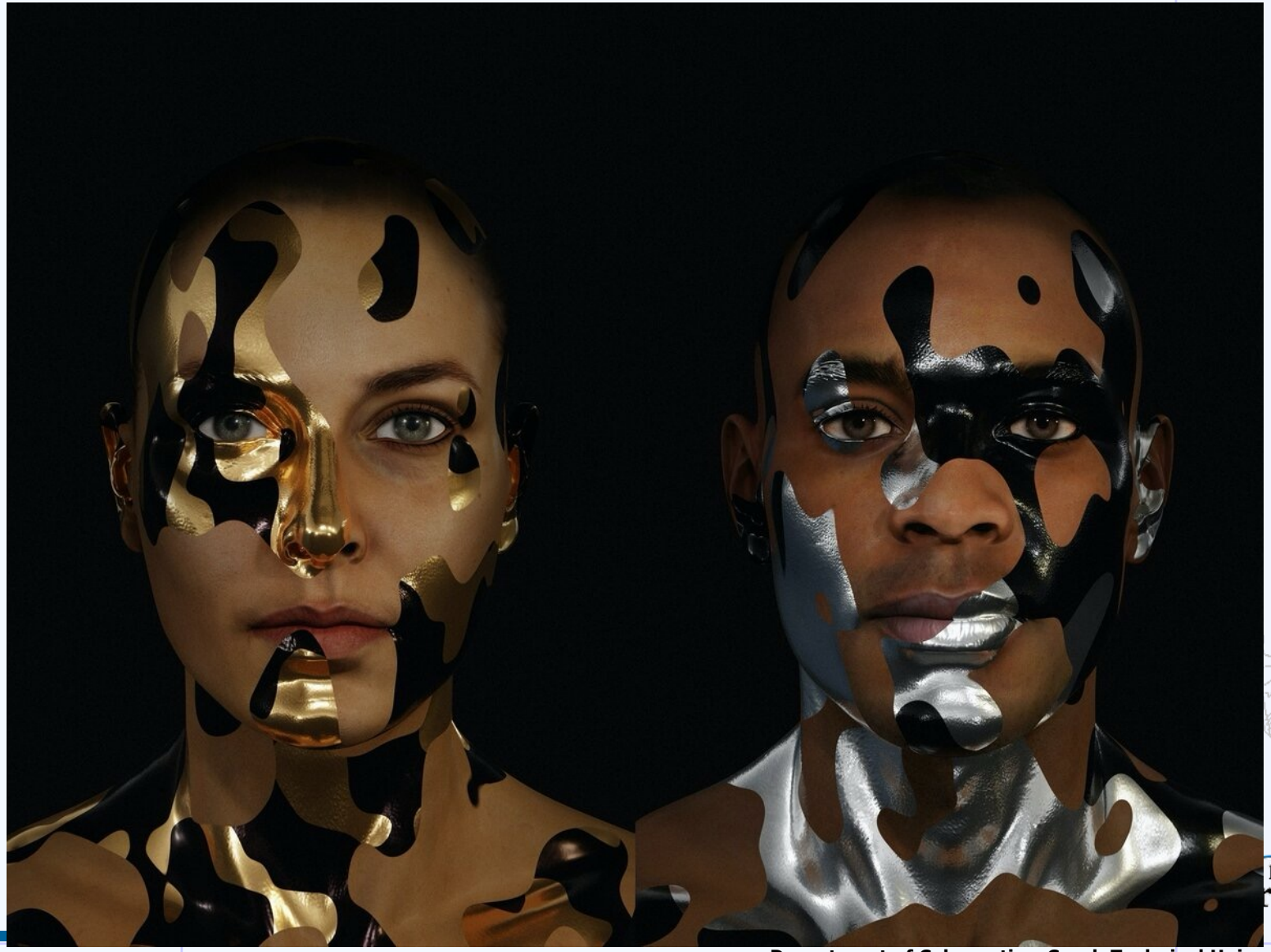
CREATE ASYMMETRY

Facial-recognition algorithms expect symmetry between the left and right sides of the face. By developing an asymmetrical look, you may decrease your probability of being detected.

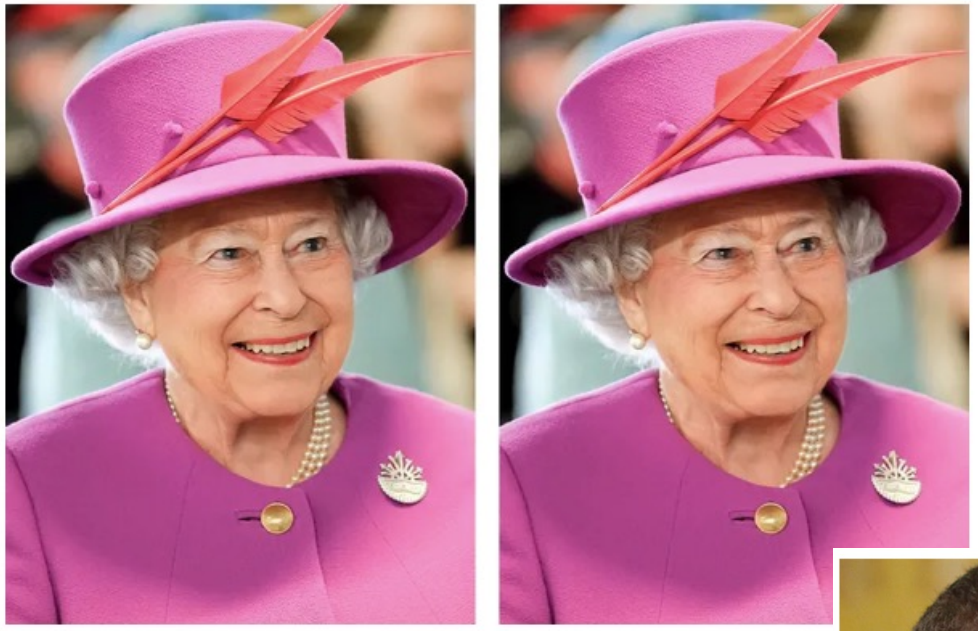
CONCEAL THE NOSE BRIDGE

Some algorithms rely on the nose bridge area as a key facial marker. Use hairstyling or fashion accessories to conceal the area above the nose and between the eyes.

Privacy – Hacking



Privacy – Cloaking



http://sandlab.cs.uchicago.edu/fawkes/#code

SAND Lab
security, algorithms, networks and data