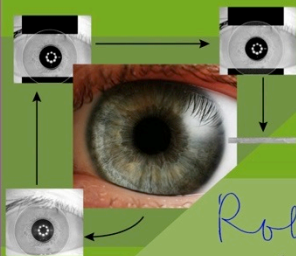


Nový předmět katedry kybernetiky, FEL ČVUT

# BIOMETRIE (A6M33BIO)



Předmět je zaměřen na výklad nejpoužívanějších metod v biometrii. Sami si naimplementujete dynamické rozpoznávání podpisu, detekce vlastního otisku prstu či duhovky!

Disponujeme profesionálním vybavením, pracujeme v Matlabu s předpřipravenými skripty, neztrácíte zbytečně čas na na cvičeních. Soustředíme se na bezpečnostní rizika biometrických systémů. Pro každý biometrický systém je provedeno vyhodnocení z hlediska rychlosti, ceny a přesnosti.

Předmět doporučujeme zejména studentům oborů Otevřená informatika, Kybernetika a robotika a Biomedicínská informatika & inženýrství.

Zdroje duhovka - Petr Novák, Wikipedia  
podpis - databáze SVČ2004

? Jak funguje snímač otisku prstů?

? Proč se neujalo rozpoznávání hlasu?

? Lze jednoduše prolomit biometrický systém?

? Proč je detekce duhovky nejpřesnější metodou?



[www.predmet-biometrie.cz](http://www.predmet-biometrie.cz)

Kontakt:  
Ing. Daniel Novák, Ph.D.  
Katedra kybernetiky, ČVUT FEL  
Technická 2, 166 27 Praha 6  
Tel.: 22435 7314  
xnovakd1@fel.cvut.cz

# Biometrics Introduction

Daniel Novák

5.10.2023, Prague

Acknowledgments:  
Chang Jia, [Andrzej Drygajlo](#)



laboratory  
**Gerstner**



# Podmínky předmětu

- Garant předmětu: Daniel Novák, místnost G202, [xnovakd1@fel.cvut.cz](mailto: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>

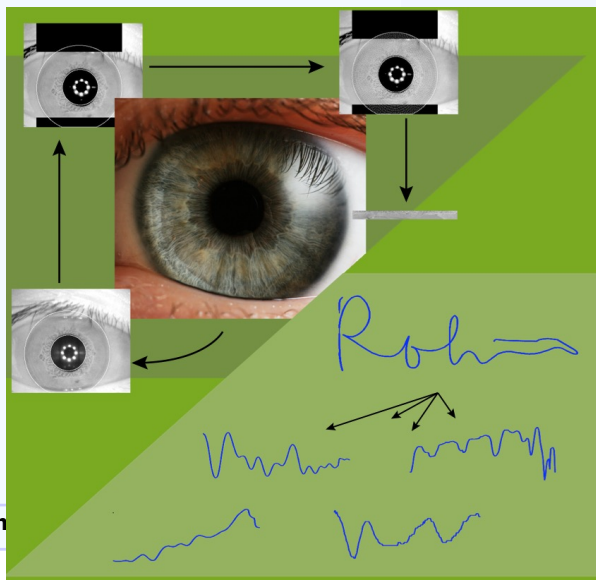
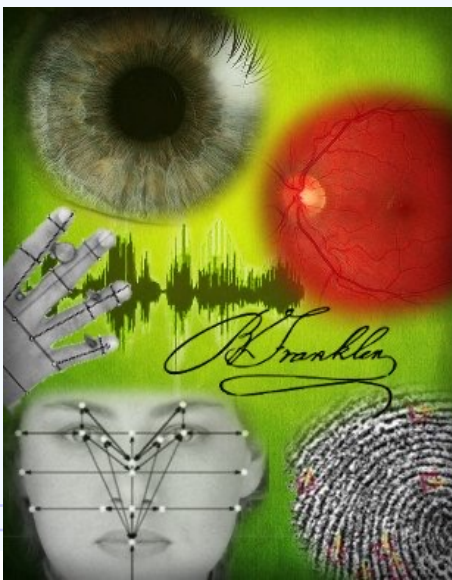
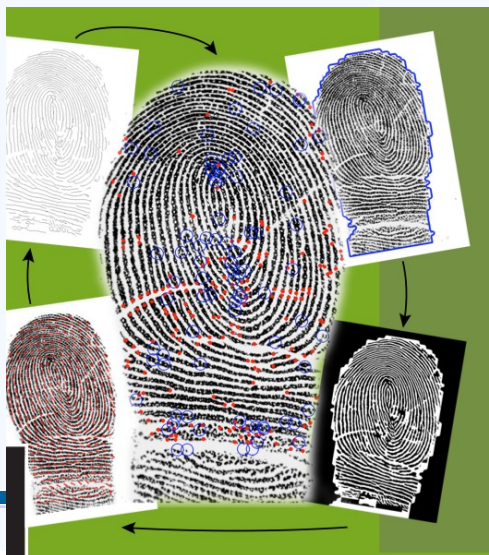
Body z předmětu	Stupeň ECTS	Známka
100–90	A	výborně
89–80	B	velmi dobře
79–70	C	dobře
69–60	D	uspokojivě
59–50	E	dostatečně
49 a méně	F	nedostatečně





# 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.independent.co.uk> > [topic > biometrics](#)



# Najdete něco zajímavého



INDU/LIRC

The Facebook logo is seen on an Apple iPhone on 28 August, 2017 (Getty)



laboratory  
erstner



# Proč Biometrie ?



"I'm sorry, but someone else with that identity is already here."



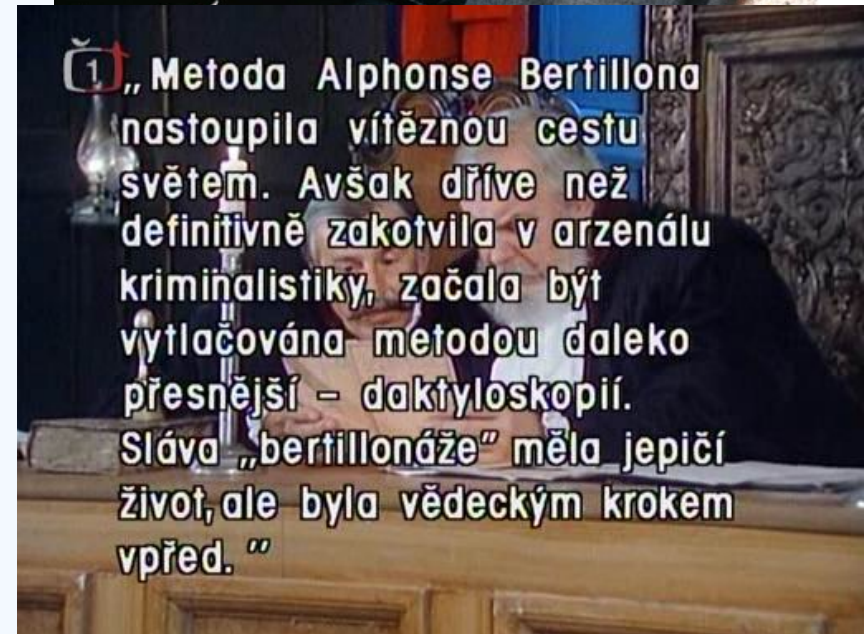
laboratory  
**Gerstner**

Technical University

# Alternativní úvod



- [Dobrodužství kriminalistiky](#) na csfd
- [Dobrodužství kriminalistiky](#) na CT

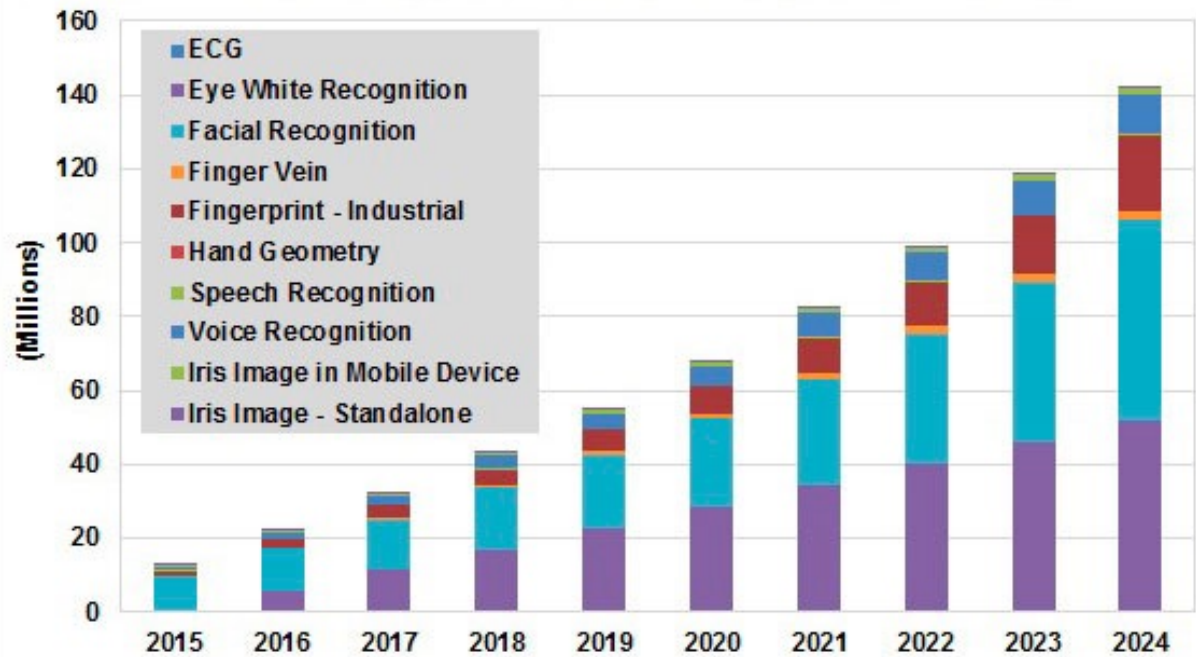






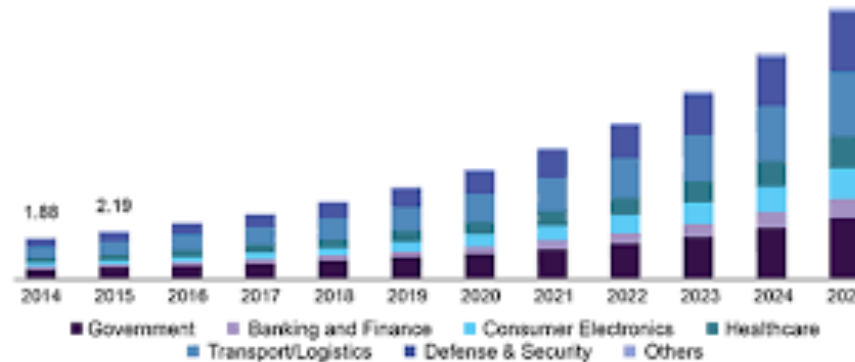
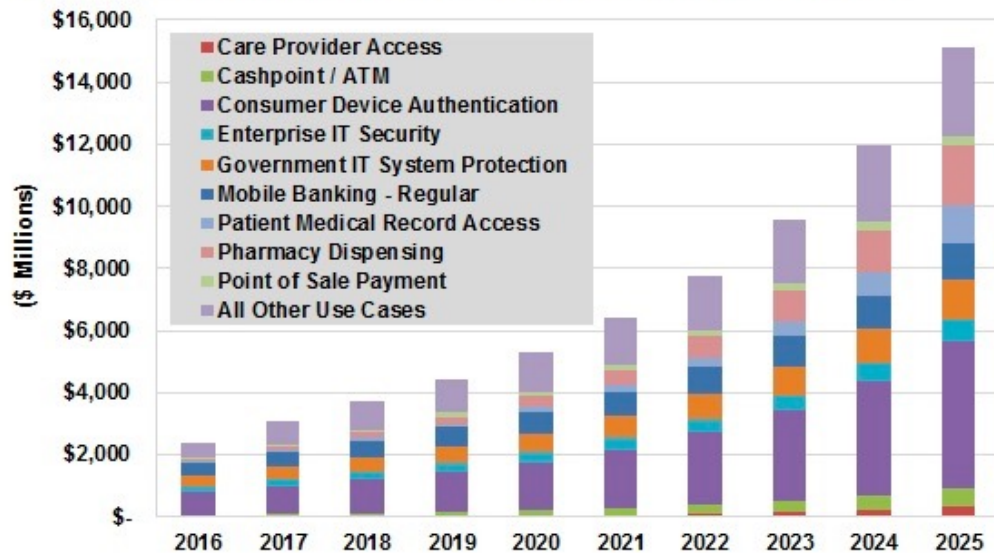
- [http://cs.wikipedia.org/wiki/Alphonse\\_Bertillon](http://cs.wikipedia.org/wiki/Alphonse_Bertillon)
- [http://cs.wikipedia.org/wiki/Dreyfusova\\_af%C3%A9ra](http://cs.wikipedia.org/wiki/Dreyfusova_af%C3%A9ra)

# Trend



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

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



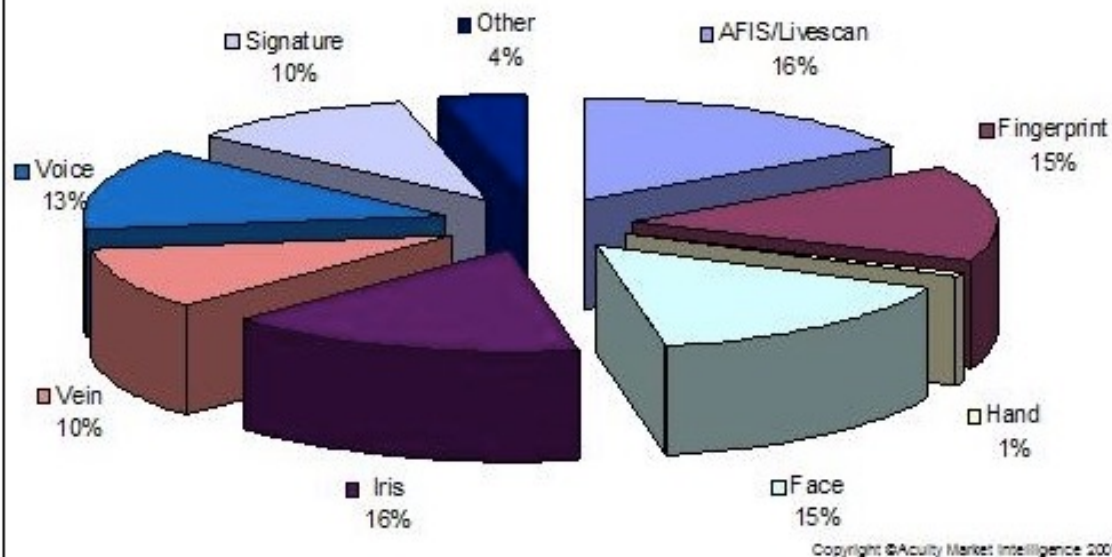
Source: www.gandienresearch.com



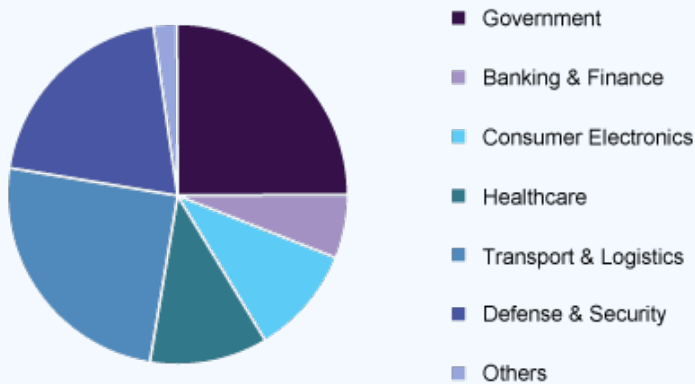


# Market Share

## Global Market by Technology 2015



## Europe contactless biometrics technology market share, by end use, 2019 (%)



laboratory  
**Gerstner**

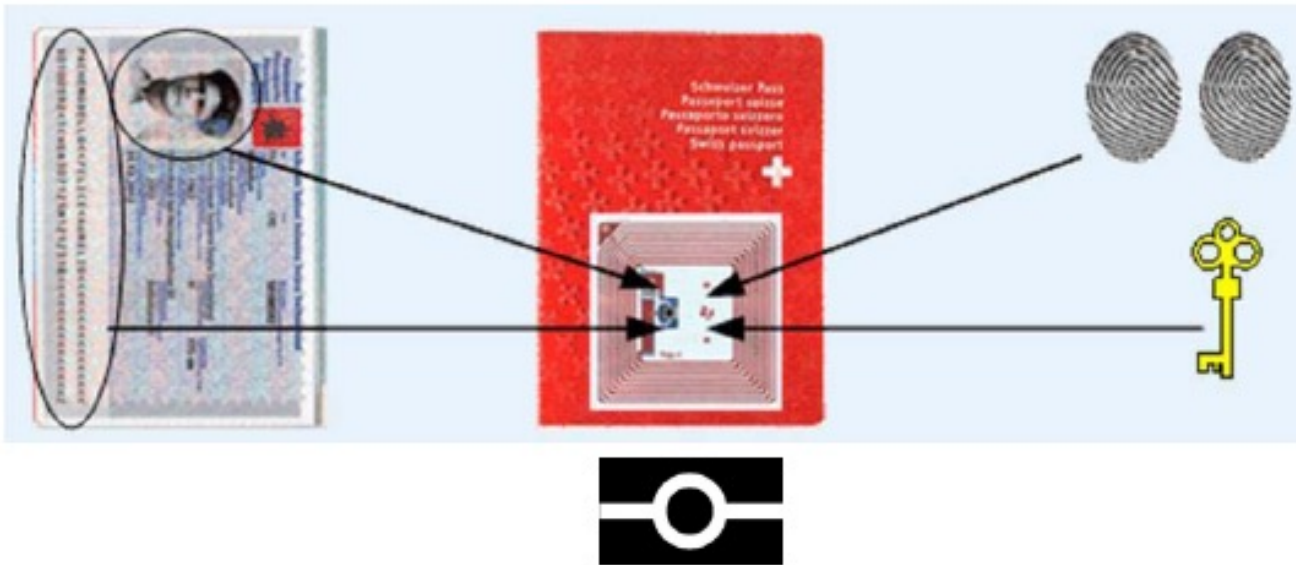
# ePassport – Biometrický pas

**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://czech.prague.usembassy.gov/biometricky_pas.html)

[http://www.youtube.com/watch?v=ptb\\_nxCpgYQ](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





# 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

## AADHAAR: HOW IT WORKS AND HOW IT'S EVOLVED

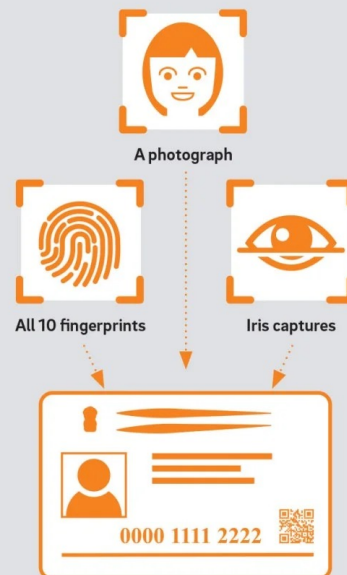
### The enrolment process

To ensure that each person receives only one Aadhaar number, the UIDAI (Unique Identification Authority of India) set up a deduplication database built on three features.

The Aadhaar Card is primarily a means of individual identification.

An Aadhaar ID is:

- Universal, digital and secure
- Linkable to multiple applications
- Suitable for use as a banking address



Infographic World bank snapshot 2012; United Nations



laboratory  
**Gerstner**

Roland  
Berger

cal University

# 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

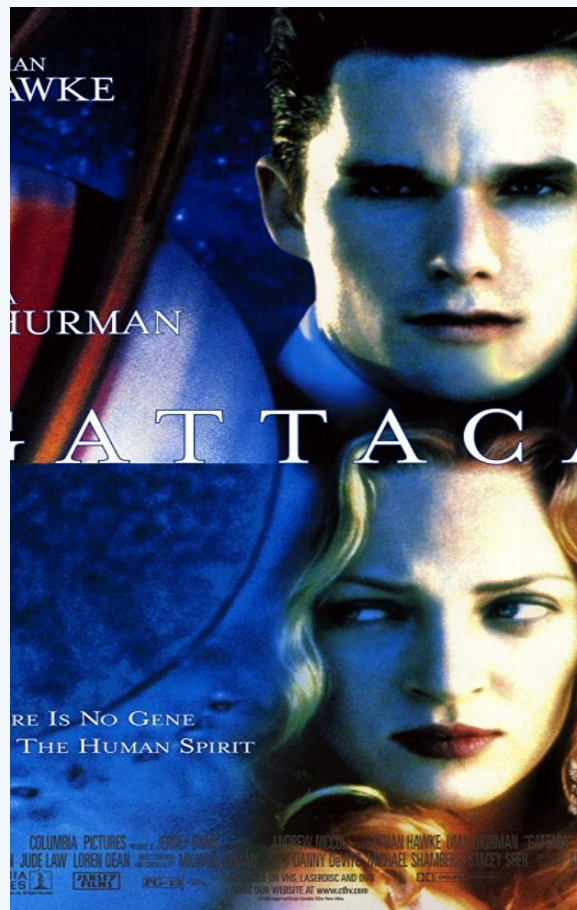
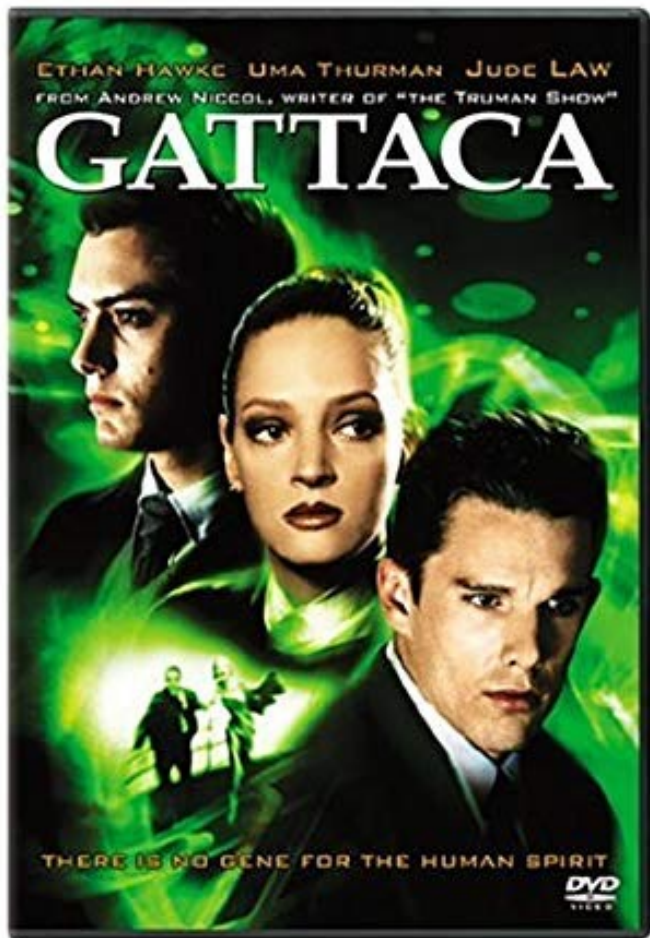




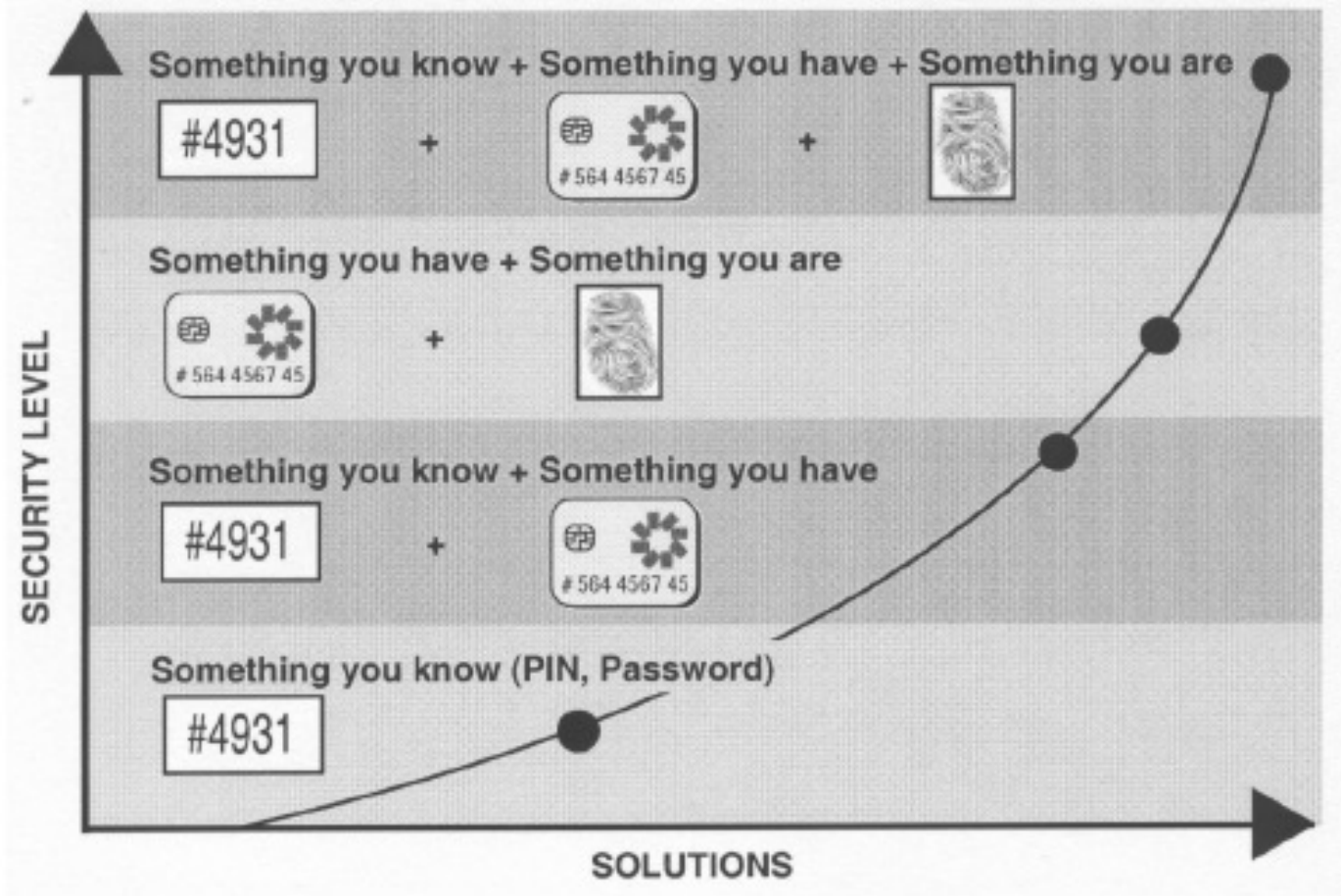
# Další krádež identity



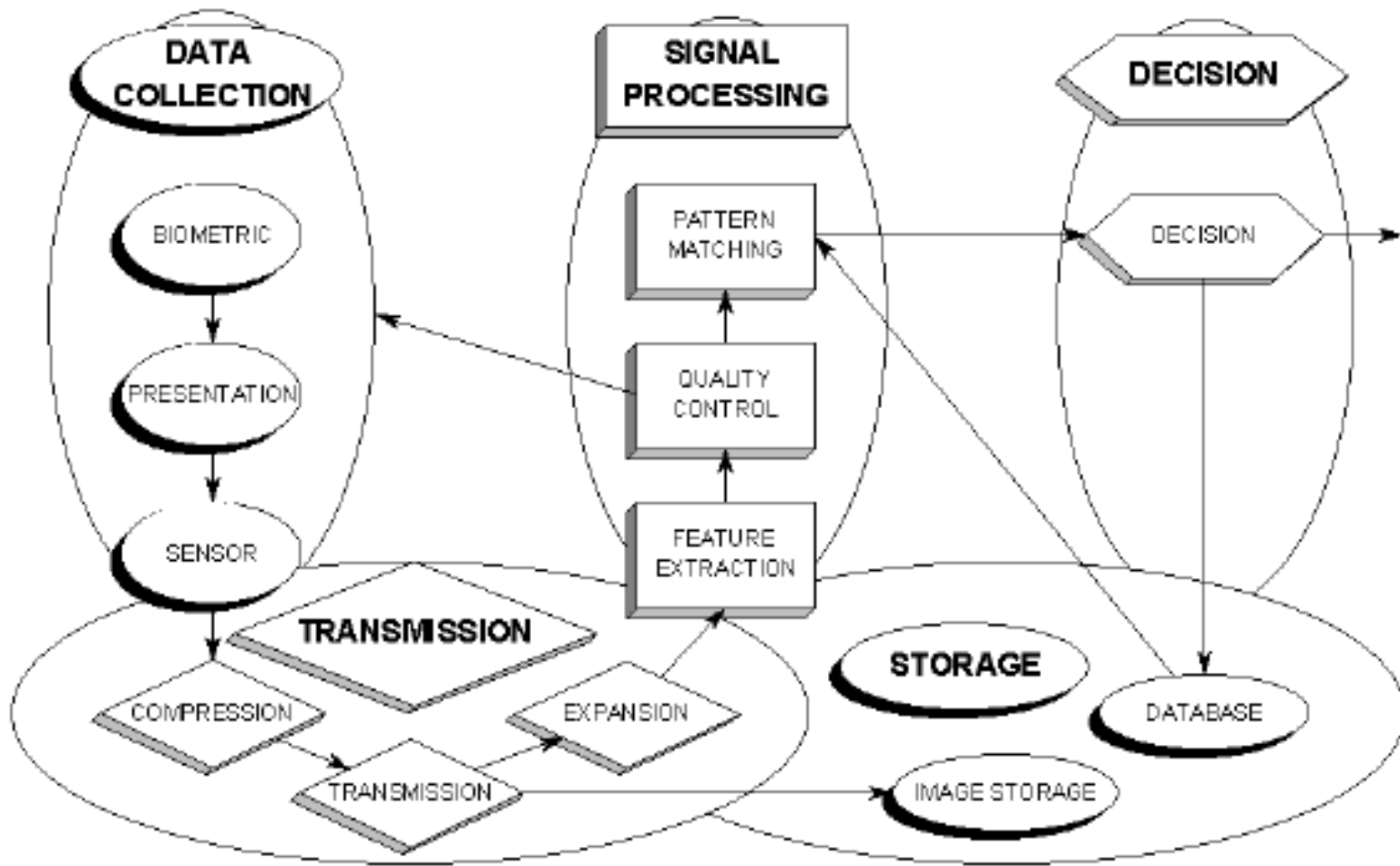
- DU – [Gattaca](#) podívat se a ohodnotit na CSFD (83%)



# Three basic means



# Generic Biometric System







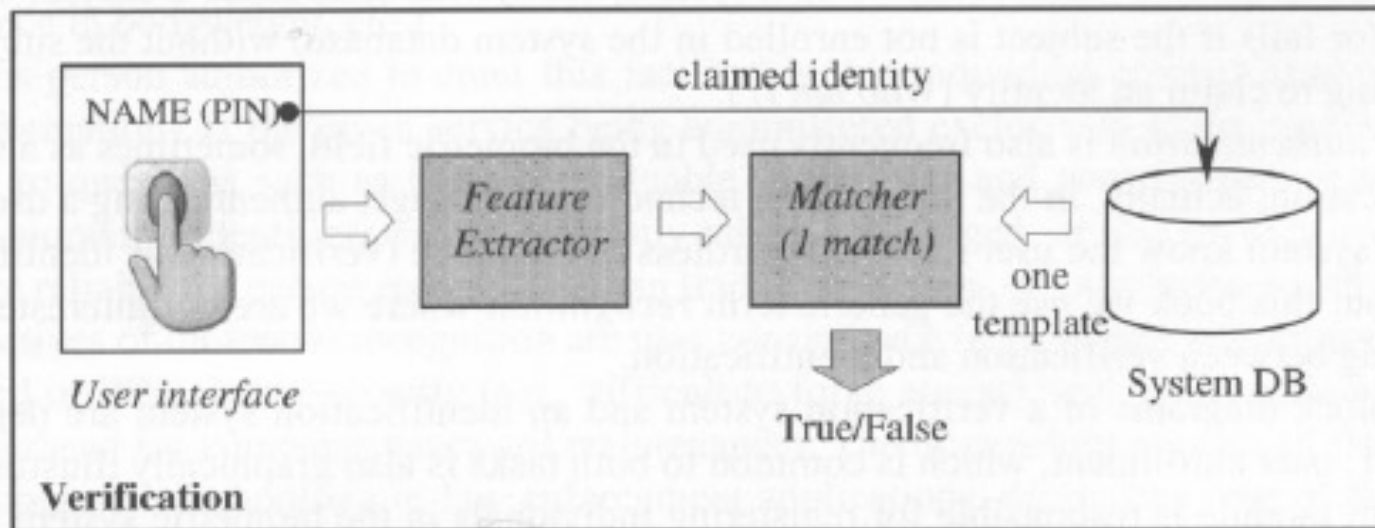
# Pattern Recognition System

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



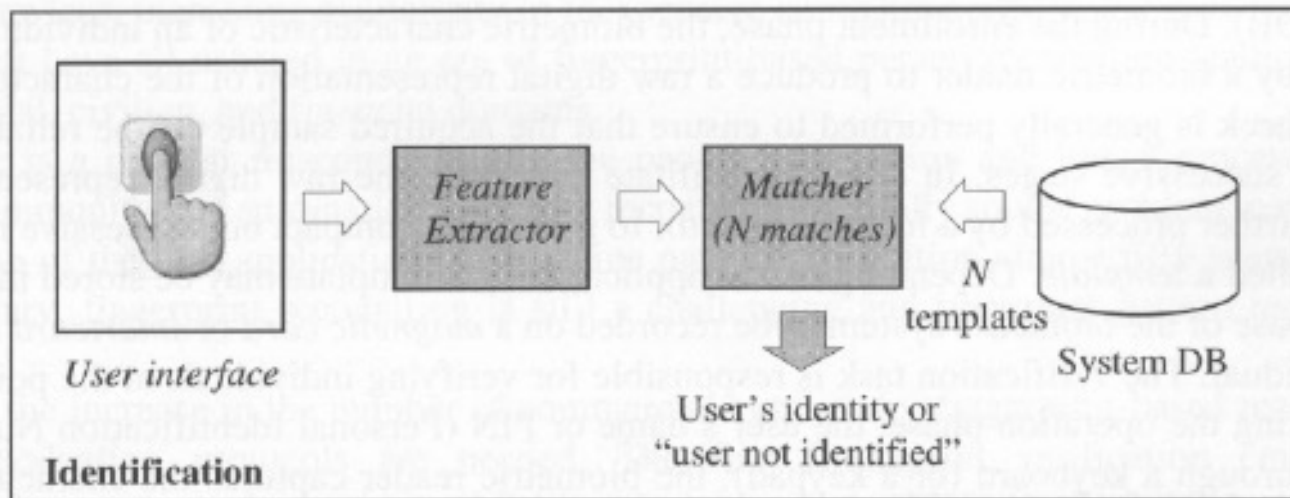
# Person recognition

- **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

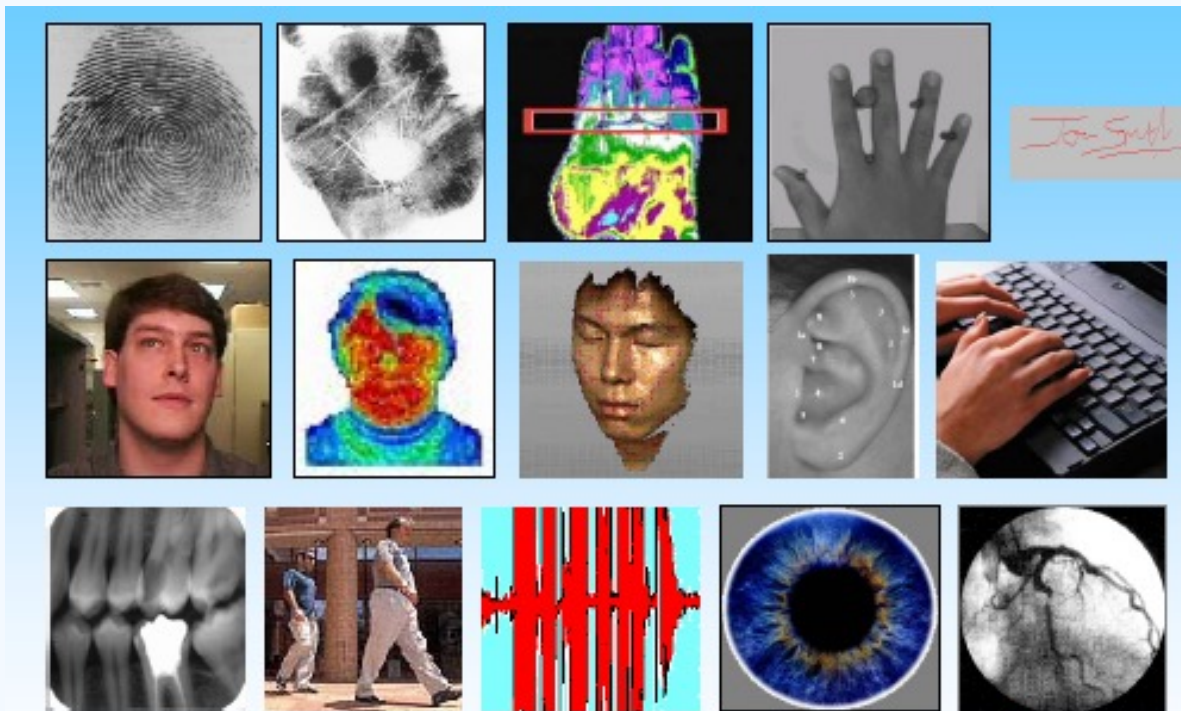
Biometrics can be sorted into two classes:

- 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





# 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?



Scan left index finger



Thin image to a single pixel



Sample minutia graph



Identify minutiae



ending minutiae



bifurcation minutiae



Minutia graph

Acceptable score ?



Reference minutia graph for individual

No  
Access denied  
cannot sign record

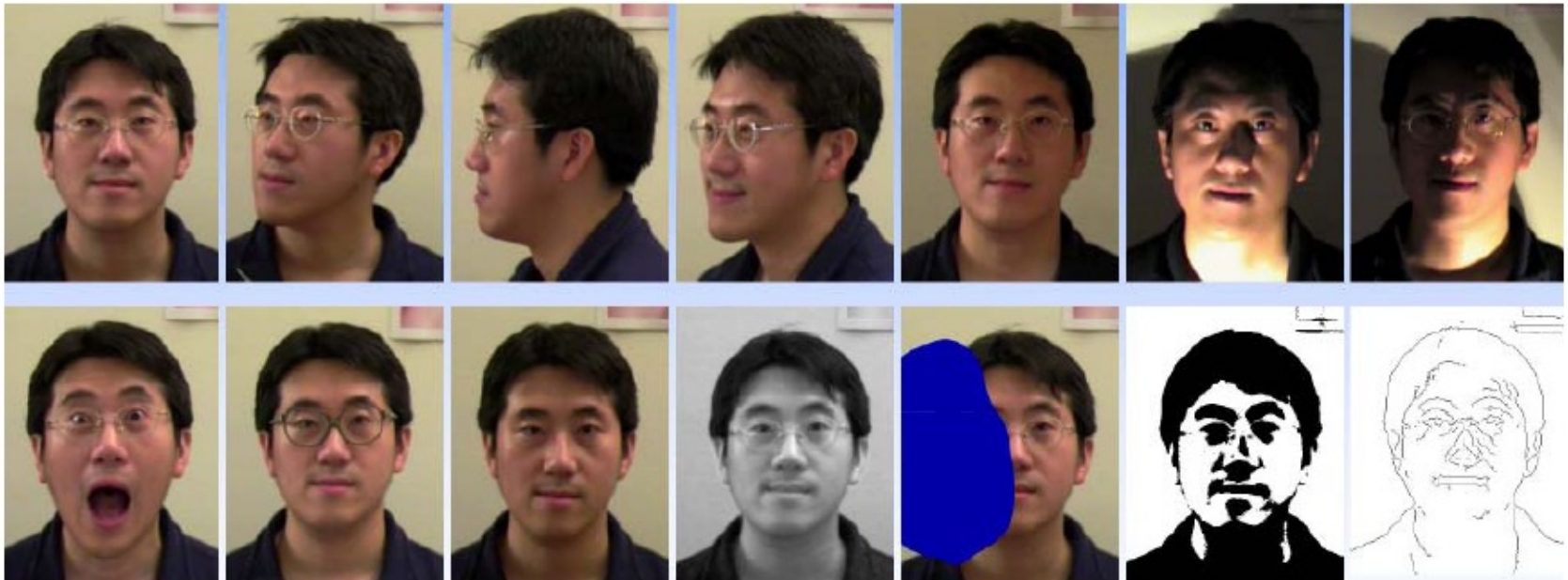
Yes  
Access to application  
sign records





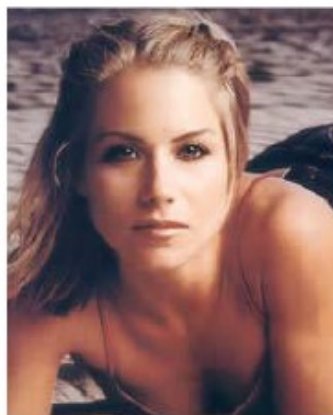
# Intra-class variability

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

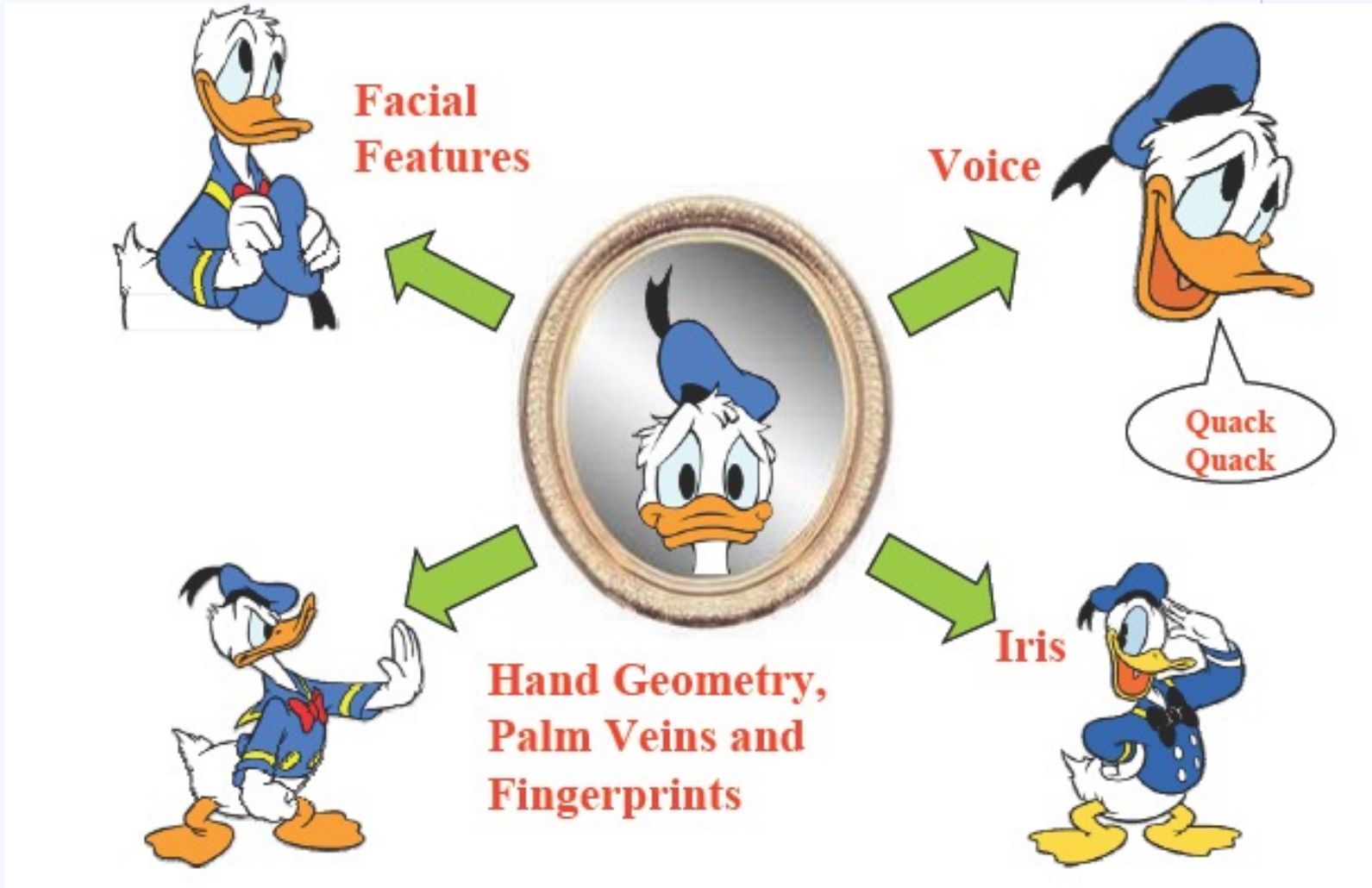




# The power of make up

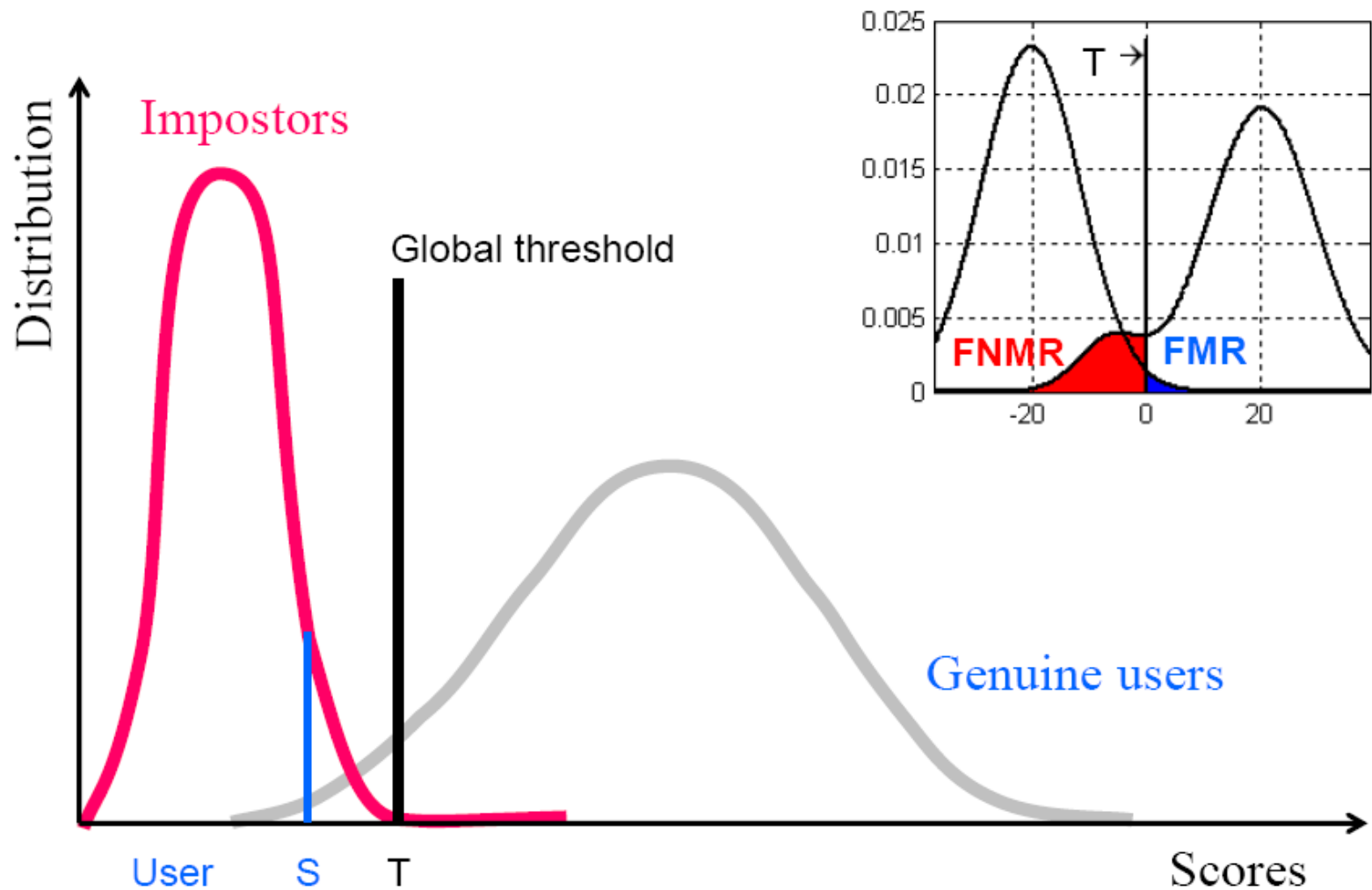


# Multimodal Biometrics





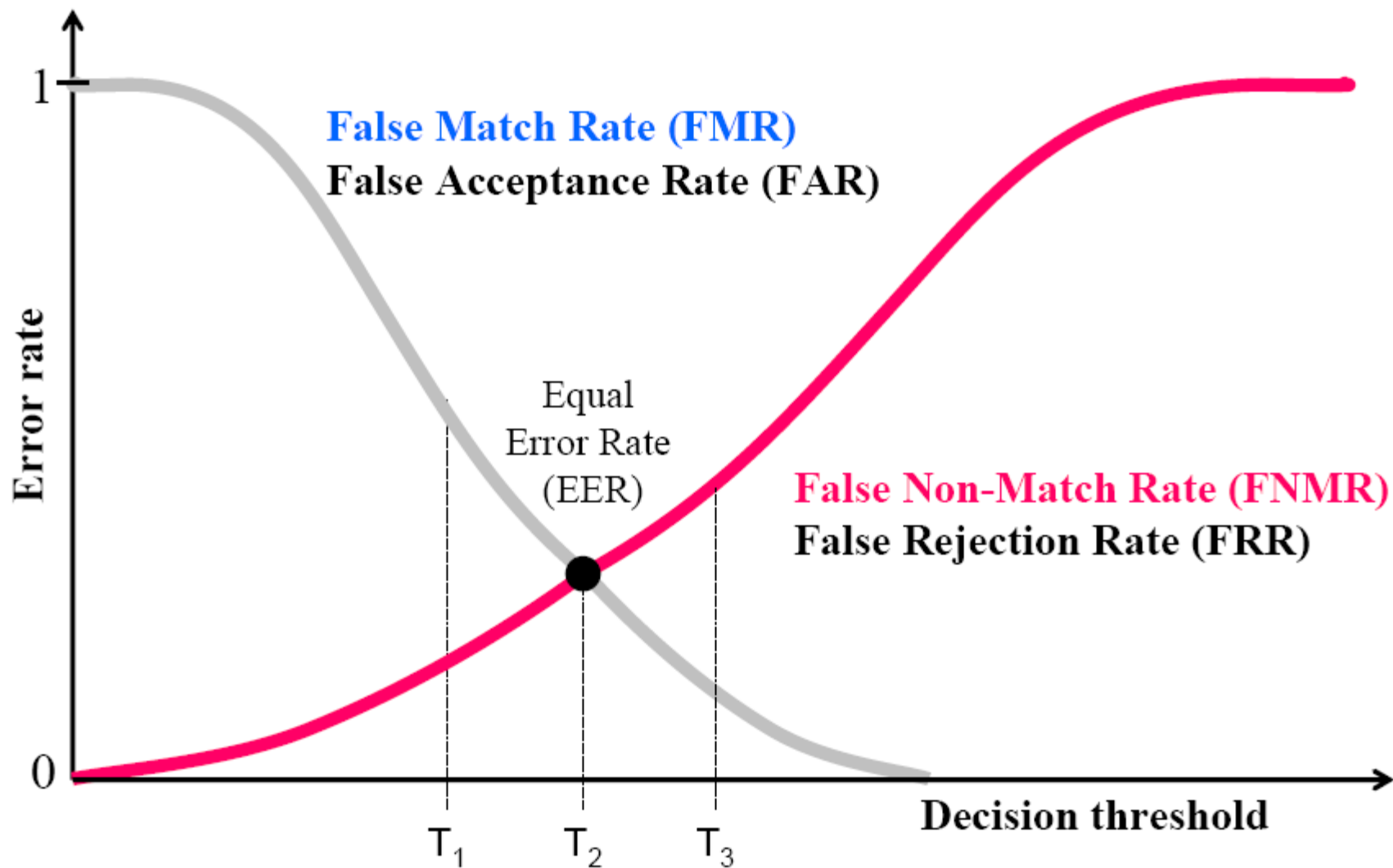
# Performance evaluation







# FMR and FNMR





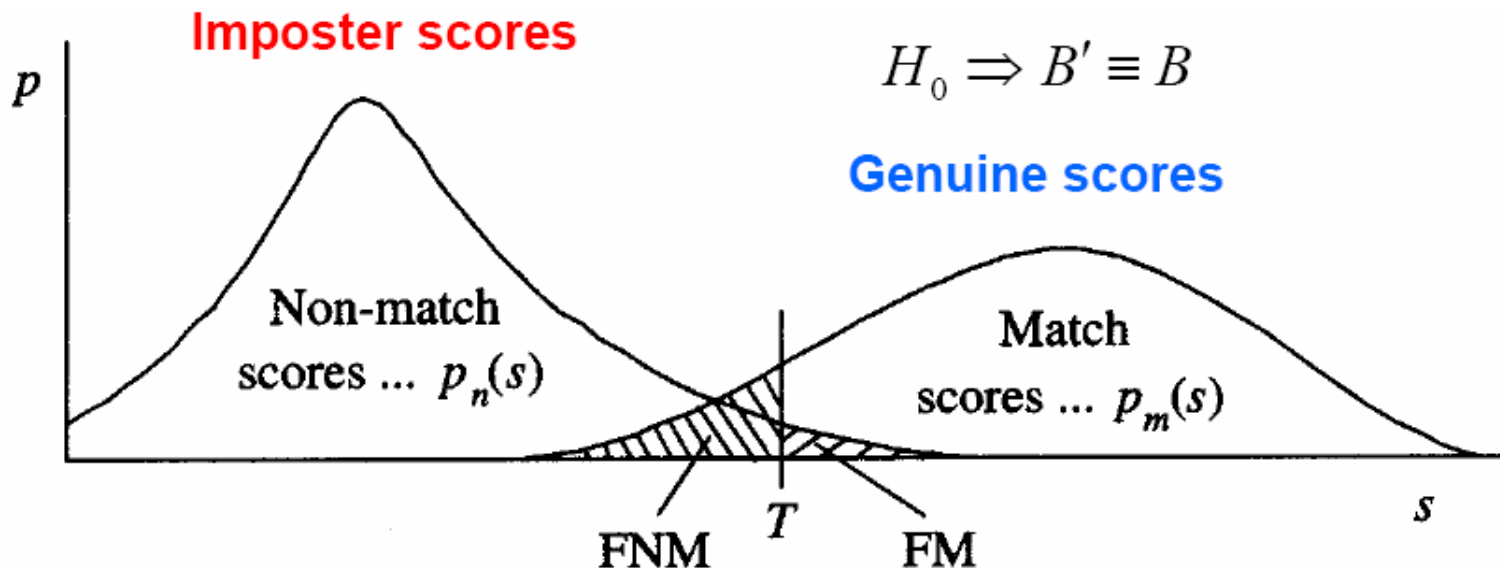
# FA & FR

- **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

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



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:

Decide  $H_0$  is true: if  $s > T$ ,

Decide  $H_a$  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



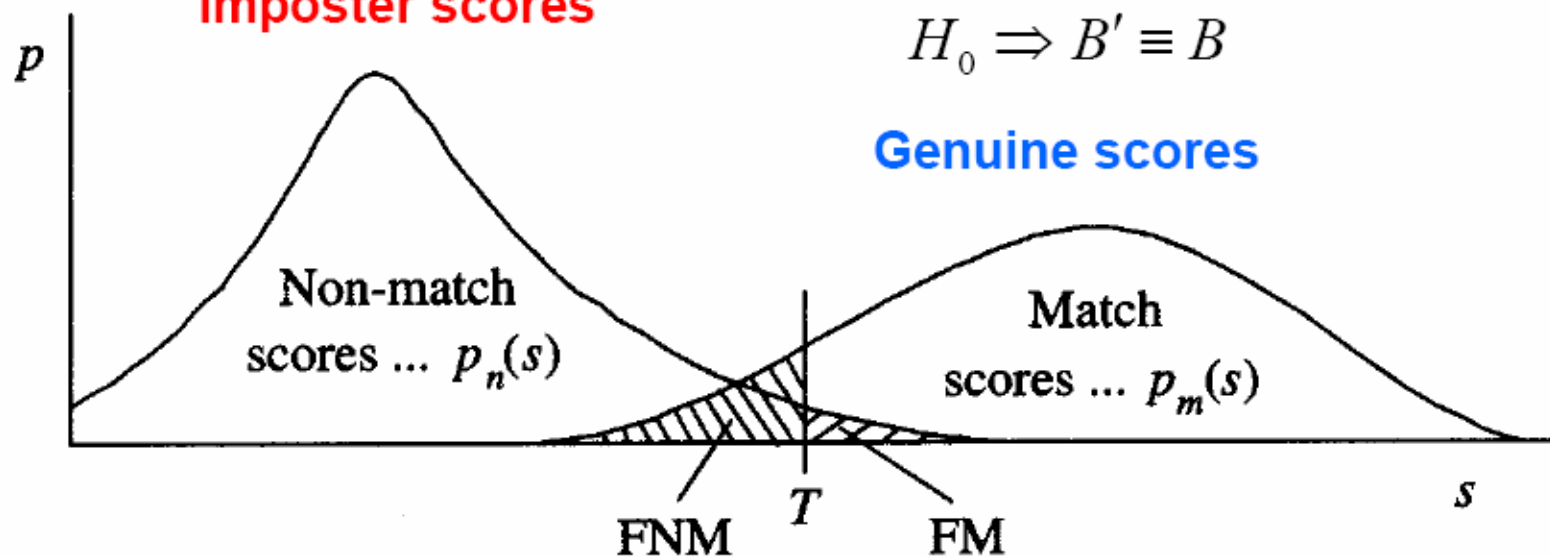
# Two kinds of error

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

Imposter scores

$$H_0 \Rightarrow B' \equiv B$$

Genuine scores



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

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

# Errors & Accuracy

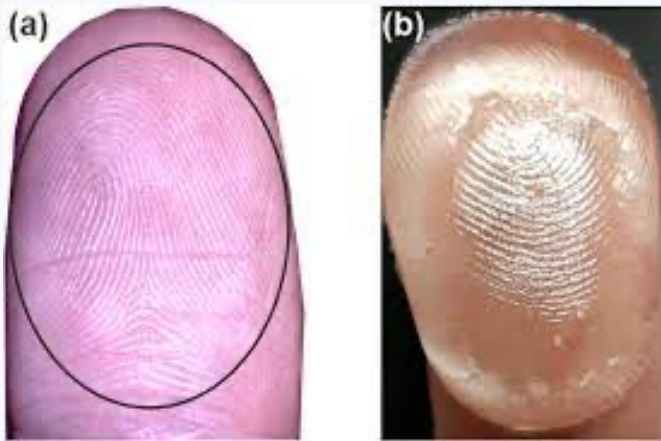


- There are about 30 minutiae: the U.S. Federal Bureau of Investigation (FBI) has evidenced that no two individuals can have more than **eight minutiae** in common
- NIST found that 0.2% of searches in a database of 26.6 photos failed to match the correct image, compared with a 4% failure rate in 2014.
- 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.**





# Liveness in biometrics



gelatin fingerprints, fake irises, and special glasses



# Privacy - camera towers



# Privacy – Hong Kong



laboratory  
stner



# 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.

### 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.



### 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.

### 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



laboratory  
rstner



# Privacy – Cloaking



**SAND Lab**  
security, algorithms, networks and data



laboratory  
**Gerstner**