Technical University of Lodz
Institute of Electronics

Biometrics

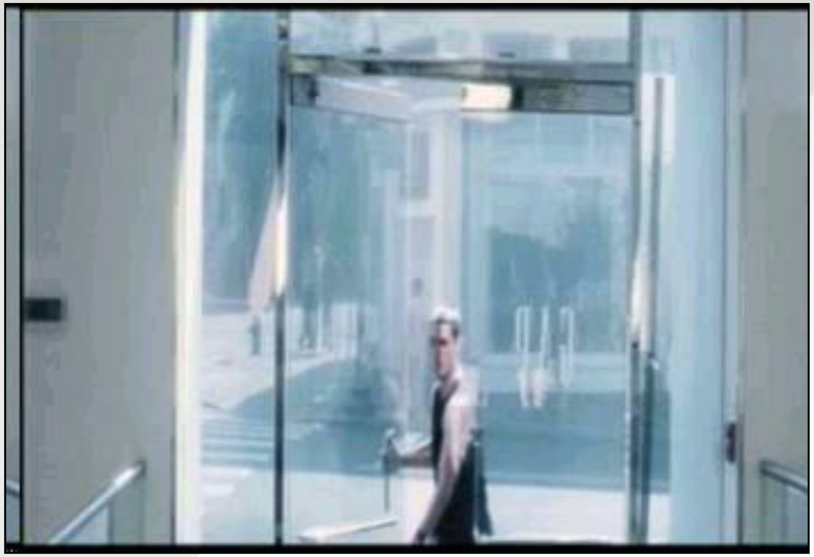
Krzysztof Ślot, Michal Strzelecki

Institute of Electronics,
Technical University of Lodz, Poland

ECCA Conference, May 2013, University of Porto, Portugal

Identification of people by measuring some aspect of individual anatomy or physiology, or other behavioral characteristic, or something that is a combination of the two

www.primode.com/glossary.html



Unattended retinal scans, *Minority Report*

Presentation outline

- Basics
- A review of the state-of-art
- Applications and recent advances

Introduction

Strategies of identity assessment

- A possession - **something that we have** (keys, badges, tokens, smart cards, ...)
- Knowledge - **something that we know** (secret information, like passwords, PIN numbers, ...)
- An individual property of a person - **something we are** - biometrics

Personal identity resolution tasks

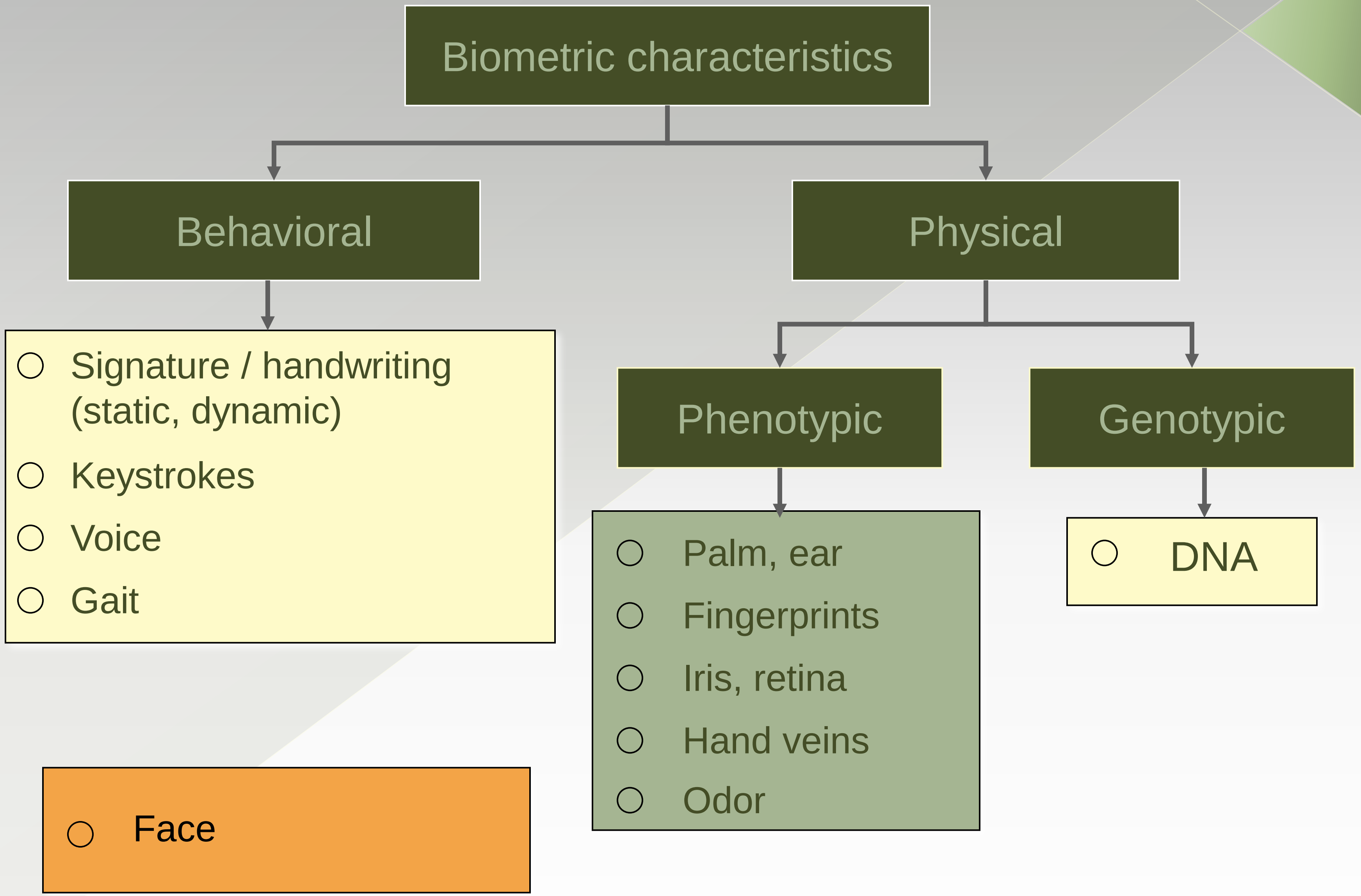
- **Verification (authentication)** - confirmation or denial of the claimed identity (Am I who I claim I am?)
- **Recognition (identification)** - establishing of subject’s identity (Who am I?)

Personal characteristics for biometrics

Basic requirements

- **Uniqueness** - a property must be distinct for different individuals (not a blood group etc.)
- **Permanence** - a property cannot change over time
- **Universality** - everyone (almost) must possess such a property
- **Collectability** - it has to be possible to measure (easily) a property
- **Immunity to circumvention** - it has to be hard to fool the system
- **Acceptability** - physical contact considerations, privacy considerations, religious issues, ...

Personal characteristics for biometrics



Biometric characteristics

Behavioral

- ○ Signature / handwriting (static, dynamic)
- ○ Keystrokes
- ○ Voice
- ○ Gait

Physical

Phenotypic

- ○ Palm, ear
- ○ Fingerprints
- ○ Iris, retina
- ○ Hand veins
- ○ Odor

Genotypic

- ○ DNA

- ○ Face

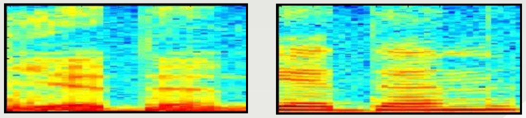
Why biometrics is difficult?

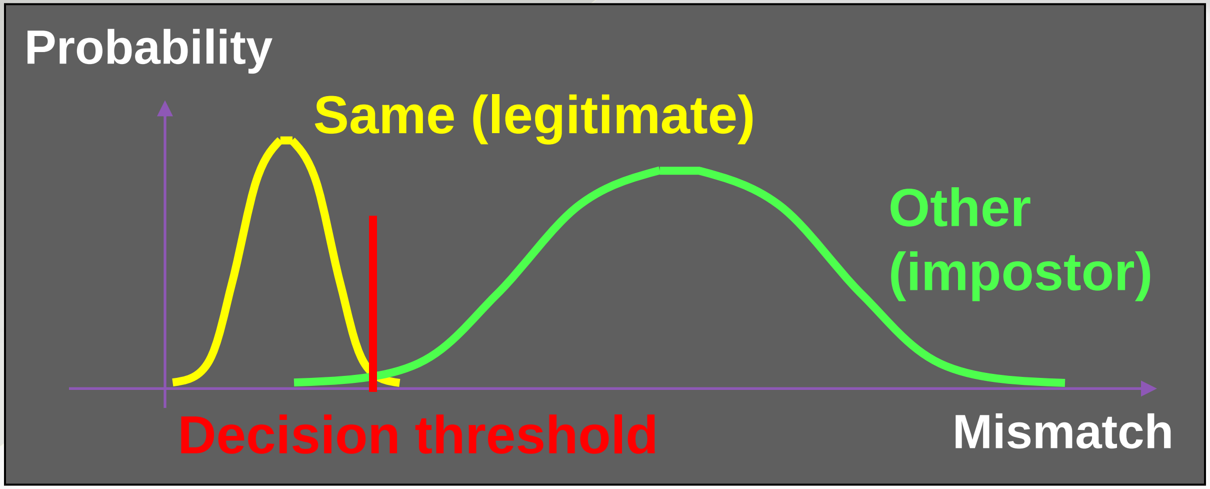
Expectations – fast and reliable recognition

- Samples are never exactly the same

Same face

Same speaker

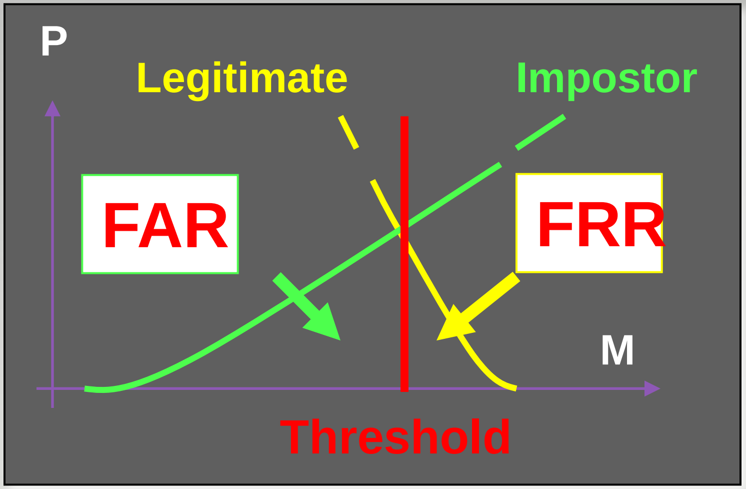


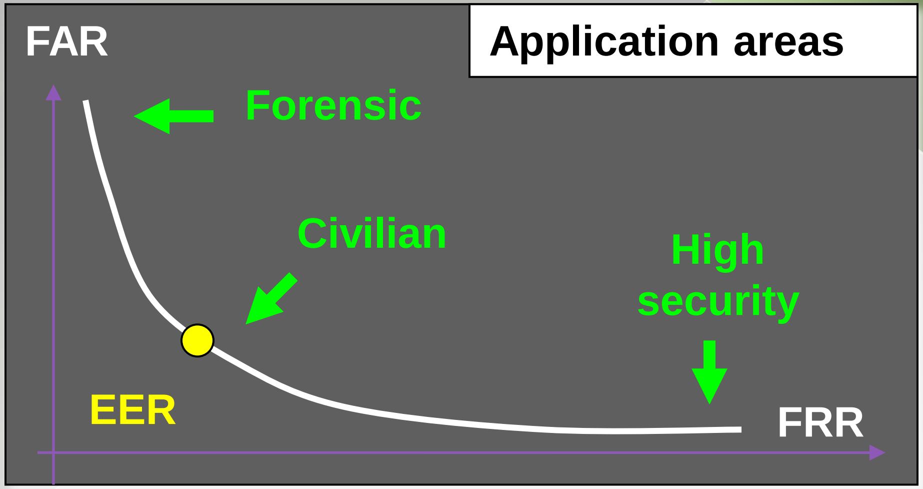


Quantitative performance measures

- FAR - False Acceptance Rate – impostor acceptance
- FRR - False Rejection Rate – legitimate user rejection

Performance measures



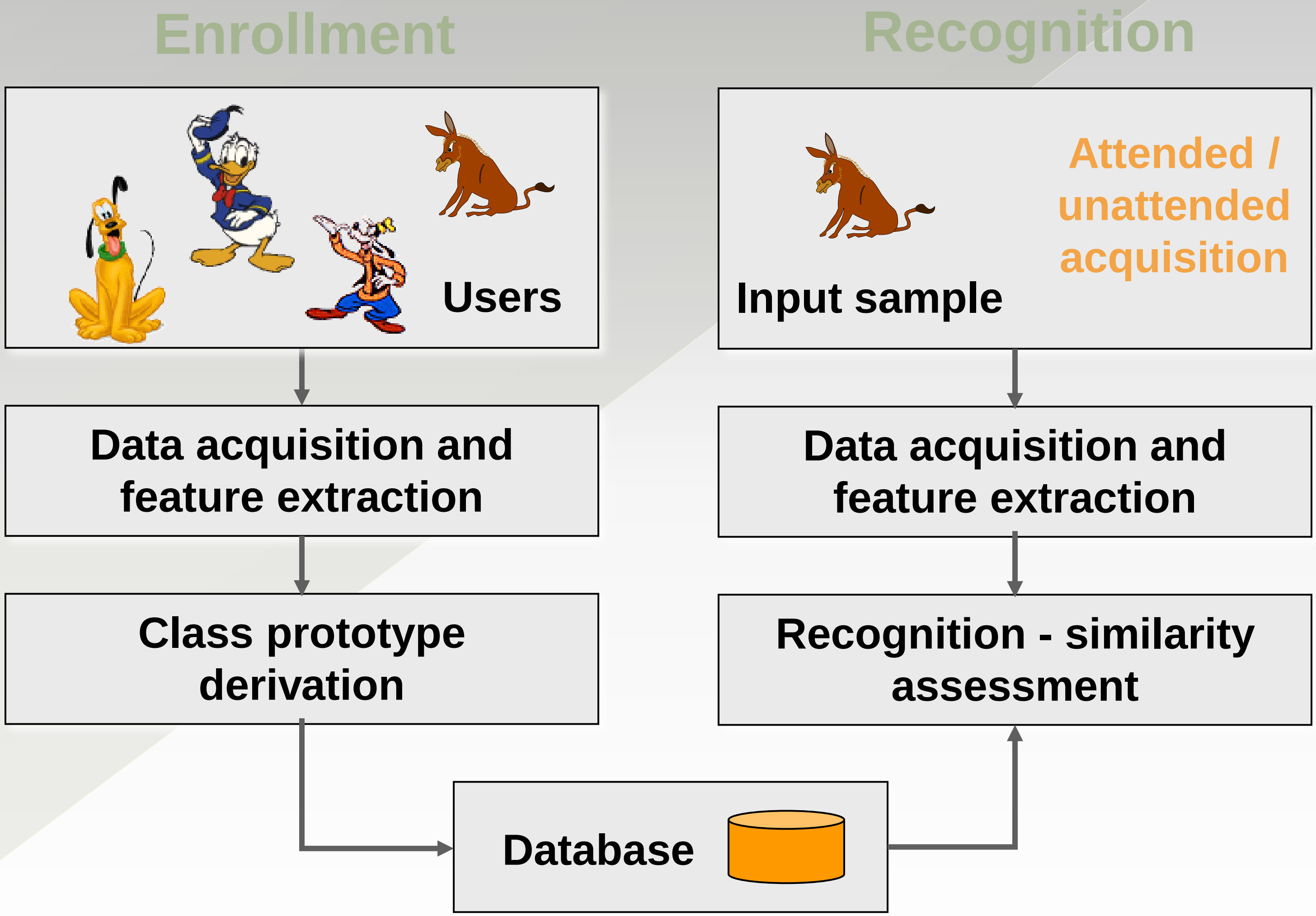


Biometric system design considerations

- Security requirements – **liveness test**
- Objective - verification or identification
- Operation mode - attended or unattended, covert or overt
- Resources - storage requirements, analysis time

Biometric system operation

Enrollment (training) – Execution (recognition)



Enrollment

Users

Data acquisition and feature extraction

Class prototype derivation

Recognition

Input sample

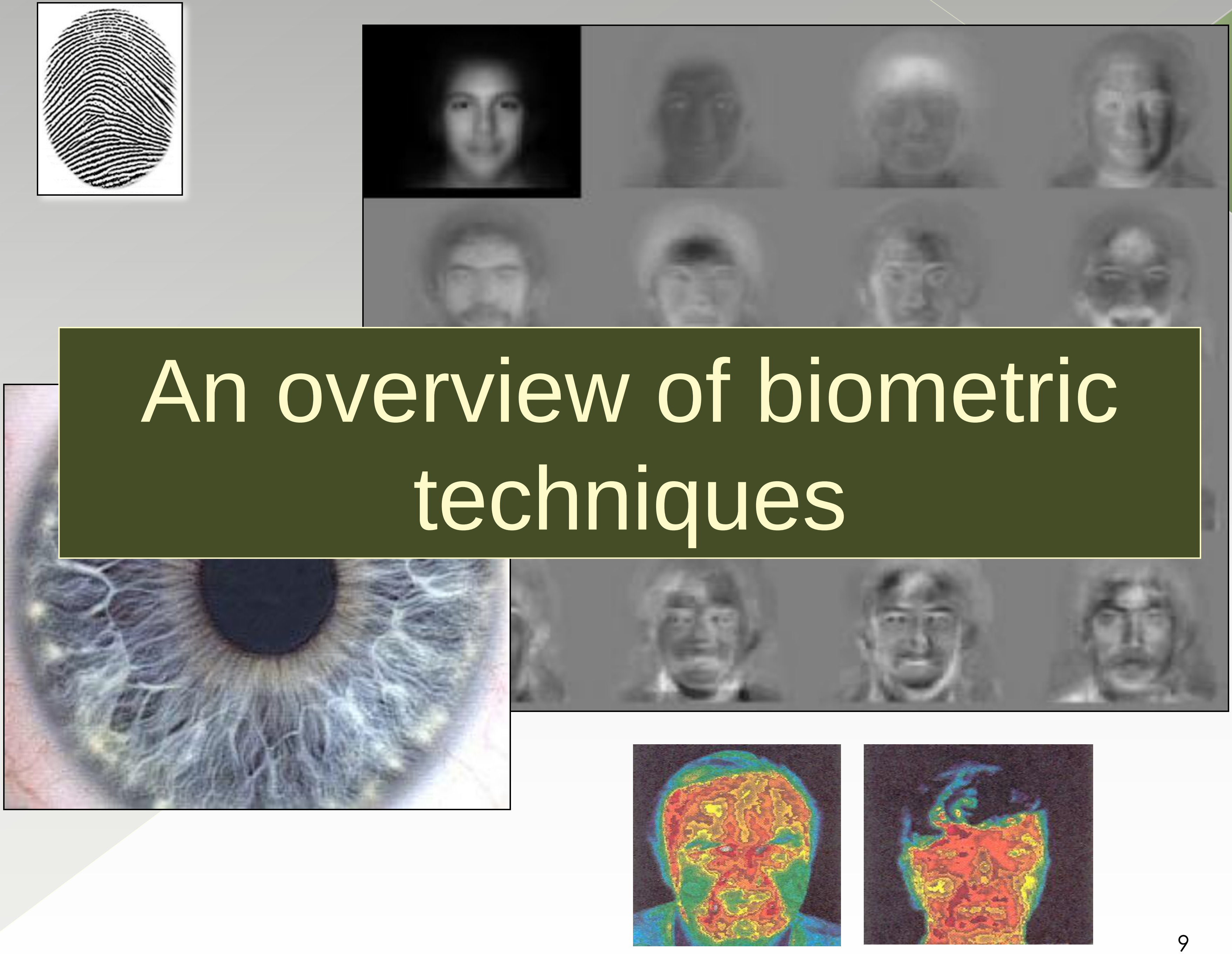
Attended / unattended acquisition

Data acquisition and feature extraction

Recognition - similarity assessment

Database

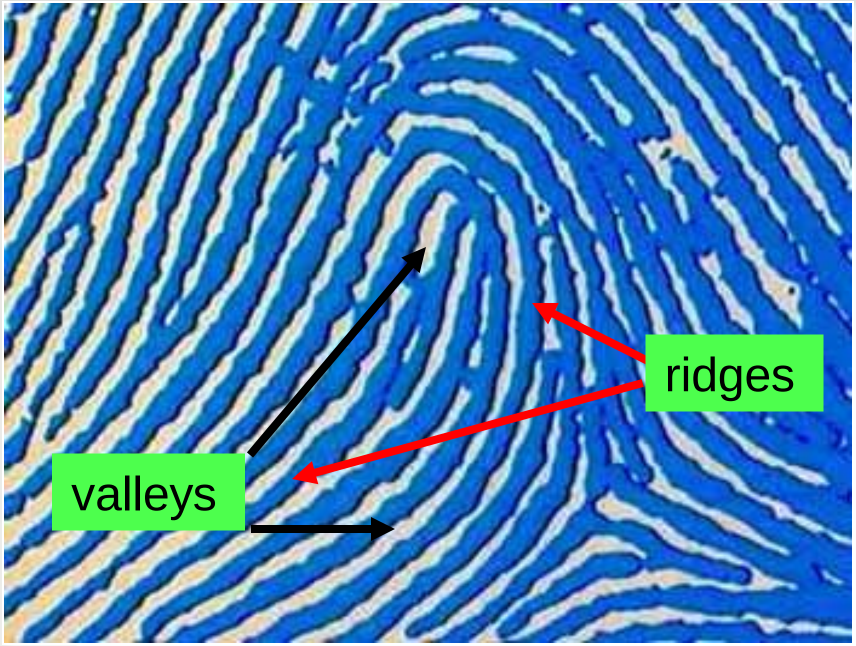
An overview of biometric techniques



Fingerprint-based recognition

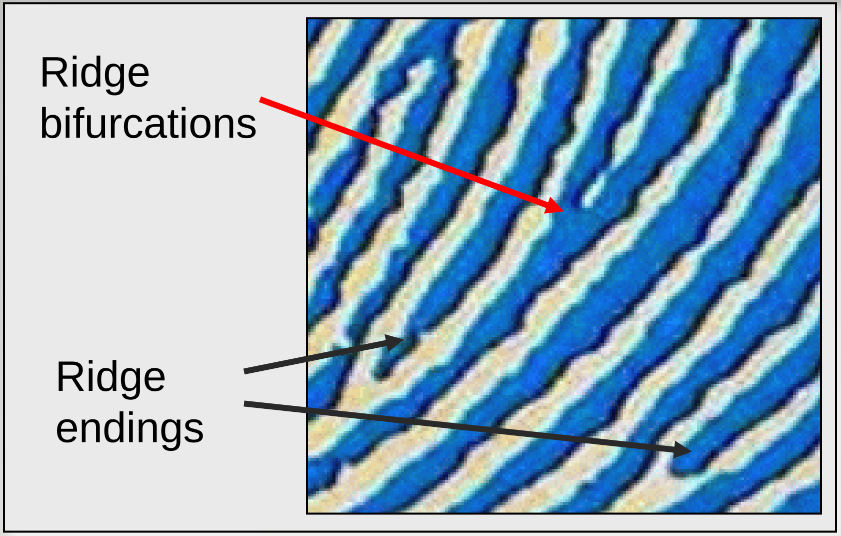
Major current biometric technology

- Earliest records - authentication imprints on clay tables - Babylon, 1700 B.C.
- Approved to be a forensic method in Great Britain in 1901



- No identical fingerprints found among recorded hundreds of millions - **uniqueness**
- Completely forms in early natal period and remains unaltered - **permanence**
- Most of us have it - **universality**
- Easy to **collect** in an **acceptable** way (subject’s cooperation)

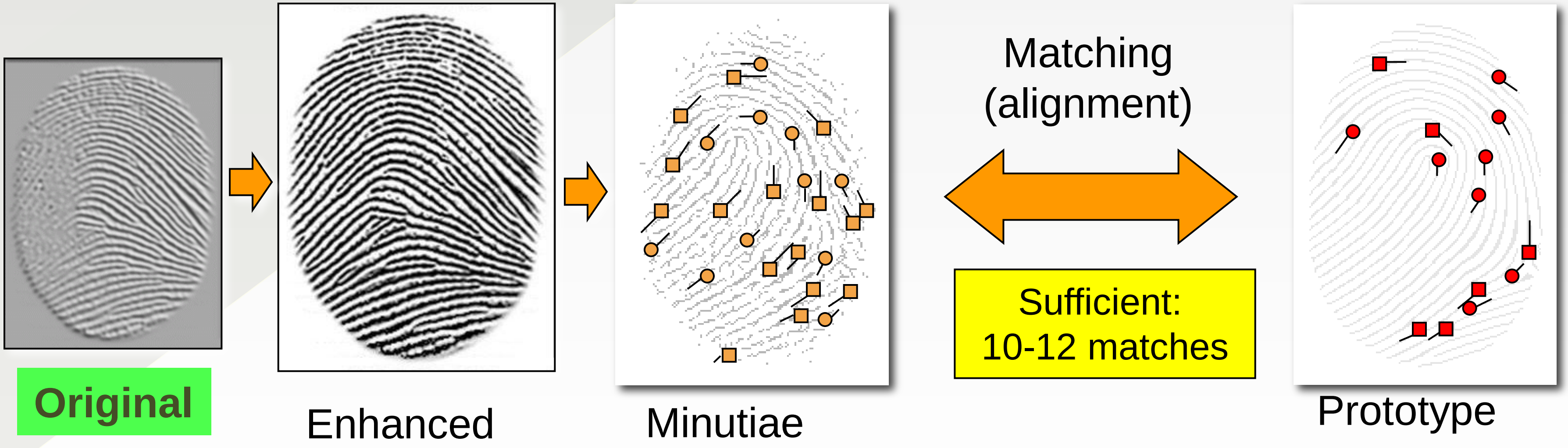
Automated fingerprint recognition



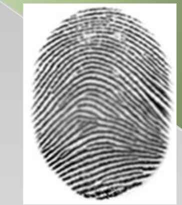
Minutiae-based

- Features: ridge endings and ridge bifurcations
- Typically 40-60 minutiae per fingerprint

Main steps of the minutiae-based recognition

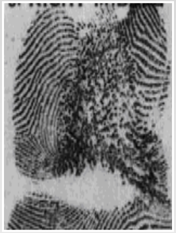


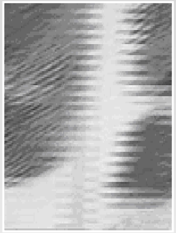
Fingerprint acquisition



Optical readers

- Inexpensive
- Easy to fool (not all types) - photos etc.
- Image quality can become low due to dirt (reader or finger), residual imprints etc.
- Low-cost, low-security systems – PC access





Ultrasound readers

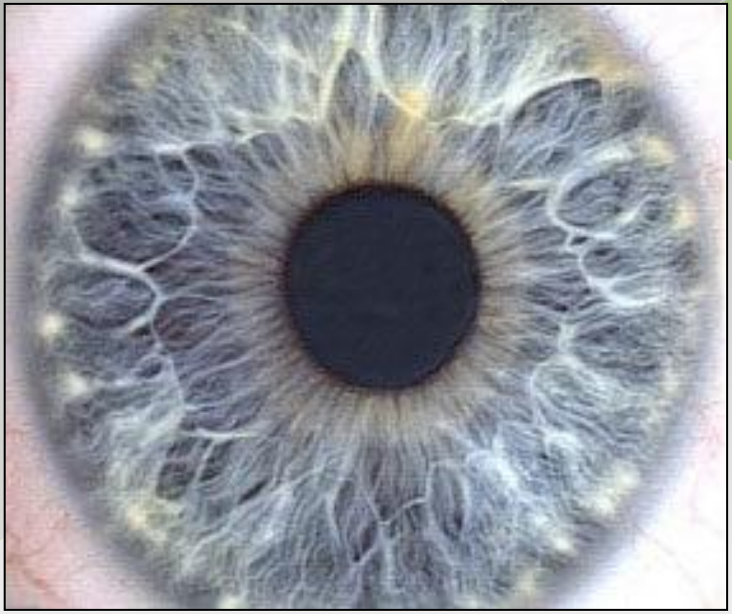
- Inner layers of skin are subject to scanning
- Very expensive
- Considered to be the most difficult (impossible) to circumvent

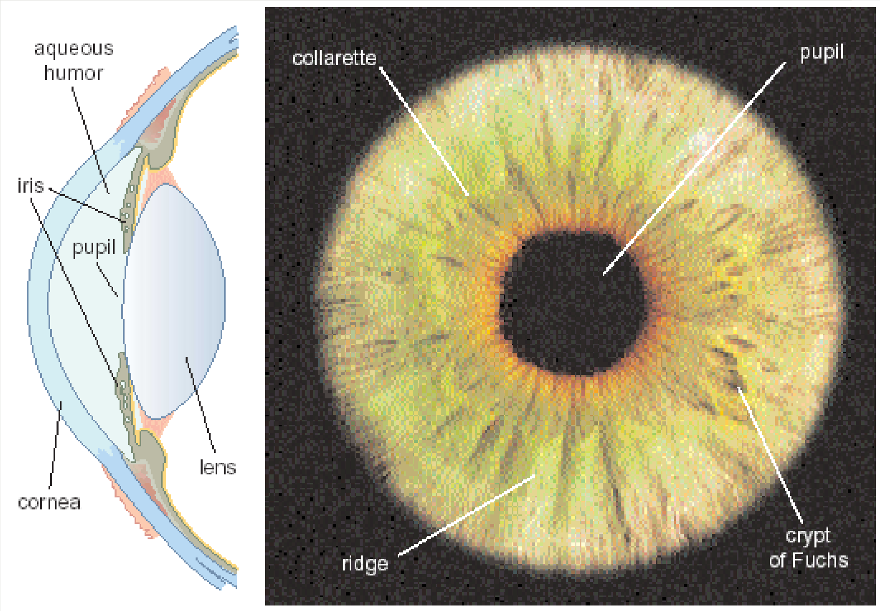
Thermal readers, capacitive readers

Iris-based recognition

Major prospective technology

- No identical irises found among recorded hundreds of millions - **uniqueness**
- Completely forms in early natal period - **permanence**

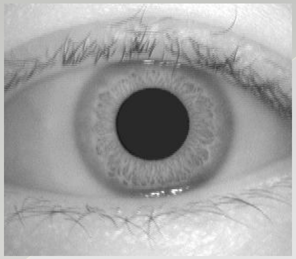




- Most of us have it - **universality**
- Easy to get - **collectabilty**
- No physical contact nor cooperation required - **acceptability**
- Hard to circumvent

Iris image analysis - J. Daugman's algorithm (preprocessing, localization, segmentation, code extraction, classification)

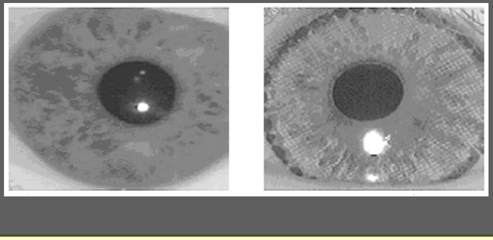
Visible light



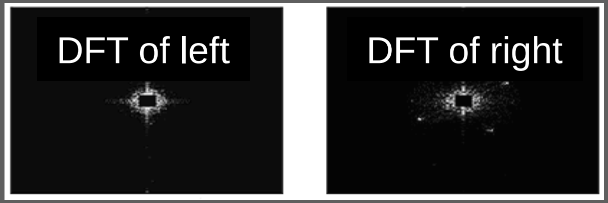
Near infrared

- Perfect (no false matches reported) if sufficient image quality
- Extremely difficult to circumvent

Original



With contact lenses

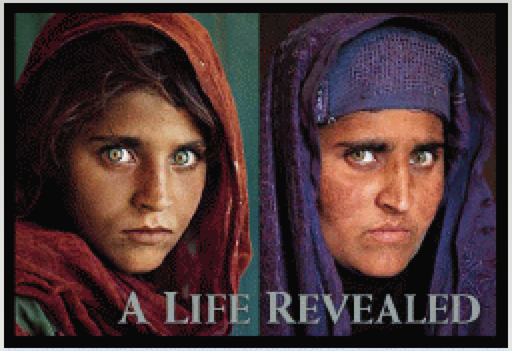


Simple liveness test – variable illumination

Face-based recognition

The most acceptable

- Surveillance and monitoring systems
- Permanence ☹: aging, diseases



Sharbat Gula in 1985, 1992

- Uniqueness ☹: twins, beard, facial expressions, make-up ...

Other challenges

- Face localization (detection)
- Acquisition errors - illumination, background

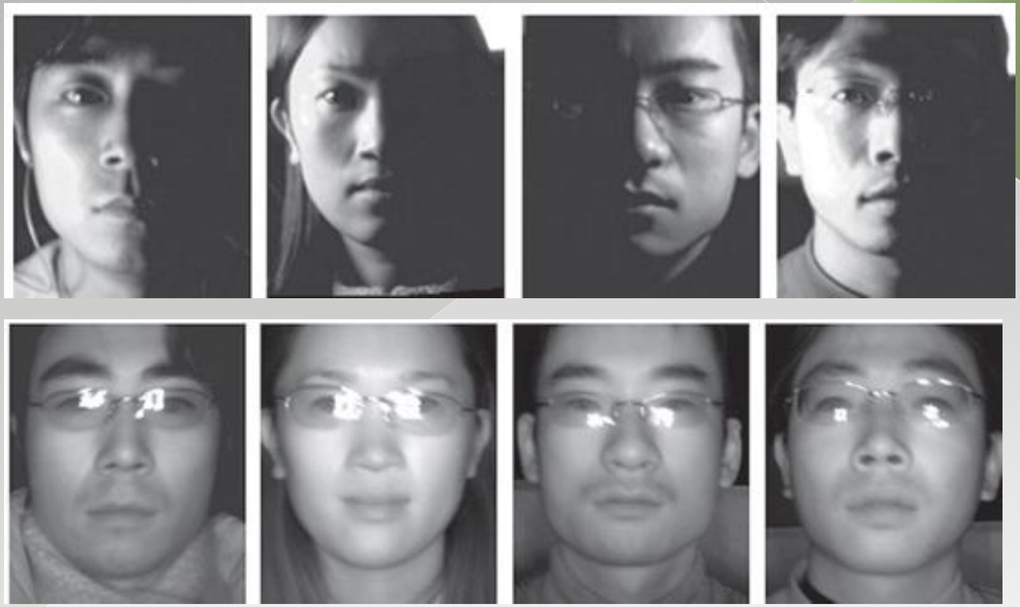
Huge security market

- Massive deployments in airports

Performance in access-control systems

Poor (10% EER if uncontrolled acquisition, otherwise – 1%)

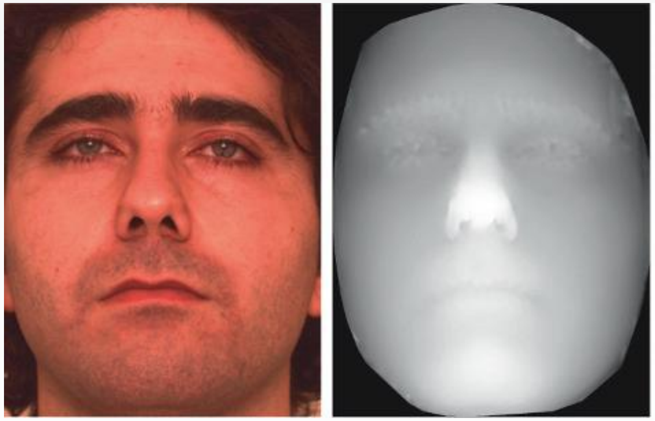
Recent advances in face-based recognition



Near infrared face recognition

- Minimizing lighting from other sources
- No color variation

3D Face Recognition



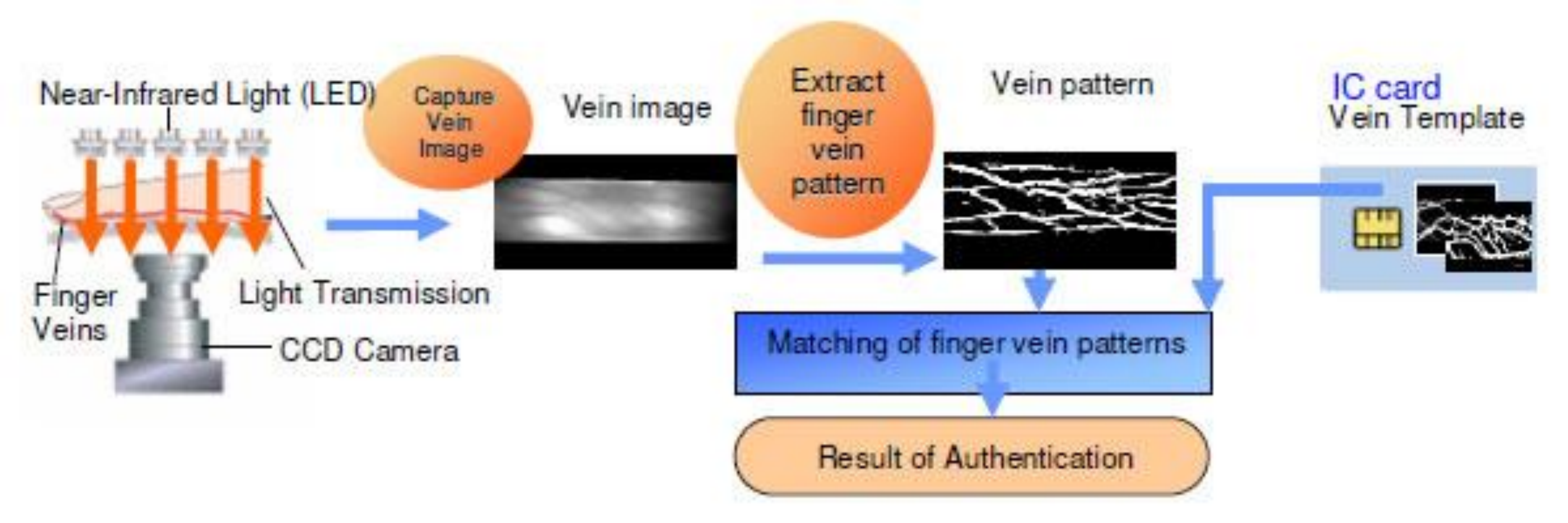
- Stereovision or laser active sensing to obtain depth information
- Access to shape and texture information
- Recognition algorithms less sensitive to variable or poor illumination and pose change -> better performance

Finger vein recognition

- Unique shape and distribution of human vessel tree
- Pattern-recognition techniques for images of human finger vein patterns beneath the skin's surface
- Easy and non-invasive image acquisition based on near-infrared radiation
- High acceptance

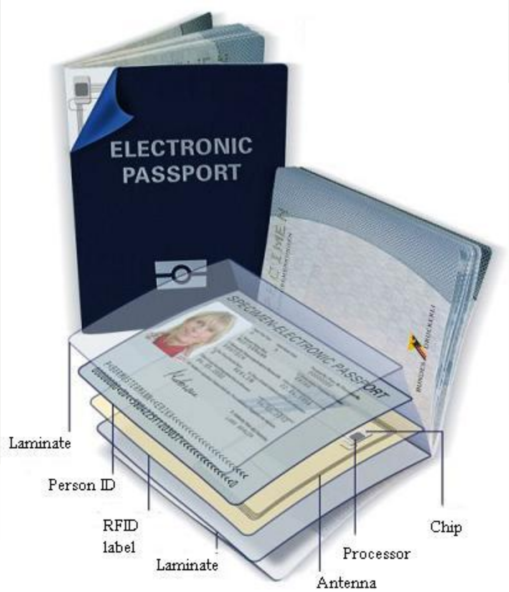
Finger vein recognition

- Developed by Hitachi, 2005
- Analysis time < 2s
- FAR < 0,0001%, FRR < 0.01%
- Applications: ATM, employee time and attendance tracking, computer and network authentication



Biometrics and smart cards

- Biometric data included in card microchips
- Finger print, face and iris templates
  (or their combination – multimodal biometrics)
- Biometric processing: match-off-card vs. match-on-card
- Threats: template decoding by reverse engineering
- Countermeasure: advanced data coding algorithms (fuzzy extractors)

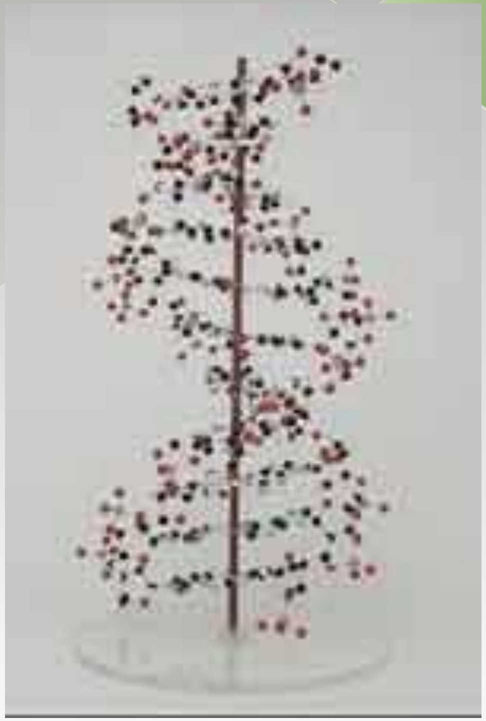


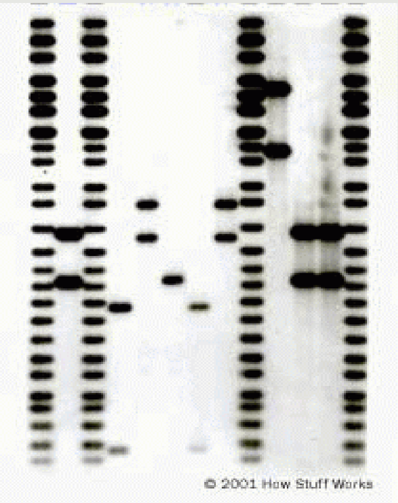
Microchips are also implemented
in biometric passports

DNA-based recognition

Highlights

- Approximately 3 million DNA base pairs (0.1% of a genome) vary from person to person (except twins)
- DNA evidence analyzes identical particle sequences in non-coding DNA - Variable Number Tandem Repeats - VNTR
- DNA individual profile: a number of VNTRs





Major drawbacks

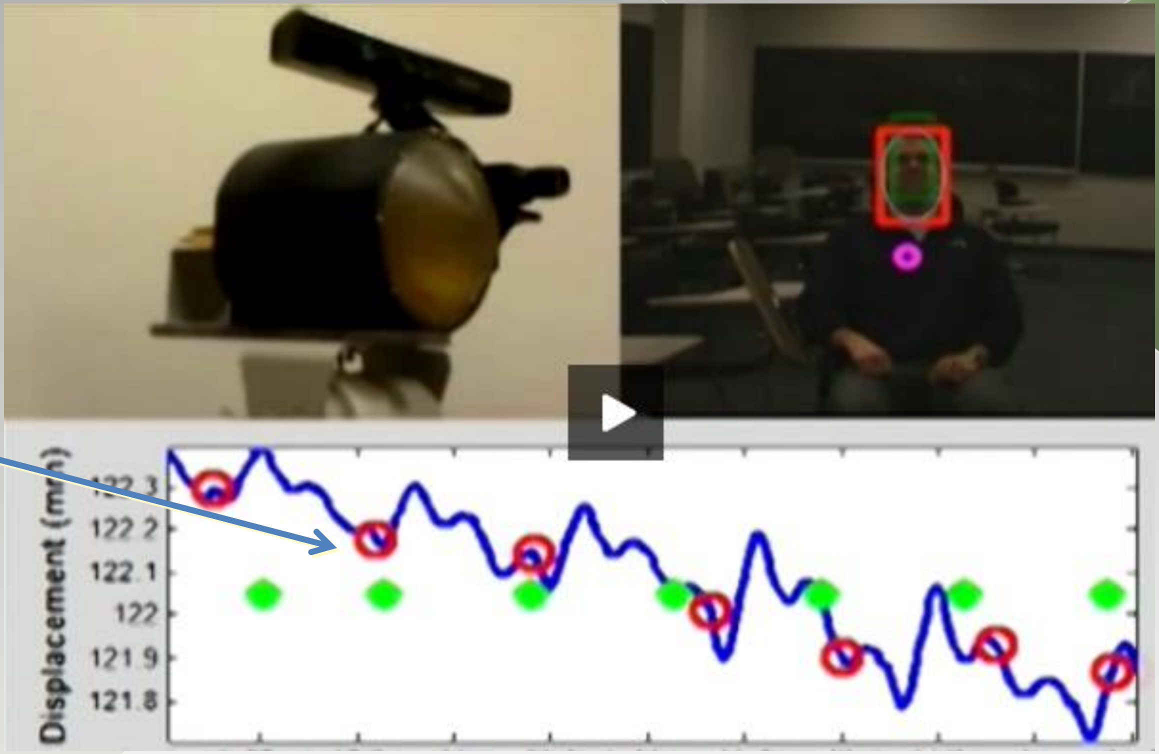
- Low acceptability - a rich pool of additional information unrelated to identity determination
- Samples are easy to steal and plant
- Time consuming procedure, high costs

New DNA analysis system by NetBio, USA (2013)

- Analysis of repeated DNA sequences of the human genome (short tandem repeats, STR)
- Odds of two unrelated people having the same STR profile are 1 in 575 trillion
- STR profile generated based on 16 STR regions (this type of DNA data is widely accepted in the criminal justice systems in Japan, the United States, and Western Europe)
- Cotton swabs (RFID tagged) to collect cheek cells from inside a person’s mouth
- Analysis time < 90 min, easy to use

Biometrics future

- Biomedical signals as biometrics (e.g. ECG)

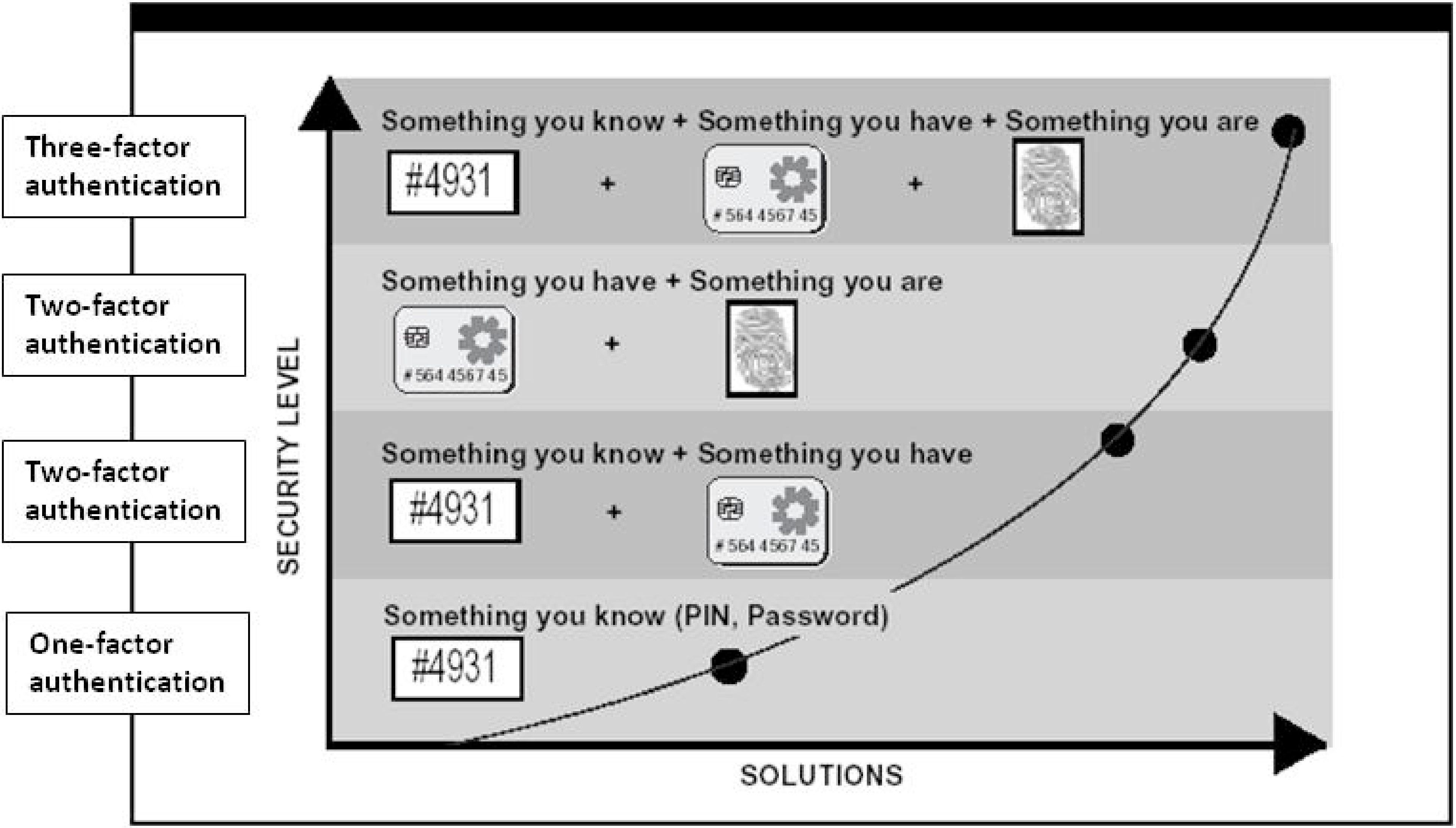


Argonne Nat. Lab., USA

- Remote biometrics (mobile device performs template matching)

3M Cogent, USA

Biometrics + SC improve security

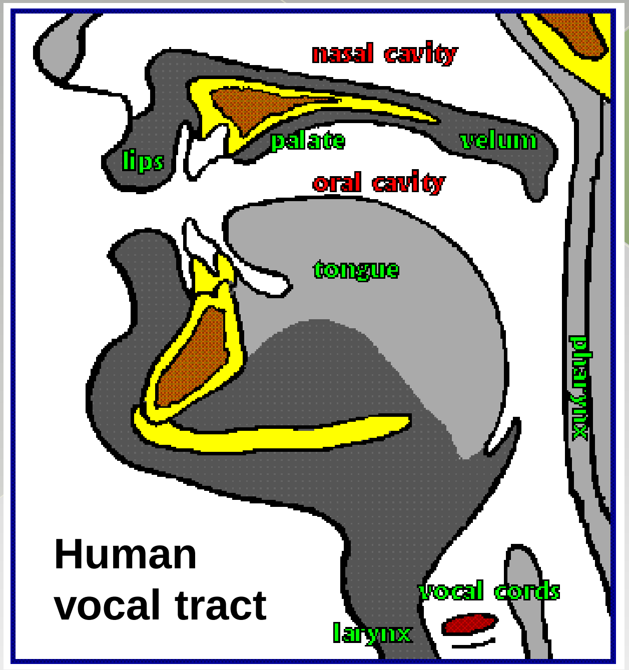

Three-factor authentication
Two-factor authentication
Two-factor authentication
One-factor authentication
SECURITY LEVEL
Something you know + Something you have + Something you are
#4931
+
# 564 4567 45
+
Something you have + Something you are
# 564 4567 45
+
Something you know + Something you have
#4931
+
# 564 4567 45
Something you know (PIN, Password)
#4931
SOLUTIONS

Thank you for your attention

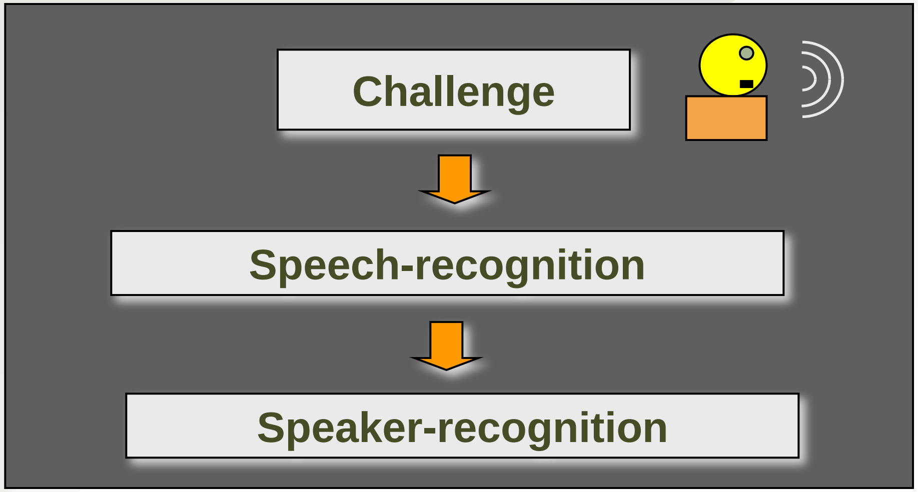
Voice-based recognition

Highlights

- Most of us have it - **universality**
- Easy to acquire (no cooperation)
- Gets changed (aging, health…) ☹
- Uniqueness hard to be proved ☹



- Combination of individual physical properties and learned elements



Challenge

Speech-recognition

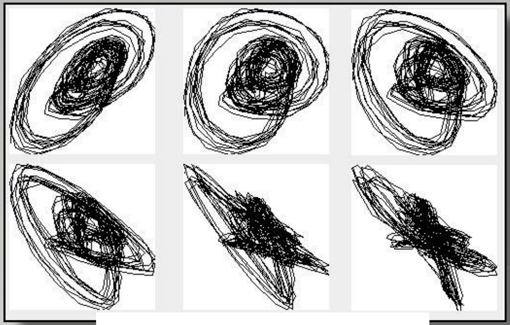
Speaker-recognition

The only means for remote applications

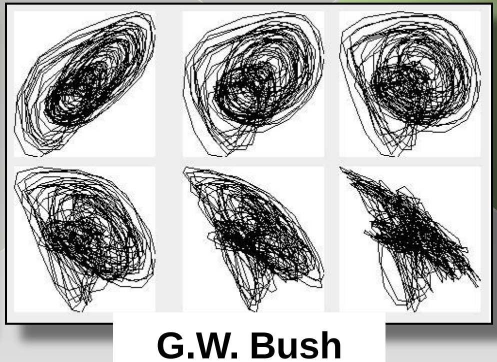
Successive increase in recognition confidence level

(nr)

Voice-based recognition



Impersonator



G.W. Bush

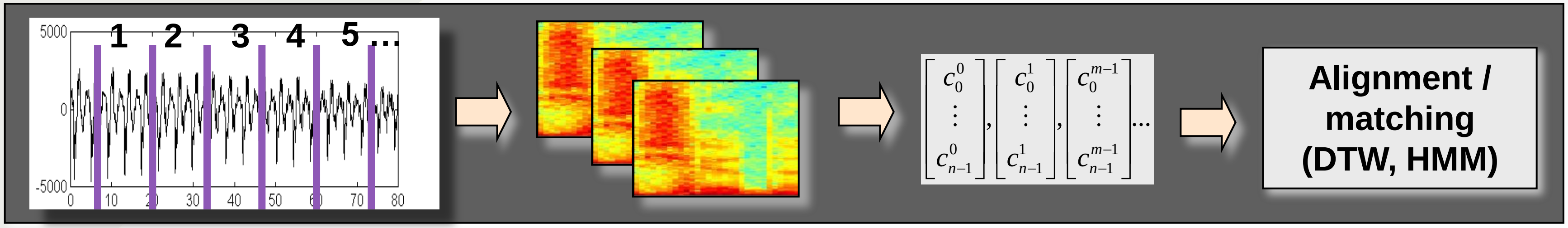
Other challenges

- Deliberate imitation
- Noise

Features

- Adopted from speech recognition (LPC, Mel …)
- Specific (e.g. pronunciation variability)

Recognition procedure



$$\begin{bmatrix} c_0^0 \\ \vdots \\ c_{n-1}^0 \end{bmatrix}, \begin{bmatrix} c_0^1 \\ \vdots \\ c_{n-1}^1 \end{bmatrix}, \begin{bmatrix} c_0^{m-1} \\ \vdots \\ c_{n-1}^{m-1} \end{bmatrix} \ldots$$

Alignment / matching (DTW, HMM)

- Poor recognition rates 1:50, 1:100

(nr)

Basics