Computer security Lecture 3

Identification and Authentication Biometrics

Ingo Hölscher

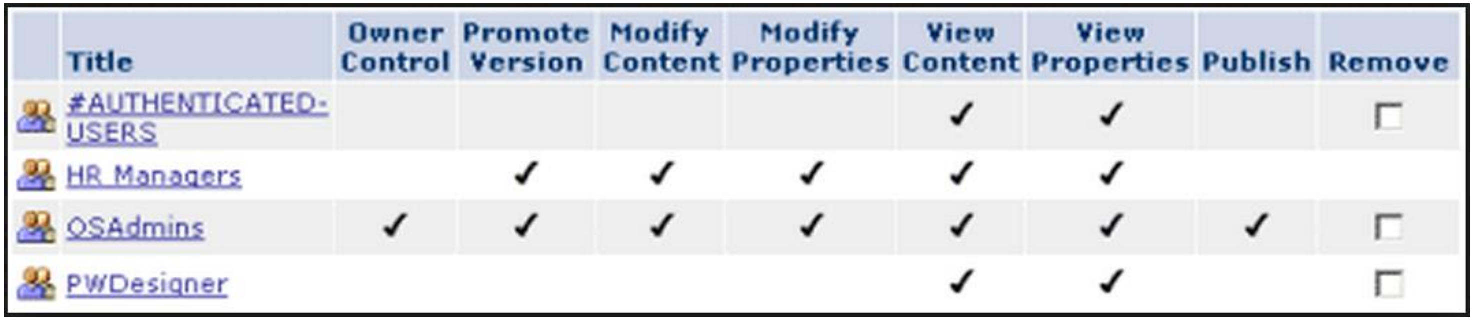
LINKÖPING UNIVERSITY

You will hear about:

- ACL – access control list
- Authentication vs authorization
- Biometrics
  Basics / Characteristics
  Difficulties with biometrics
  Biometric techniques
  Attacks on biometrics
  Future – Present in biometrics

Access Control List (ACL)

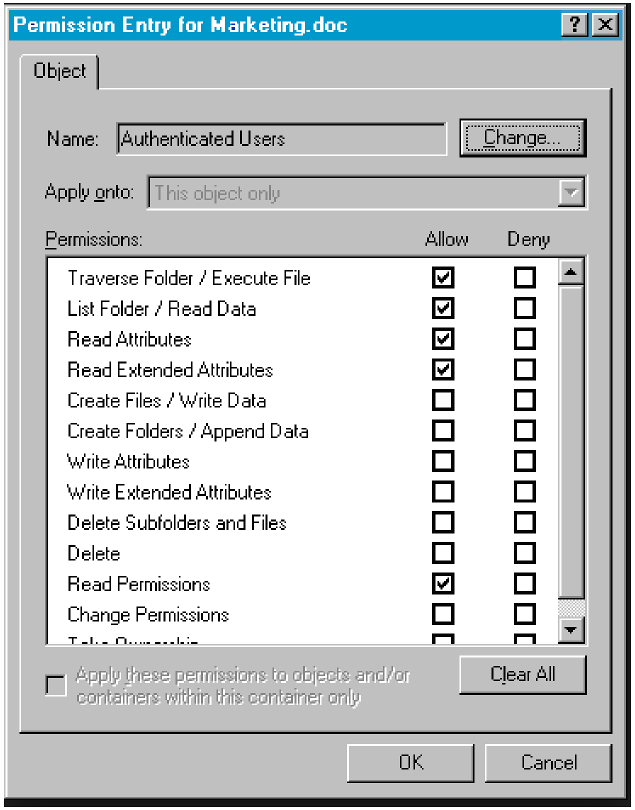
- A table (list) that defines which access rights a user (group) has to a particular object
- Example: John Doe, read



Title	Owner Control	Promote Version	Modify Content	Modify Properties	View Content	View Properties	Publish	Remove
#AUTHENTICATED-USERS					✓	✓		□
HR Managers		✓	✓	✓	✓	✓		
OSAdmins	✓	✓	✓	✓	✓	✓	✓	□
PWDesigner					✓	✓		□

Access Control List (ACL)

- ➢ Good control to check if user is authorized to a resource
- ➢ Difficult to manage



Permission Entry for Marketing.doc

Object

Name: Authenticated Users

Apply onto: This object only

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	☑	□
Change Permissions	□	□
Take Ownership	□	□

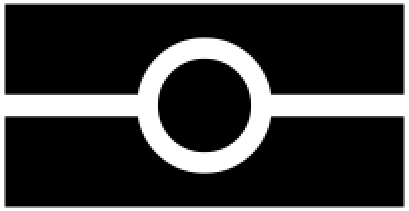
□ Apply these permissions to objects and/or containers within this container only

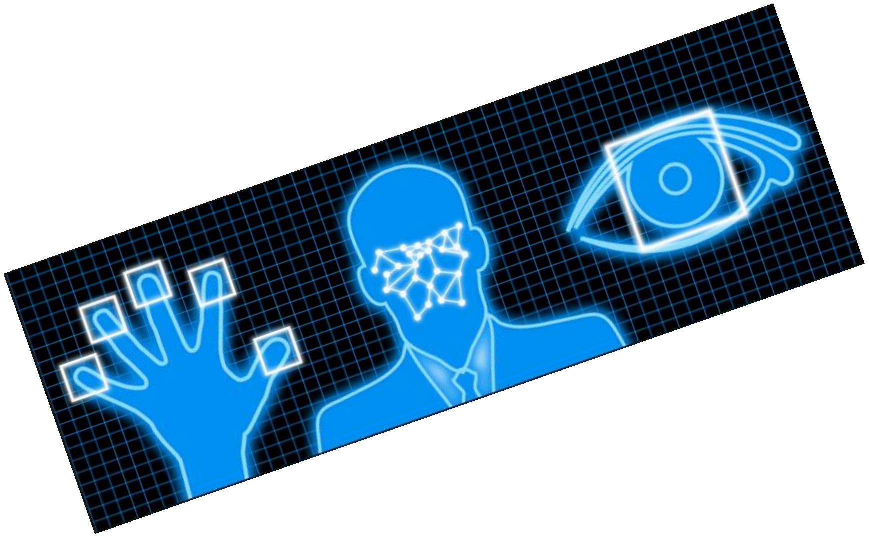
Authentication vs. Authorization

- Authentication
  Verifying the **identity** of a user
- Authorization
  controlling **what** resources a user has access to after authentication
- Authorization is **not** authentication

Authentication modes

- **Something you know** (passwords, PIN, . . .)
- **Something you have** (keys, badges, tokens, smart card, . . .)
- **Something you are** biometrics (handwriting, fingerprints, retina patterns, . . .)





Biometrics

The science of using biological properties to identify individuals

www.lexias.com/html/glossary1.html

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

www.primode.com/glossary.html

Characteristics for biometrics

➢ Basic requirements

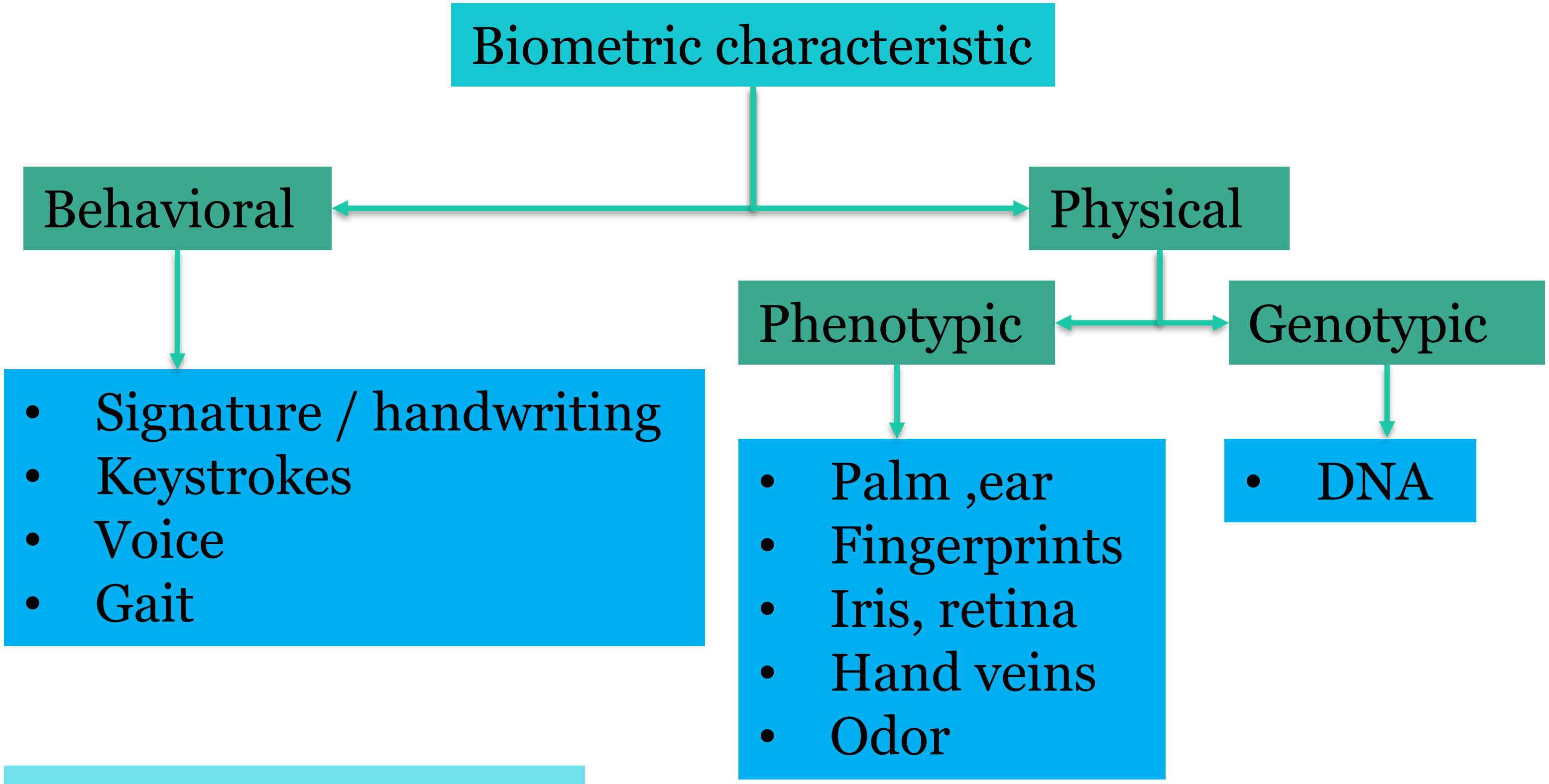
- **Uniqueness** - a property must be distinct for different individuals (not a blood group etc.)
- **Permanence** - a property cannot change over time
- **Universality** - everyone (almost) must possess such a property
- **Collectability** - it has to be possible to measure (easily) a property
- **Immunity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

Characteristics for biometrics

➢ Additional requirements

- **Acceptability** - physical contact considerations, privacy considerations, religious issues, …
- **Efficiency** - of acquisition, recognition, storage

Characteristics for biometrics



Biometric characteristic

Behavioral

- Signature / handwriting
- Keystrokes
- Voice
- Gait

Physical

Phenotypic

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

Genotypic

- DNA

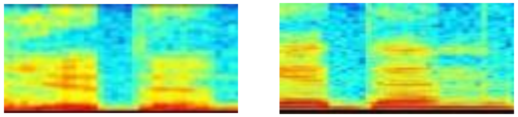
- Face
- Face thermograms

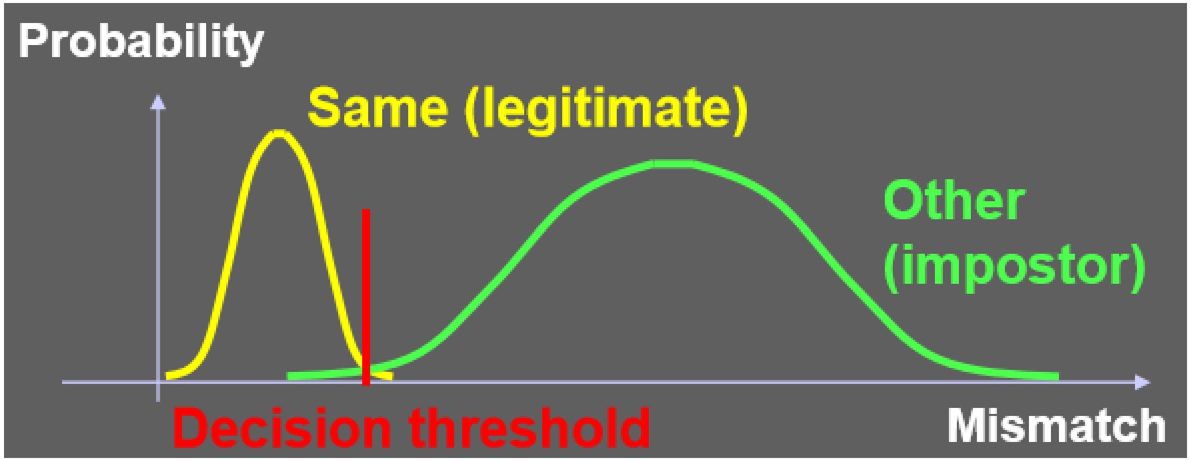
Difficulties with biometrics

- ➢ Expectations – fast and reliable recognition
- ➢ Reality
- Samples are never exactly the same

Same face

Same speaker

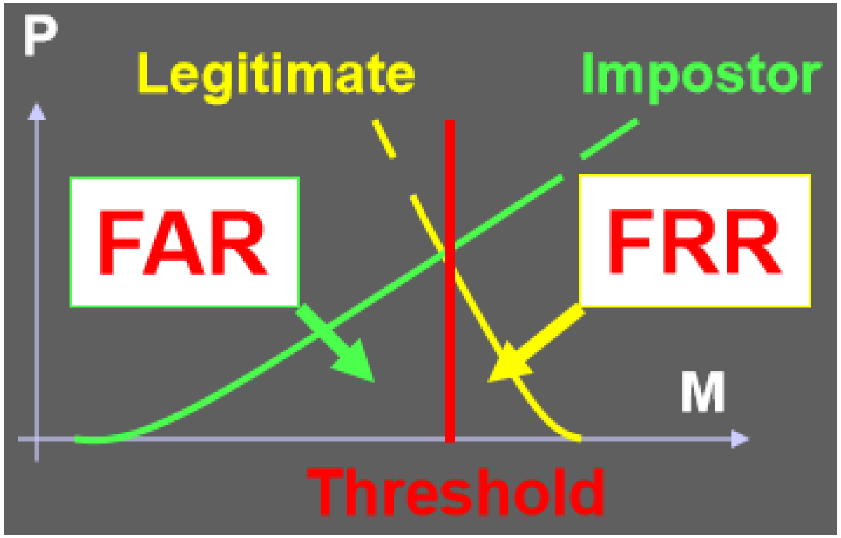




Difficulties with biometrics

False rejection / False acceptance

- Denying access to legitimate users is called false rejection
- Allowing access to illegitimate users is called false acceptance
- The probabilities of these two failures decide the quality of the biometric system



Difficulties with biometrics

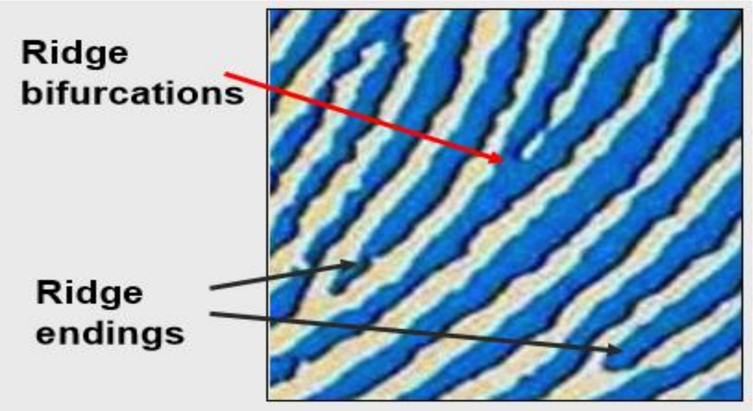
- Enrolment not accepted or to complicated
- People without index fingers
- Injury makes authentication impossible
- Human iris change with age
- . . .

An overview of biometric techniques

Fingerprint based recognition

- ➢ Major current 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)



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

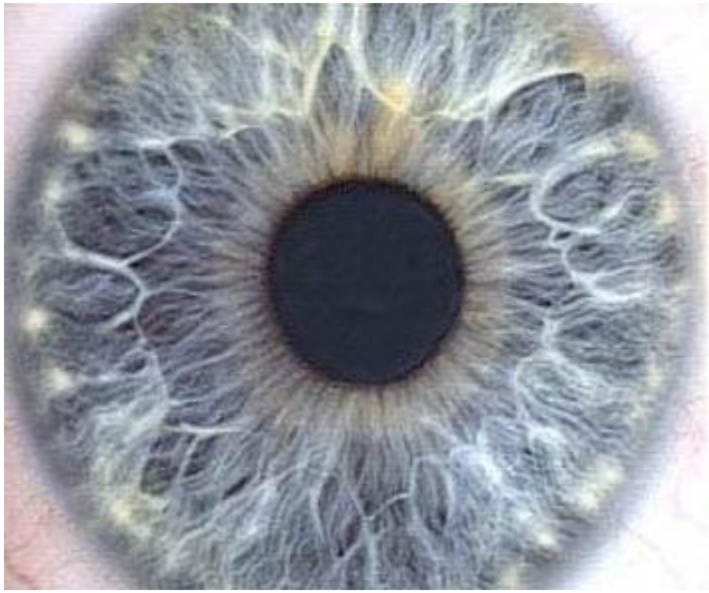
- **Ultrasound readers**
- Inner layers of skin are subject to scanning
- Expensive
- Considered to be the most difficult (impossible) to circumvent Inner layers of skin are subject to scanning

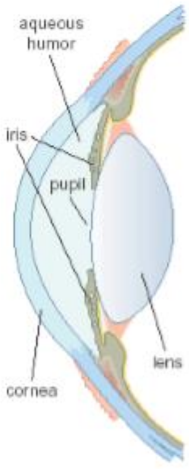
Fingerprint acquisition

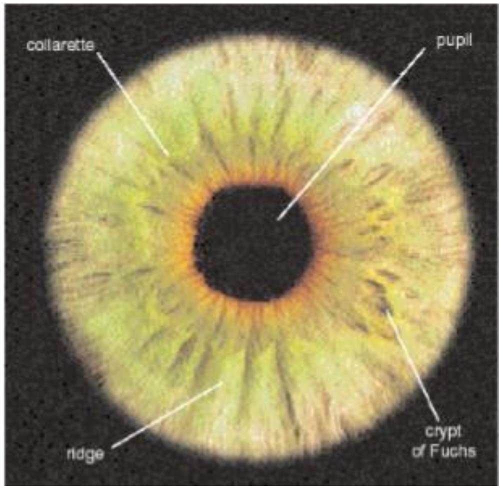
- **Thermal readers**
  - A difference in a temperature of ridges (warmer) and valleys (colder)
  - Rather inexpensive, hard to circumvent
  - Quality depends on ambient temperature (finger temperature)
- **Capacitive readers**
  - Skin surface - a capacitor’s electrode
  - Quality - usually good
  - Rather inexpensive
  - Hard to fool

Iris-based recognition

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





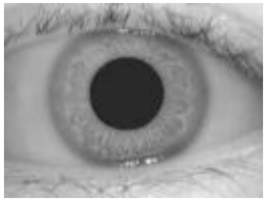


- Most of us have it – universality
- Easy to get – collectability
- No physical contact nor cooperation required - acceptability
- Hard to circumvent

Iris-based recognition

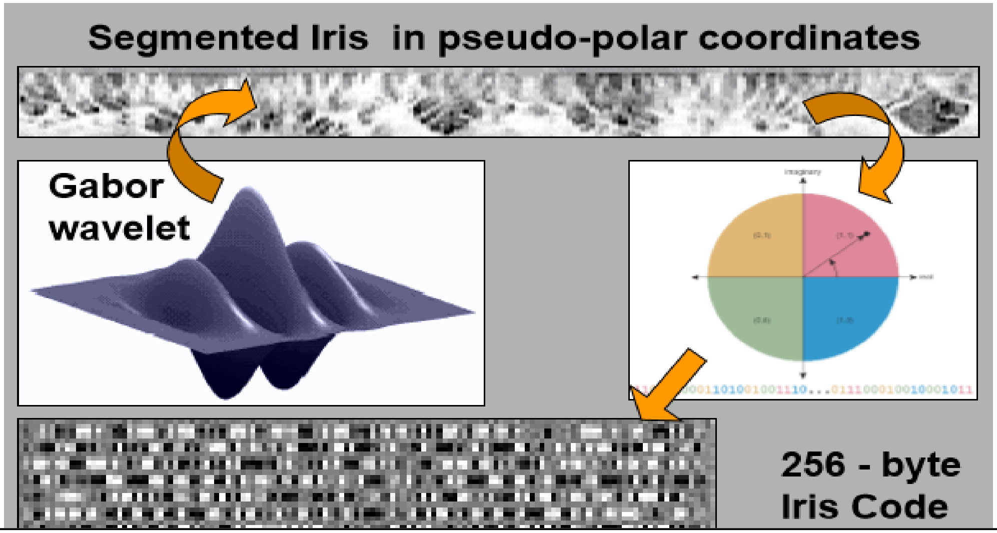
Iris analysis

Visible light



Near infrared

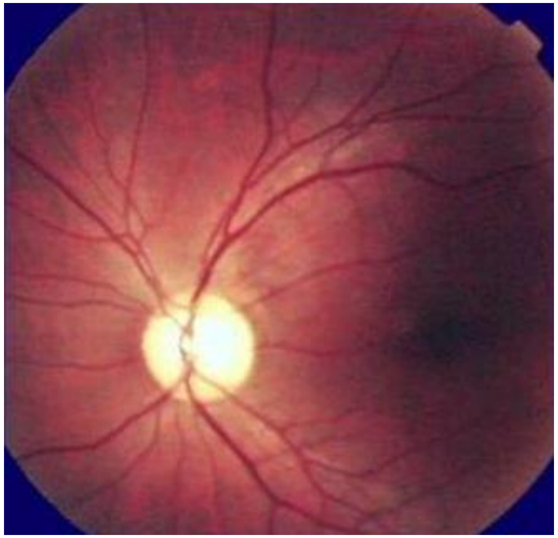
J. Daugman’s algorithm (the IrisCode)



Retina-based recognition

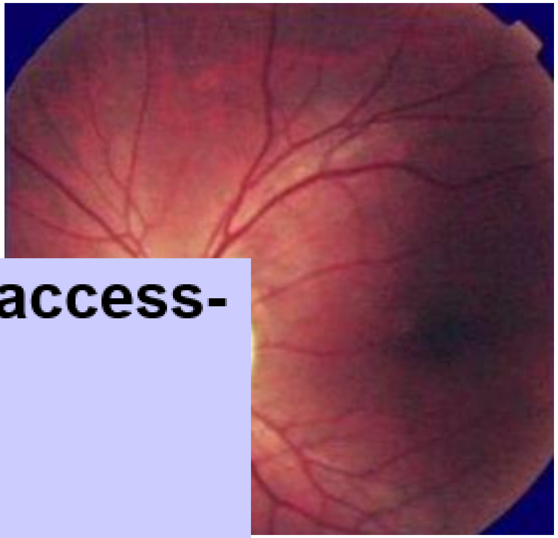
➢ Considered to be the most credible

- No identical retinas found so far - uniqueness
- Completely forms in early childhood (later changes possible) - permanence
- Most of us have it - universality
- Possible to scan – collectability
  … but: physical contact required
  - low acceptability
- Objects of interest: veins



Retina-based recognition

- Considered to be the most credible
- No identical retinas found so far - uniqueness
- Completely for
  (later changes
- Most of us hav
- Possible to sca
  … but: physical
  - low acceptab
- Objects of inte

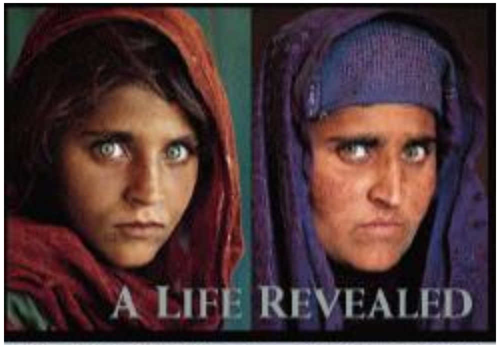


Performance in access-control systems

- Very good
- Natural liveness tests - considered impossible to circumvent
- High-security facilities

Face-based recognition

- **The most acceptable**
- Surveillance and monitoring systems
- Permanence: aging, diseases

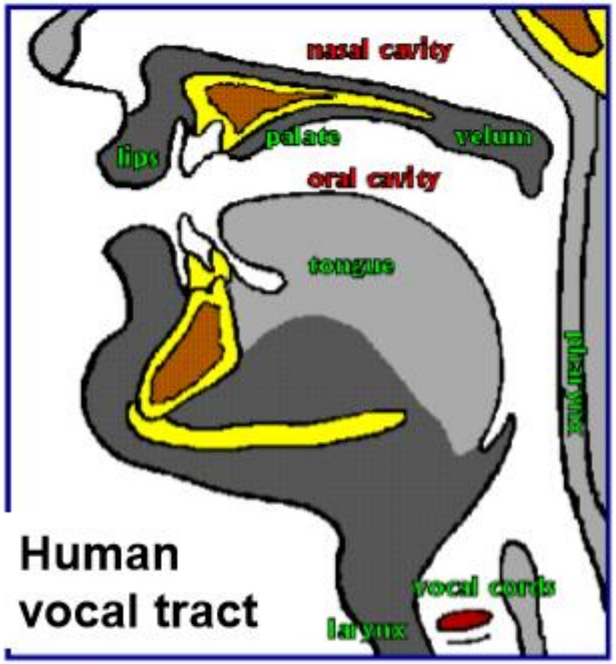


Sharbat Gula in 1985, 1992

- **Other challenges**
- Face localization (detection)
- Acquisition errors – illumination, background
- Uniqueness: twins, beard, facial expressions, make-up …

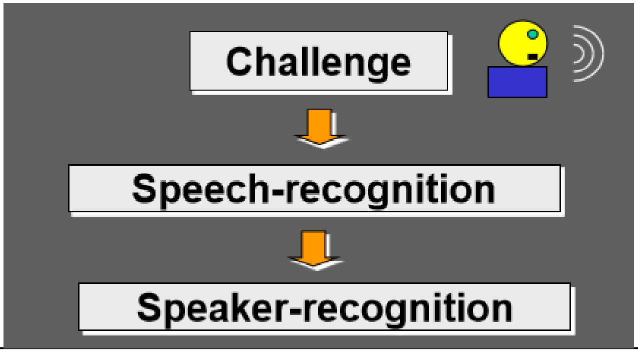
- **Huge security market**
- Massive deployments in airports after 9/11

Voice-based recognition



Human vocal tract

- ➢ **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

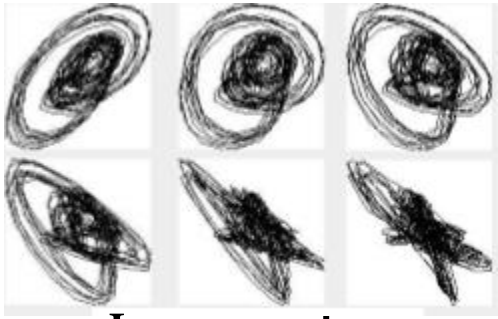
Speaker-recognition

- ➢ The only means for remote applications
- ➢ Successive increase in recognition confidence level

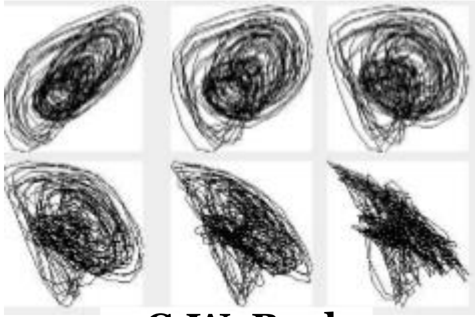
Voice-based recognition

- **Other challenges**
- Deliberate imitation
- Noise
- **Features**
- Adopted from speech recognition (LPC; linear predictive coding)
- Pronunciation
- . . .

https://youtu.be/t4N93jLVPIA



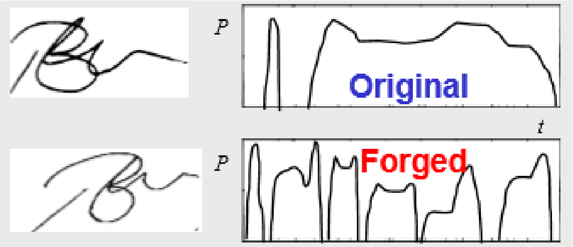
Impersonator



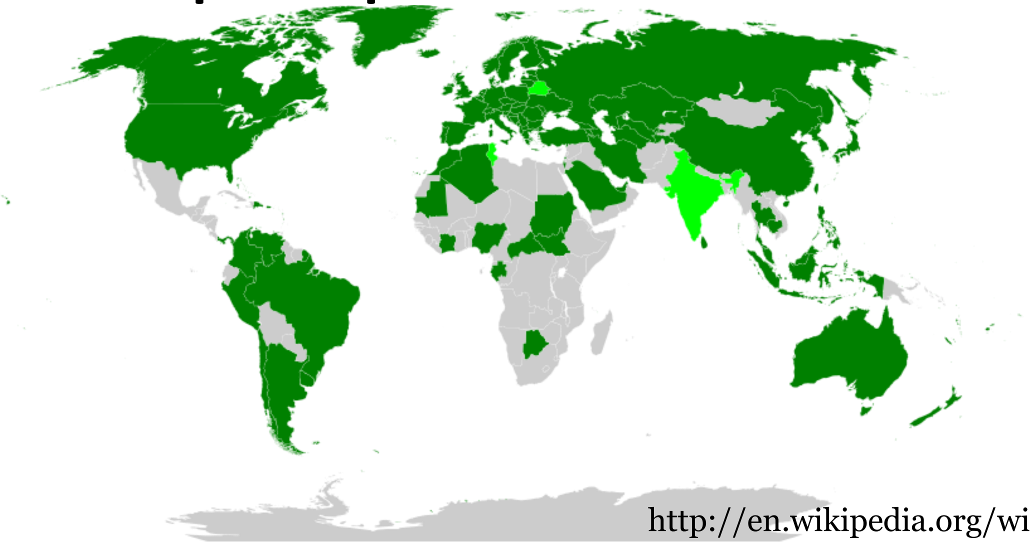
G.W. Bush

Other biometric techniques

- **Palm**
- Popular access control technique
- Acquisition of frontal and side view
- Cooperation required (can be hard for persons with arthritis - system of pegs)
- Not unique - not applicable for large-scale systems
- **Signature**
- Significant variations for the same individual
- Static and dynamic verification
- Forgery of signature dynamics is almost impossible
- **Ears, gait, odor, DNA …**



Biometric passport



http://en.wikipedia.org/wiki/Biometric_passport

- Combined paper and electronic passport
- Contactless smart card
- PKI for authentication of stored data
- Standards for face, iris, fingerprint recognition
- ICAO – Int. Civil Aviation Org. (Doc. 9303)Popular access control

Attacks on biometrics

- ➢ **Fingerprints copies by**
- Gelatin or tape and even Wine gum
  https://youtu.be/Fxdhb65iciM
- high res photos
  https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

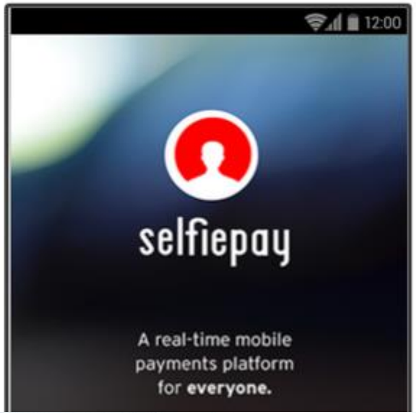
- ➢ **But**
- Modern security devices check for liveness
  (not all modern smartphones with fingerprint reader)

Biometrics – future or present?

- ➢ Camera technology
- Iris/retina scan
- Behavior analysis
- Thermoanalytics scan

Biometrics – future or present?

- ➢ Future Shop
- ➢ Pay with fingerprint, PayPal, . . .
- ➢ Visa card biometrics at ATM
- ➢ MasterCard launch selfie pay



selfiepay

A real-time mobile payments platform for **everyone.**

Recap: something you are

- Vary each time you measure them
- Scheme must allow variation
- Can deny access to legitimate users
- Can allow access to illegitimate users
- Can be copied
- Can be obtained by others quite easily
- Cannot be changed if compromised
- Cannot be handed over in duress

Final thoughts

- Biometrics are not secret
- Biometrics are (ideally) unique to each individual
- Increasing number of successful attacks against biometric identification
  -> rethink before replacing password

➢ Recommendation: Biometric should be used

- for 2FA

Or

- In combination with password

Ingo Hölscher

IT-avdelningen APP

www.liu.se

LINKÖPING UNIVERSITY