

Introduction to Biometric Technologies and Applications (III)

Fernando Alonso-Fernandez (F510)
ITE School

Email: feralo@hh.se

Course: Biometric Recognition
DI4025

Outline

Limitations of Biometrics

Unsolved Problems

Social Acceptance

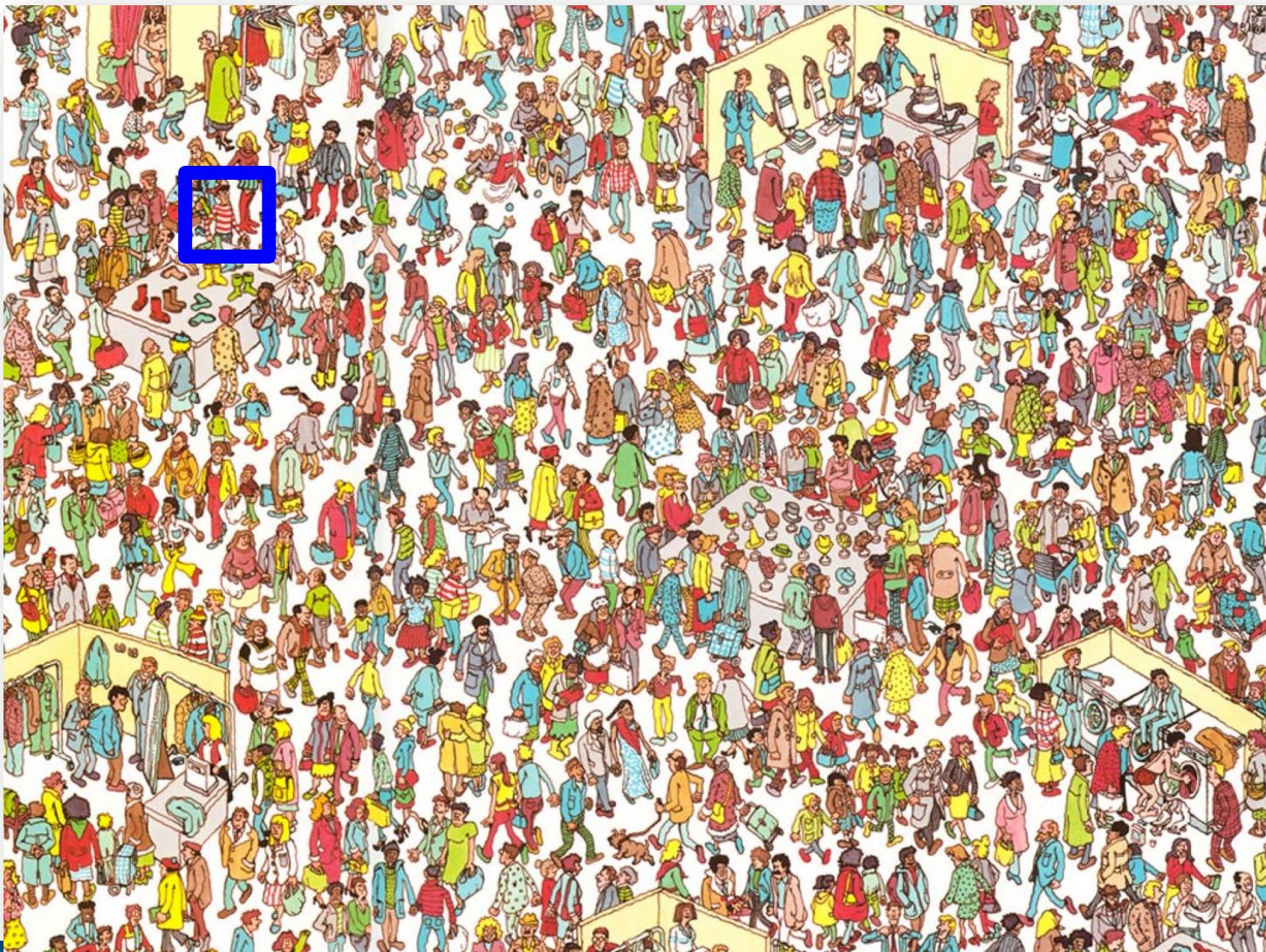
Design Considerations

Where's Waldo?

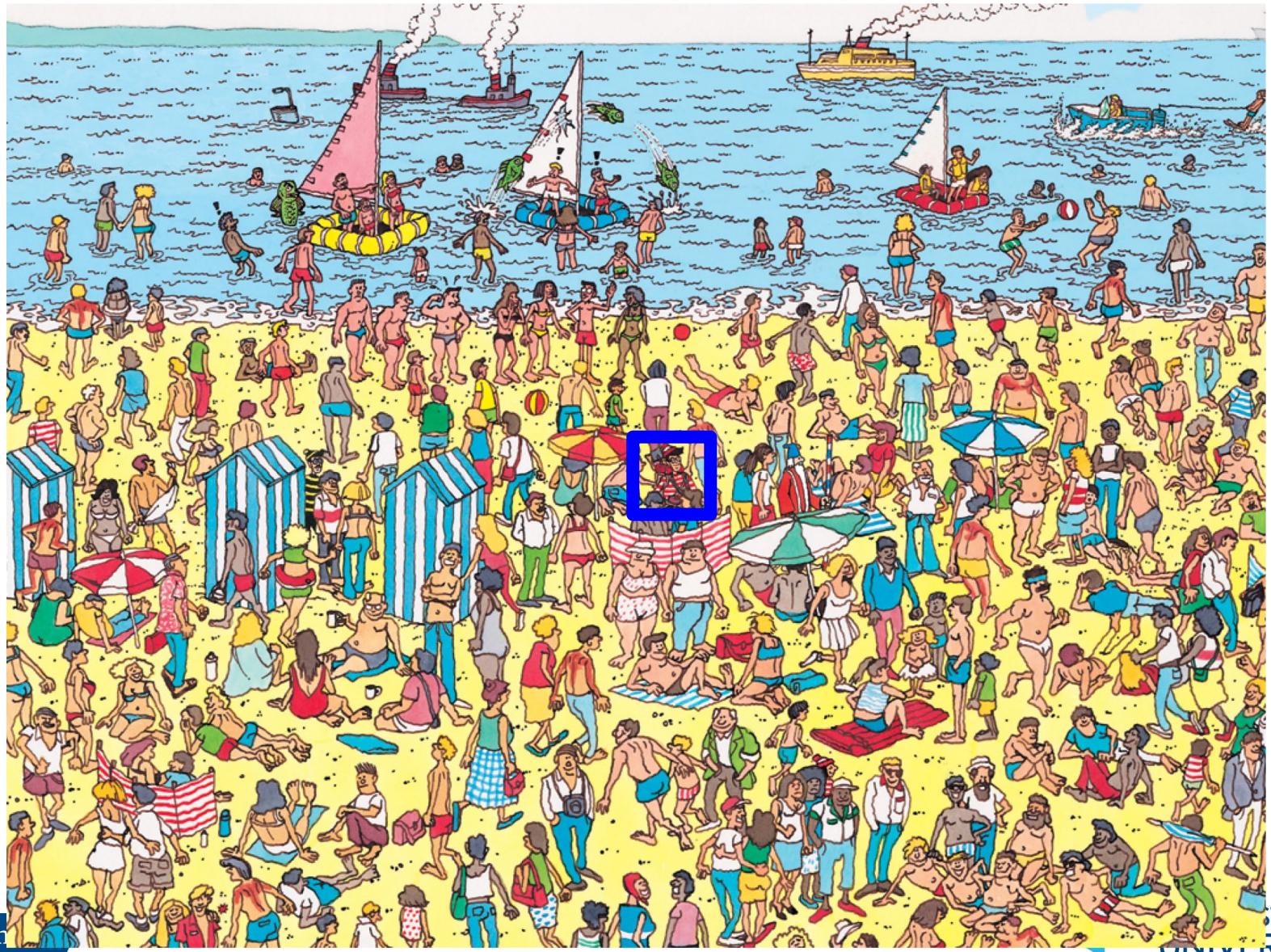
- Series of children's books created by [Martin Handford](#)
- Illustration of a large number of people engaged in various activities
- Readers are challenged to find a character named [Waldo](#)



Where's Waldo?



Where's Waldo?



Where's Waldo?



Other Characters Added



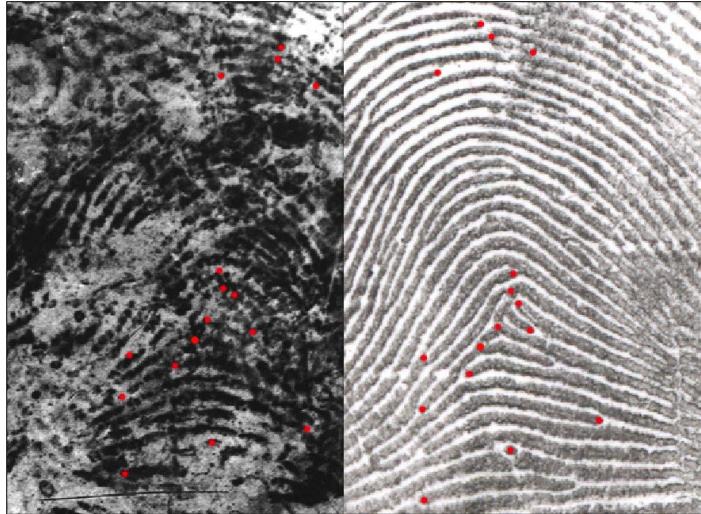
- **Odlaw, Wizard Whitebeard, Wilma, Wenda, Woof**

So Who Is Waldo?

- Waldo is defined by facial appearance, clothes, accessories
- Waldo's own appearance can change permanence
- The (challenging) environment also affects how Waldo appears:
 - different types of environments
 - large number of people around
 - some people can look similar to Waldo uniqueness
 - people (incl. Waldo) affected by:
 - engagement in diverse activities
 - variations in illumination and pose
 - occlusion or seen from different views

Real-world Matching

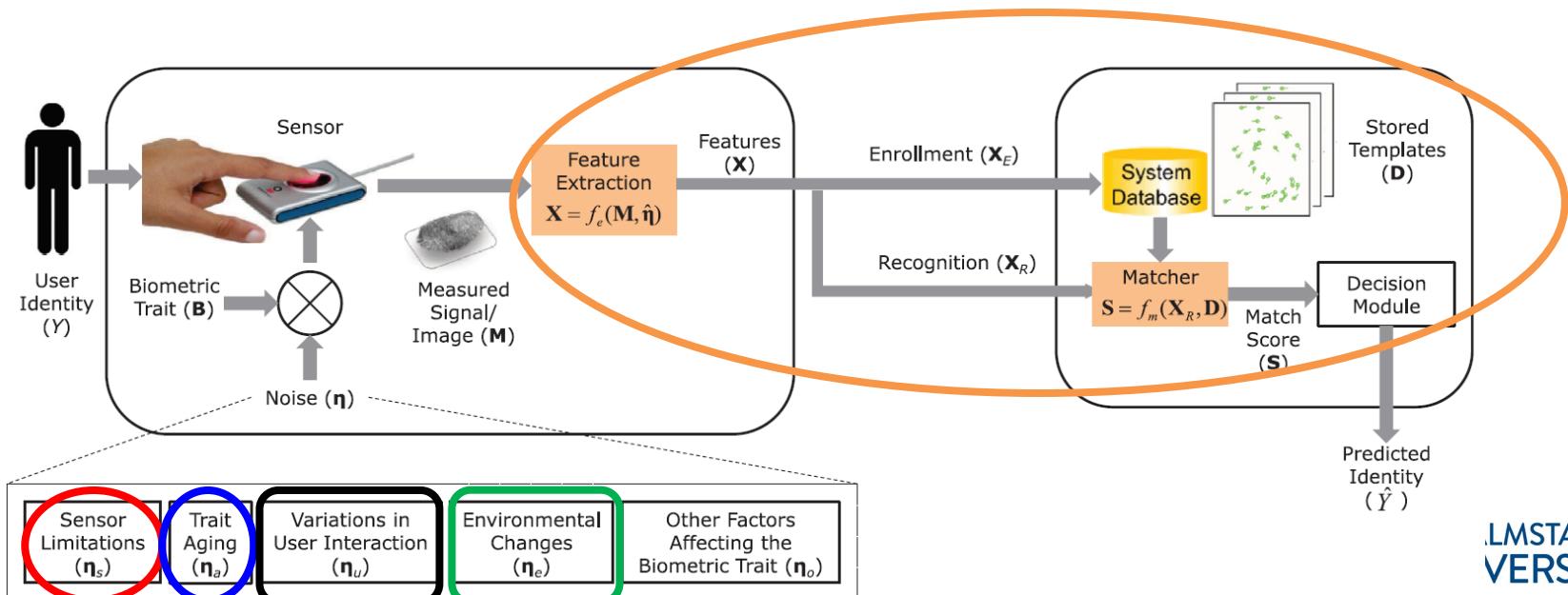
- Compute the similarity between two instances of biometric data **corrupted by noise**



Performance of Biometric Systems

Biometric systems **are not error free**. Two acquisitions of the same biometric trait are **never equal** (even if captured one after the other)

- **Sensor limitations**, e.g. low resolution/size...
- **Changes** in the biometric characteristics over time (aging)
- **Variations in user interaction/behaviour**, e.g. expression or pose, uncooperative subjects, make-up/accesories...
- **Variations in the environment**, e.g. light, weather...
- **Back-end processing** (algorithm, compression, speed...)



Performance of Biometric Systems

1) Fundamental issues related to the biometric trait itself

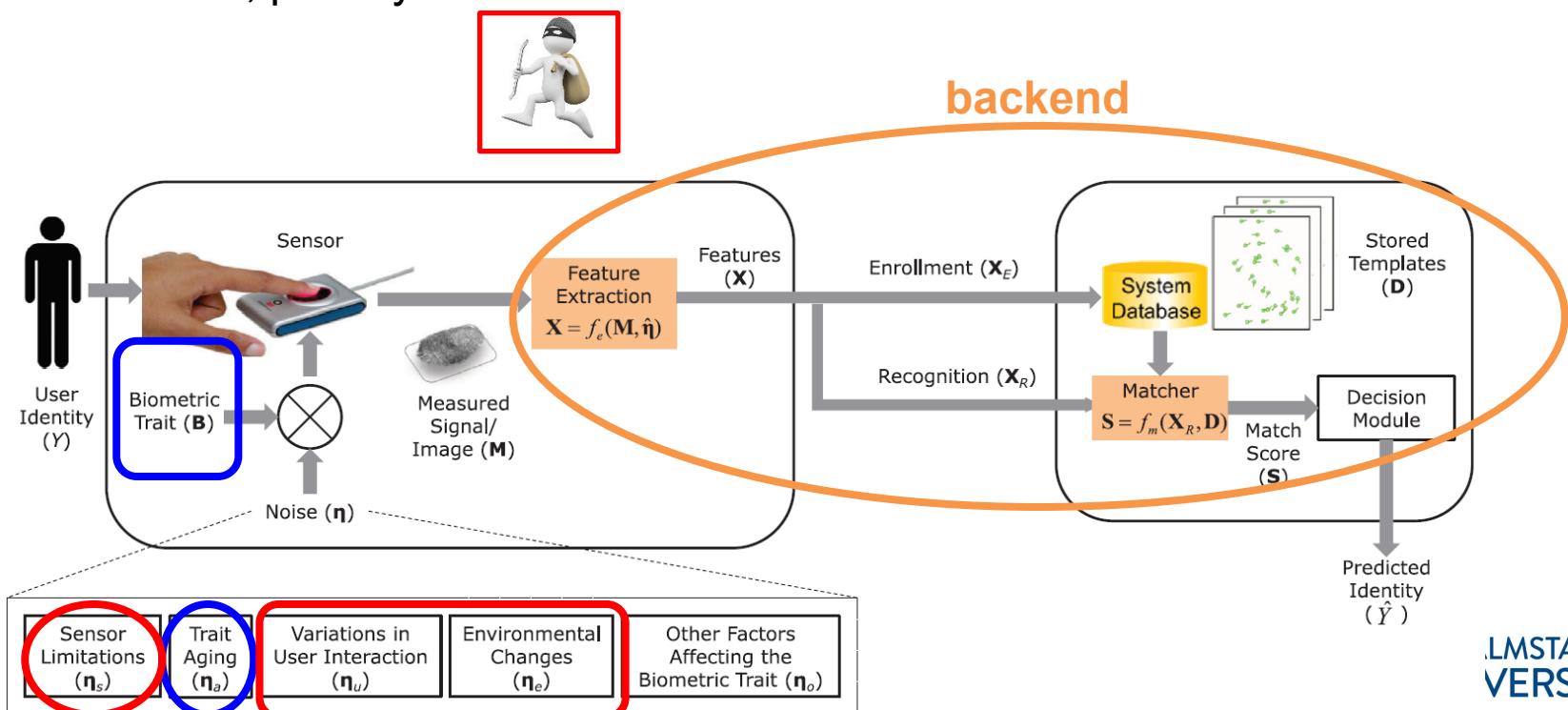
- Distinctiveness, non-universality, permanence, aging... (**trait B**)

2) Problems specific to the system

- Feature extraction/matching that can handle poor quality samples (backend)

3) Problems specific to the application

- Sensor, usability, user interaction, behaviour, environment... (previous slide)
- Attacks/threats, privacy...

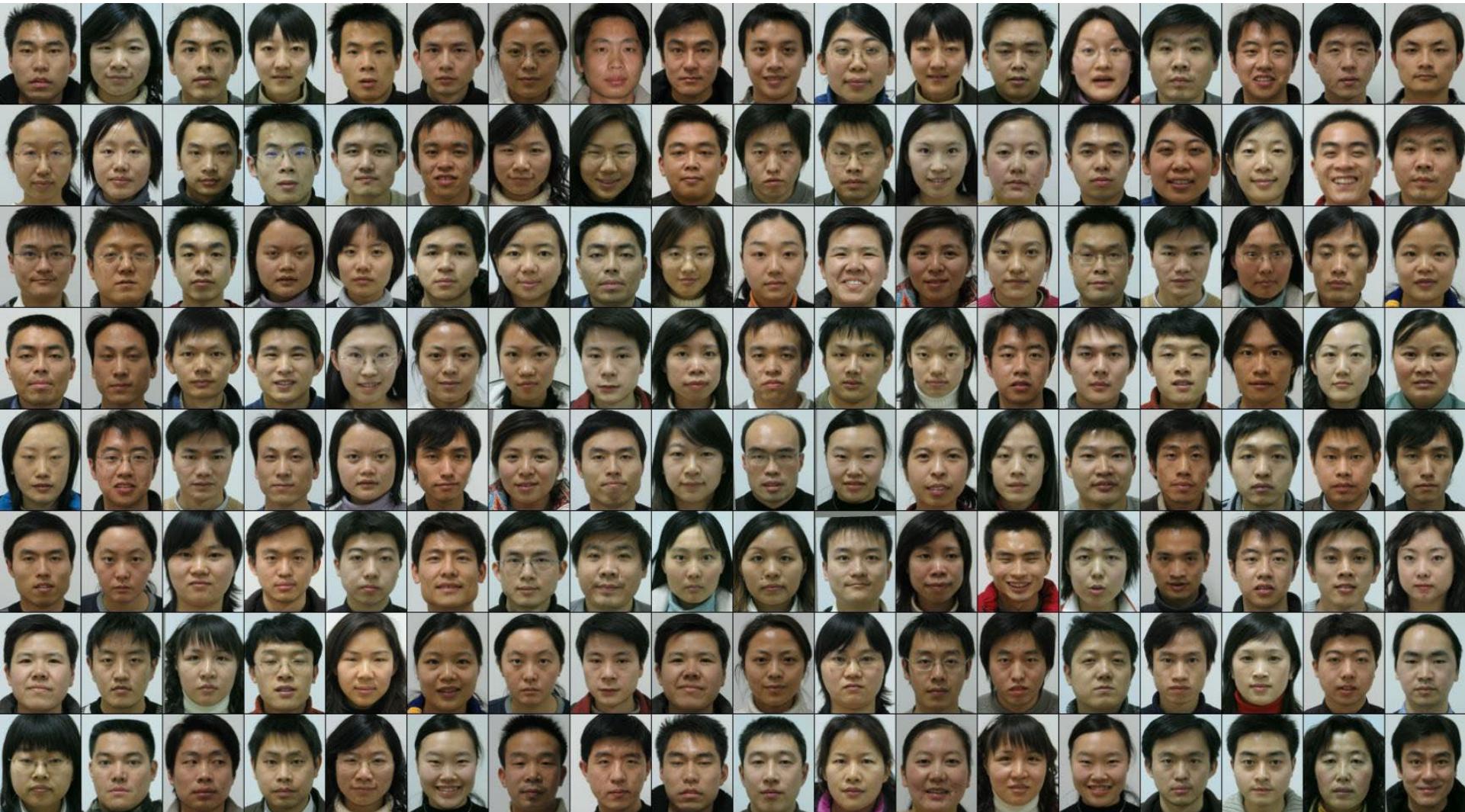


Distinctiveness/Uniqueness

- Given a 10-digit PIN, no. of unique identities that can be resolved = 10 billion
- But what can we say about a biometric trait?
- How many traits to identify 7 billion individuals?
- No rigorous scientific basis (yet)!

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Distinctiveness: Limit of a Biometric Trait?



Can we recognize all the 1.3B faces in China?

Distinctiveness: Inter-user similarity

Genetic similarity

- Face appearance
- Fingerprint and iris are known to be different for twins

Increases FMR/FAR



Identical twins



Mother and daughter

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Non-universality

- Some people may **consistently offer poor quality** fingerprint images which means they have to be identified by some other means



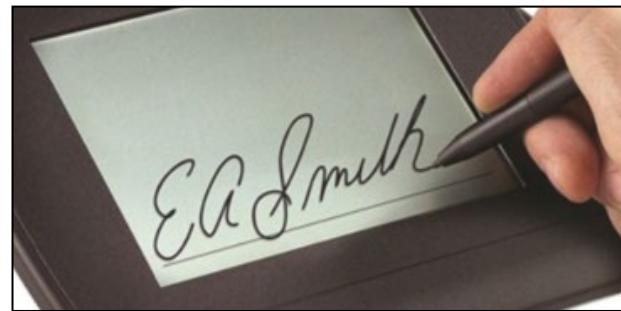
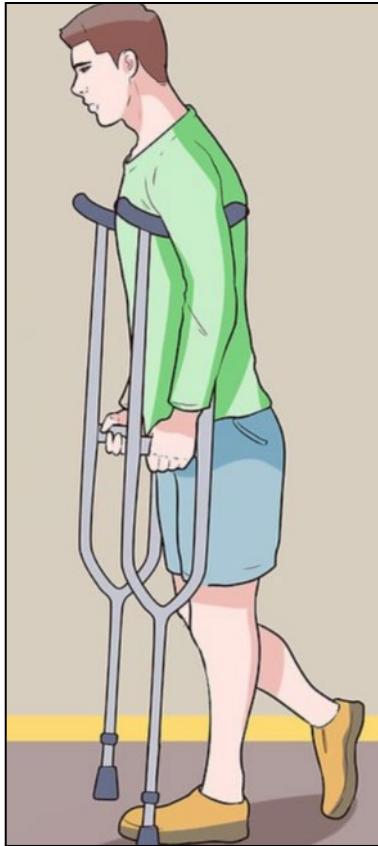
Four impressions of a user's print exhibiting incomplete ridge information

FTE: Failure-to-Enroll Problem

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Non-universality

- The same can happen to other biometric traits



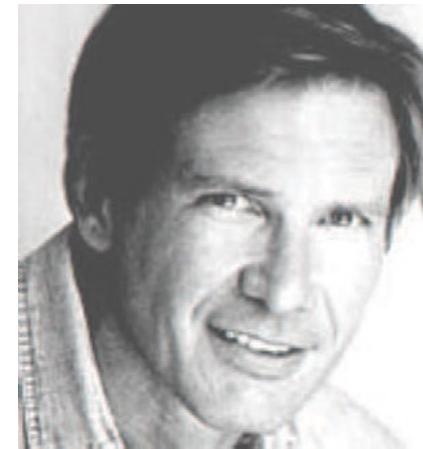
FTE: Failure-to-Enroll Problem

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Permanence (Aging)

- **Changes** in the trait over a time span
- **Inevitable, not controllable, different** for each person
- Some traits **more susceptible** to aging than others
(e.g. face, and in general behavioral traits)
- Can we **compute/predict** degree of change, so we can:
 - Account for it during **matching?**
 - Use **templates** unsensitive to the aging phenomenon?
 - Update the template in the **database?**

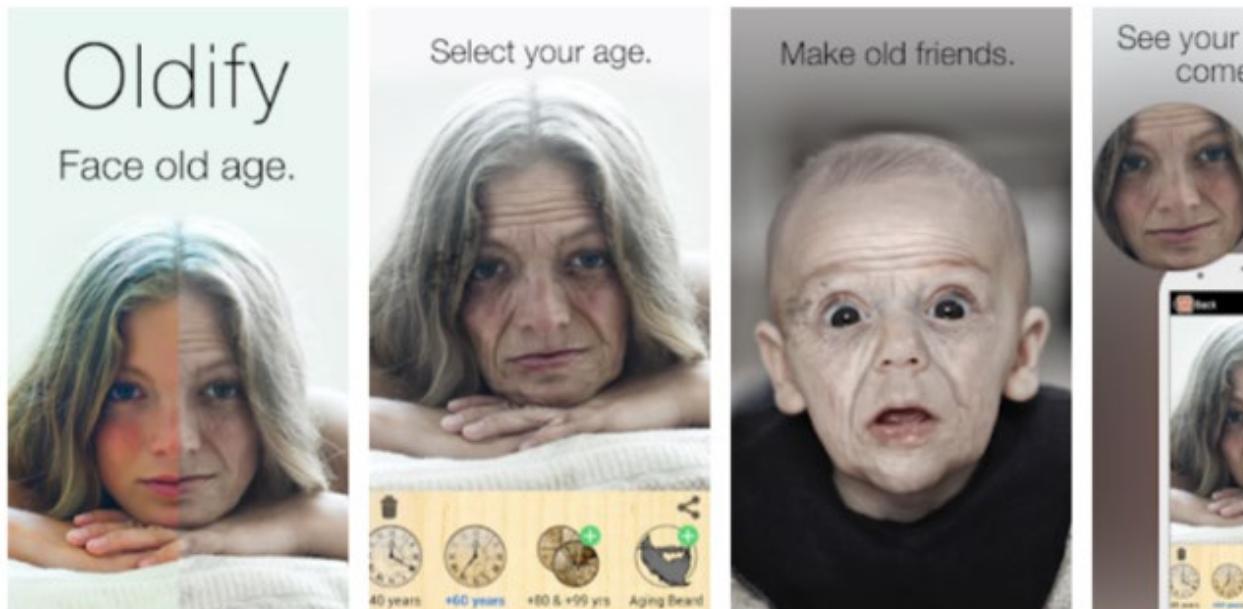
Increases FNMR/FRR



Distinctiveness
Universality
Permanence
Sensor
User
Environment

Permanence (Aging)

- Impact in **performance** is well documented for **face**, **fingerprint** (12yr) and **iris** (3 yr)...
- But **models to measure/predict** the changes, or if the degradation is due to **changes in the trait itself** (in fingerprint and iris), are yet open research questions
 - e.g. change in acquisition conditions, sensor...



Distinctiveness
Universality
Permanence
Sensor
User
Environment

Permanence (Aging)

Increases FNMR/FRR

Jan 1995



Gallery seed

Jul 1998



Score=0.99

Nov 1999



Score=0.62

Nov 2003



Score=0.41

Feb 2005



Score=0.26

Same woman arrested at different times

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Unconstrained Scenarios

In some applications, we **cannot impose requirements** to

- Sensing
- User behaviour/interaction
- Environment

For example

- **Crime scenes**
- **People on the move**
- **Surveillance**

We have to live with what we have!

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Sensor: Factors

- Ease of use and maintenance
- Ergonomics

- Capture area
- Resolution
- Noise
- Physical robustness
- Acquisition time
- Price

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Small Sensors



<https://media.giphy.com/>



© gizmodo

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Environment: Factors

Indoor use

- Surrounding light
- Dust, humidity, temperature, vibrations...

Outdoor use

- Difficult to define and fulfil illumination conditions
- Water, snow, wind, fog, temperature changes

Other people or objects (occlusion), ambient noise

Distance, motion...

Supervision by an operator

Distinctiveness
Universality
Permanence
Sensor
User
Environment

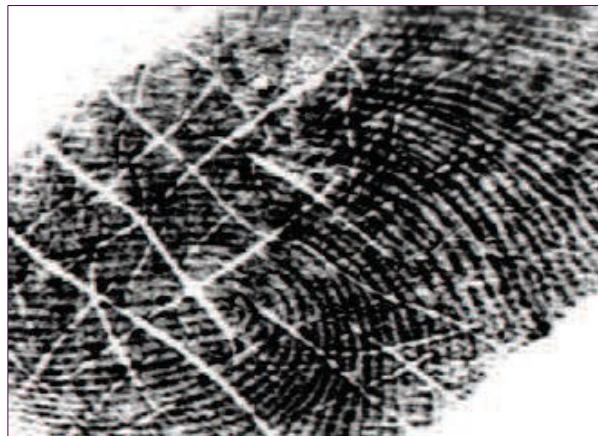
Environment: Noisy data

Can impact both FNMR/FRR and FMR/FAR

During enrolment



During recognition



Noise **due** to smearing, residual deposits, cuts and folds, etc

Environment: Variability

Can impact both FNMR/FRR and FMR/FAR



(a) Visa



(b) Mugshot



(c) Wild



(d) Border

Images from: NIST 2019 Report.

Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification.

Patrick Grother, Mei Ngan, Kayee Hanaoka

Distinctiveness
Universality
Permanence
Sensor
User
Environment

User: Factors

Changes in appearance: hair, makeup, clothes, glasses...

Changes in interaction:

- Eyes closed, expression, gaze...
- Different pressure, inconsistent contact...
- No clear (physical or other) guides

Familiarity with the system

Tired, distracted, nervous...

Cooperative

Manual work, skin condition, diseases...

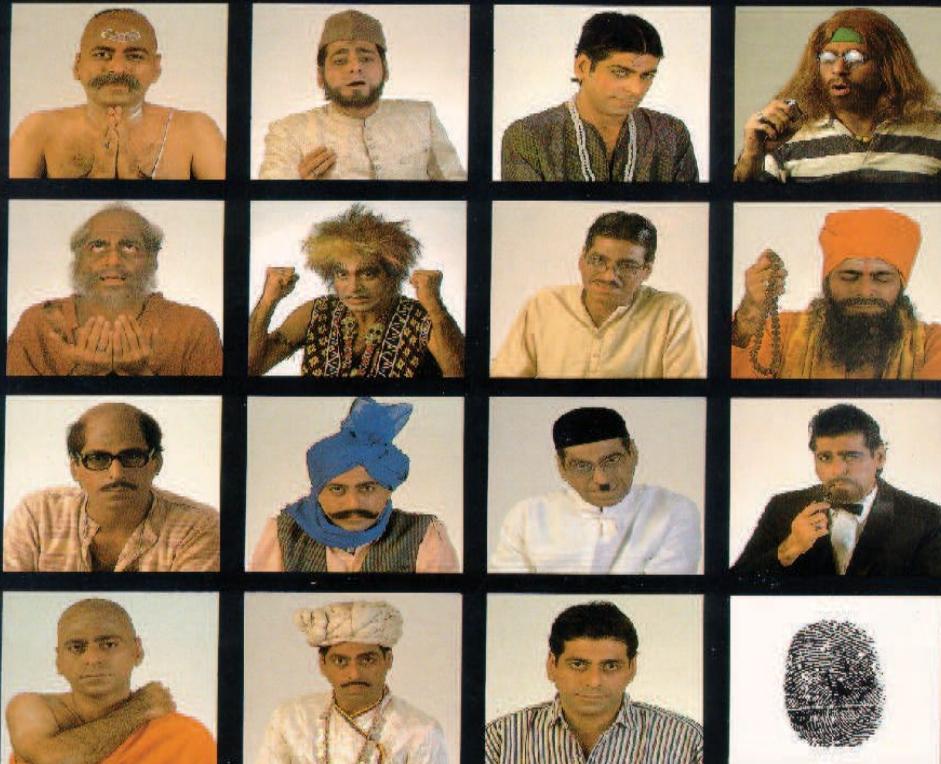
Age, gender, ethnicity...

Distinctiveness
Universality
Permanence
Sensor
User
Environment

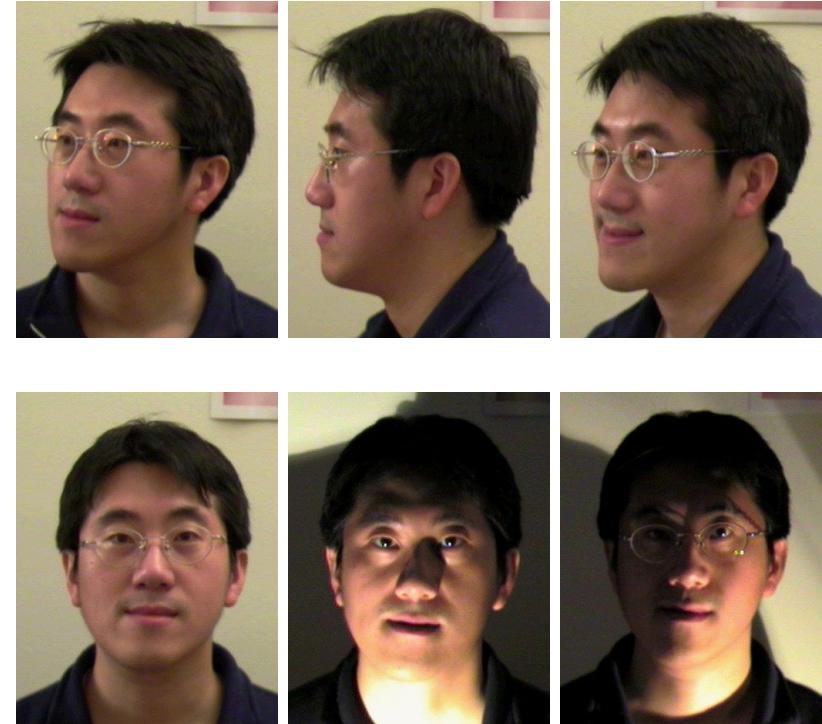
Intra-user variations

Increases FNMR/FRR

FACES CAN LIE.



FINGERPRINTS, NEVER.



Distinctiveness
Universality
Permanence
Sensor
User
Environment

Crime Scenes

Brussels attacks March 2016



Distinctiveness
Universality
Permanence
Sensor
User
Environment

Crime Scenes

International Business Times.



News

World

Business

Politics

Technology

Science

Sport

Entertainment

Opinion

Lifestyle

Crime

ISIS

Islamic state

Brussels attacks: Freelance journalist believed to be '3rd bomber' faces terror charges

By Ian Johnston

March 28, 2016 15:45 GMT



Freelance journalist Faycal Cheffou, seen presenting a media report about conditions at a centre for asylum seekers in 2014, has been charged with terrorist offences. (YouTube)

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Crime Scenes

Brussels attacks March 2016



Distinctiveness
Universality
Permanence
Sensor
User
Environment

Crime Scenes

Boston Marathon Bombings April 2013

Probes



Gallery



Tamerlan Tsarnaev



Dzhokhar Tsarnaev



1 Million PCSO Mugshots

(a)

(b)

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Crime Scenes

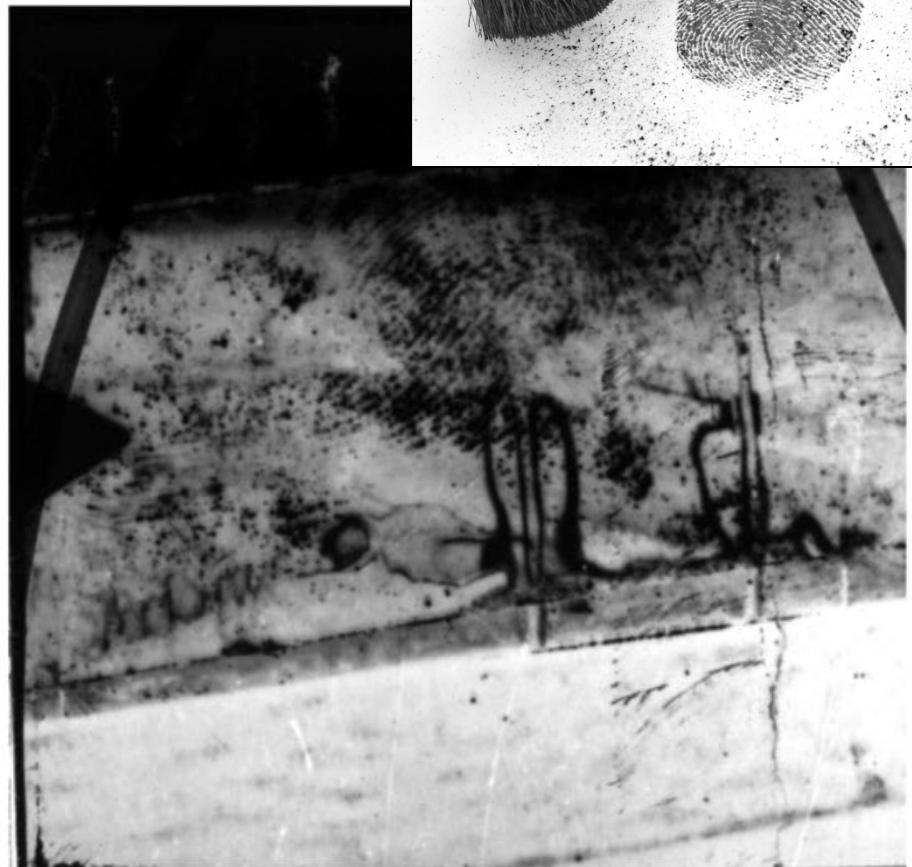
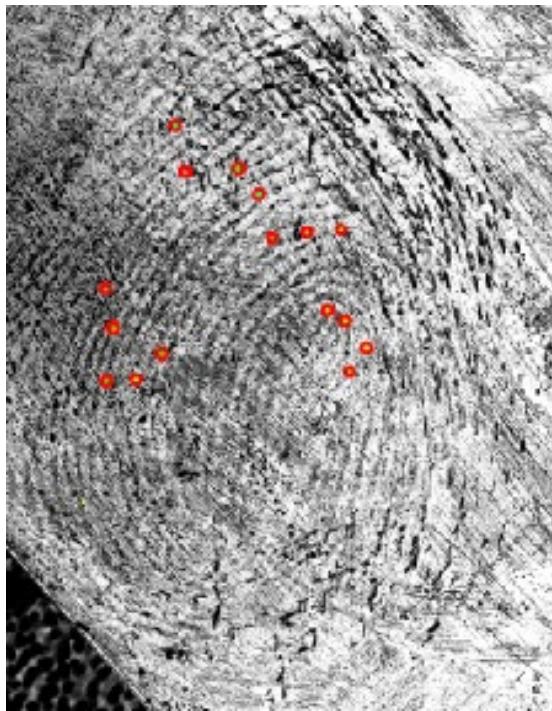


Figure 2.1: Fingerprint acquired after arrest or through background checks, tenprint (one of ten), and fingermark, developed from a latent left at crime scene. Note that only part of the corresponding tenprint is present in the fingermark, and that the quality of the images also differ significantly.

Crime Scenes

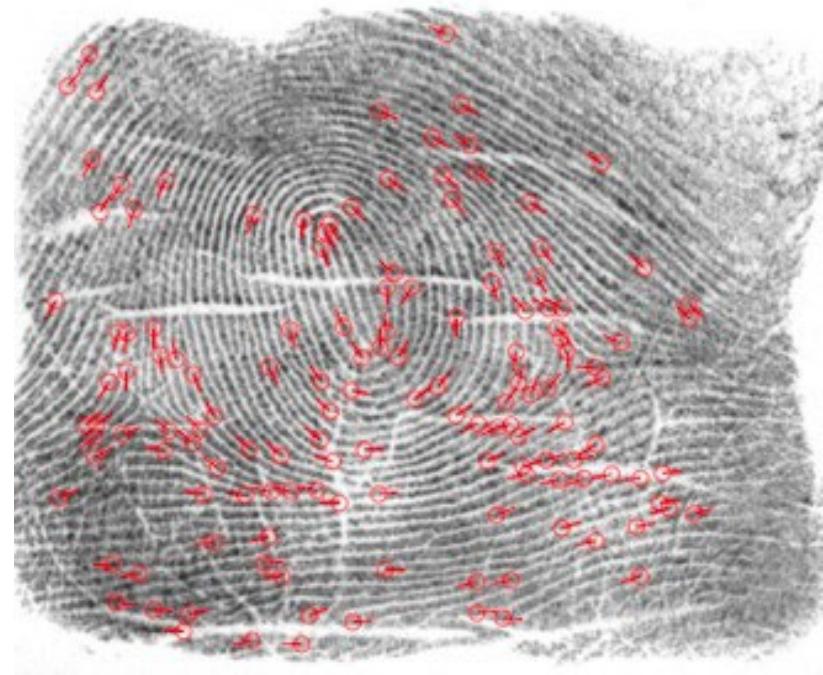
Computer-assisted approach in forensic science

Fingermark



Manual encoding

Reference Fingerprint

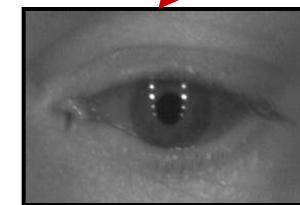
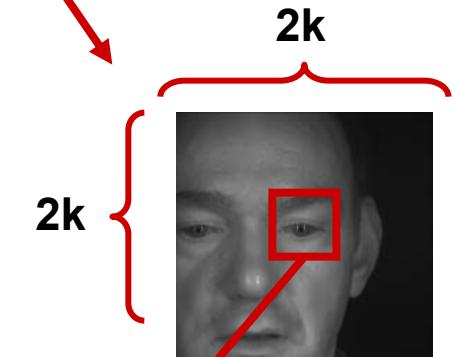
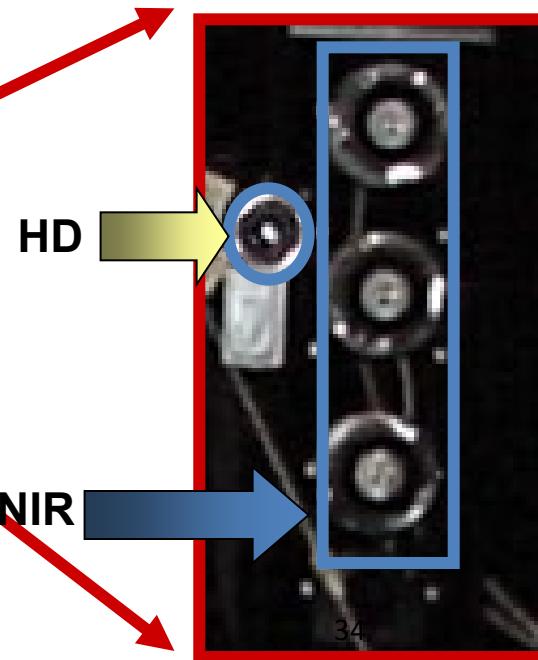
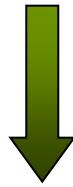


Automatic encoding

People on the Move: Iris at a Distance

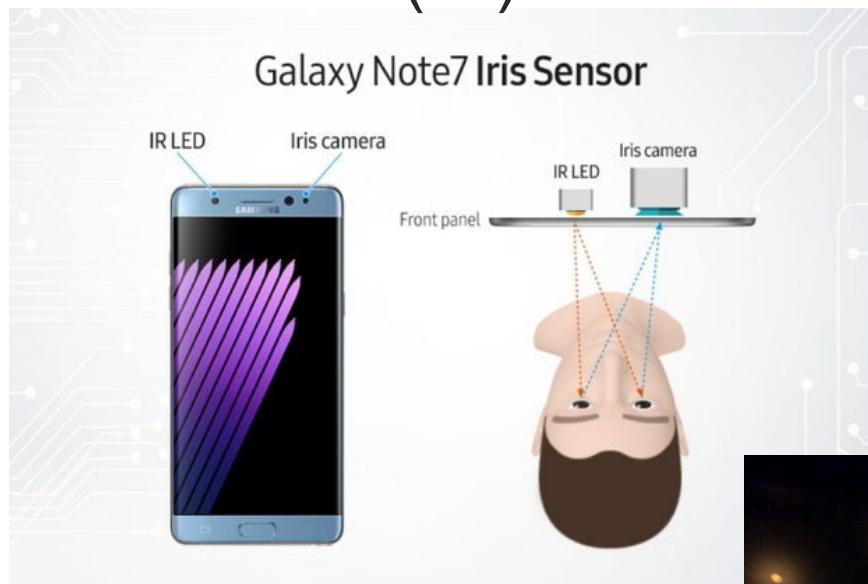
Portal video (NIR, HD)

<https://www.youtube.com/watch?v=b1uZonksCnI>



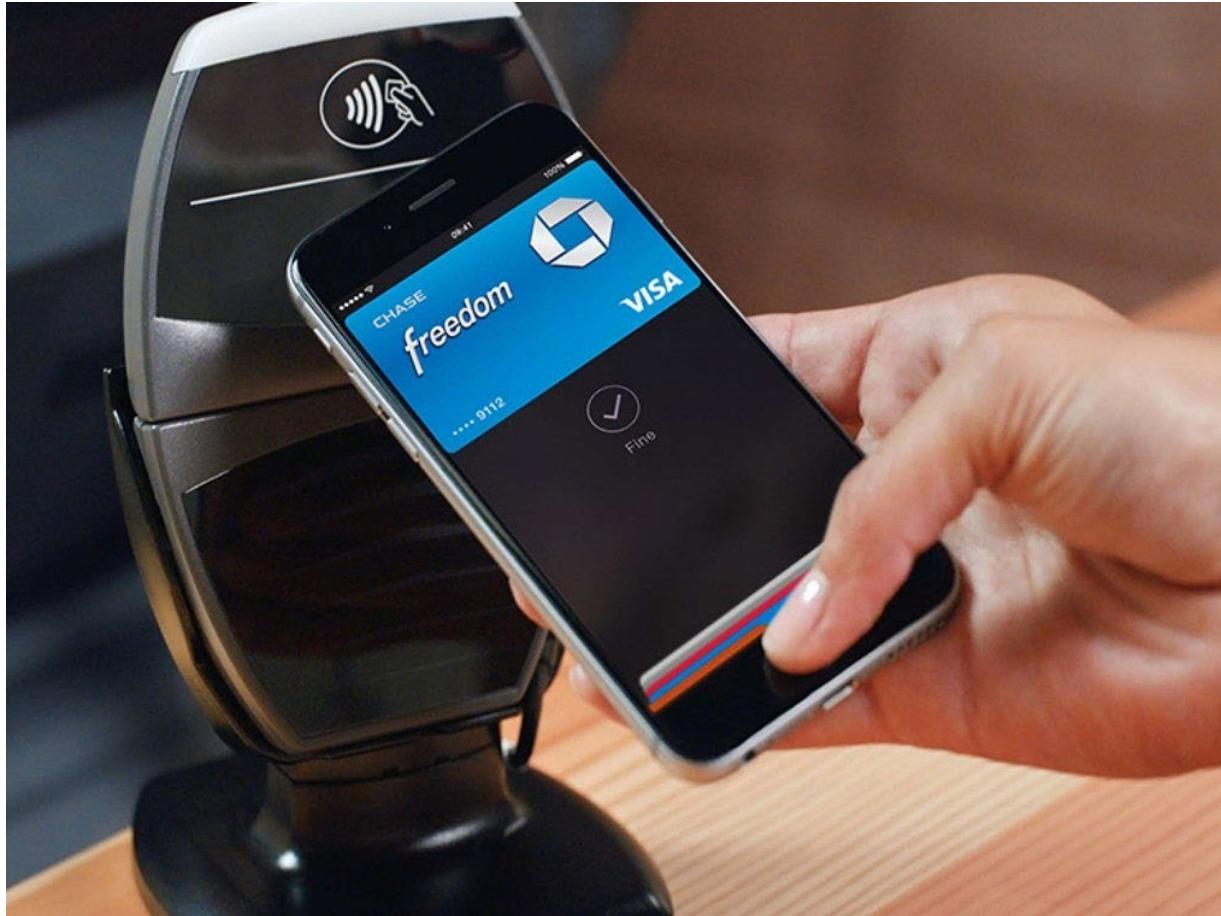
People on the Move: Iris (Smartphones)

Infra-red (IR)



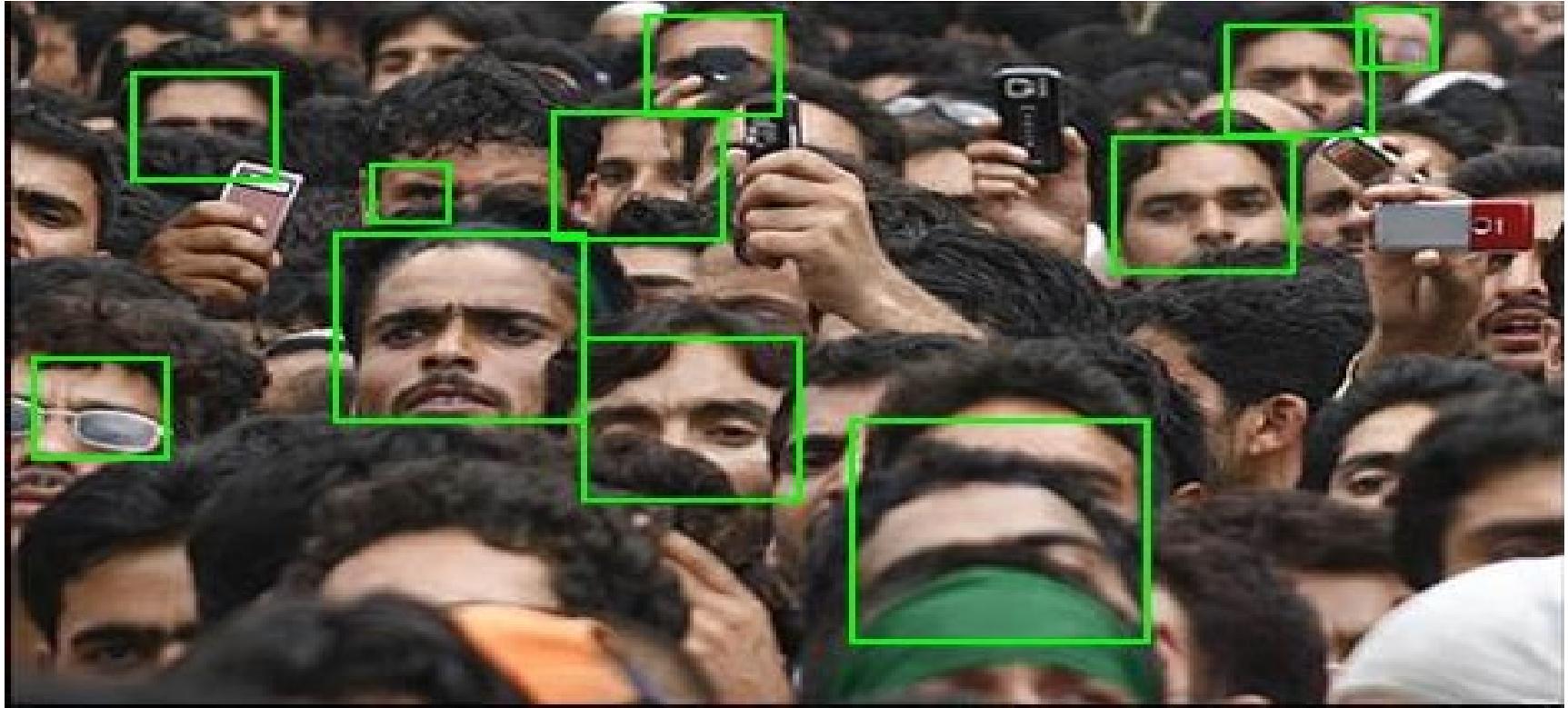
Distinctiveness
Universality
Permanence
Sensor
User
Environment

People on the Move: Fingerprint (Smartphones)



Distinctiveness
Universality
Permanence
Sensor
User
Environment

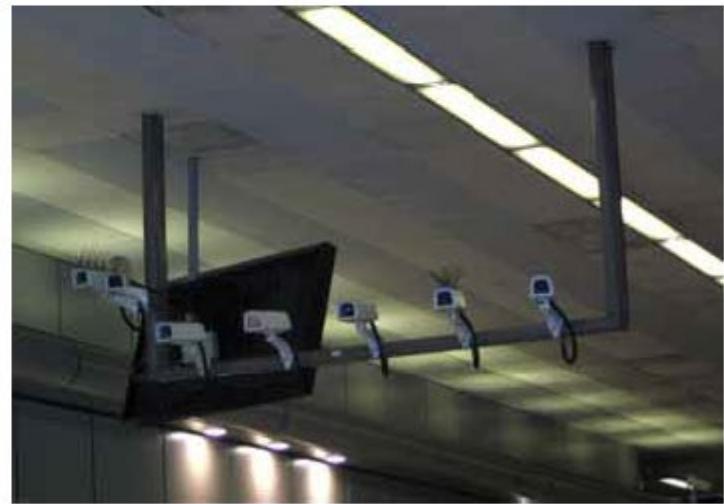
People on the Move / Surveillance



Not all faces can be detected by the best algorithm!

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Surveillance



1M CCTV cameras in London & 4M in U.K.; average Briton is seen by 300 cameras/day;
400K cameras in Beijing provide 100% coverage of public places; 150K cameras in Seoul

Surveillance

Proliferation due to deterrent factor

Poor quality

- Low resolution of the camera
- Large distance, subject moving
- Illumination, pose, expression, occlusion
- Non-cooperative, hide the face

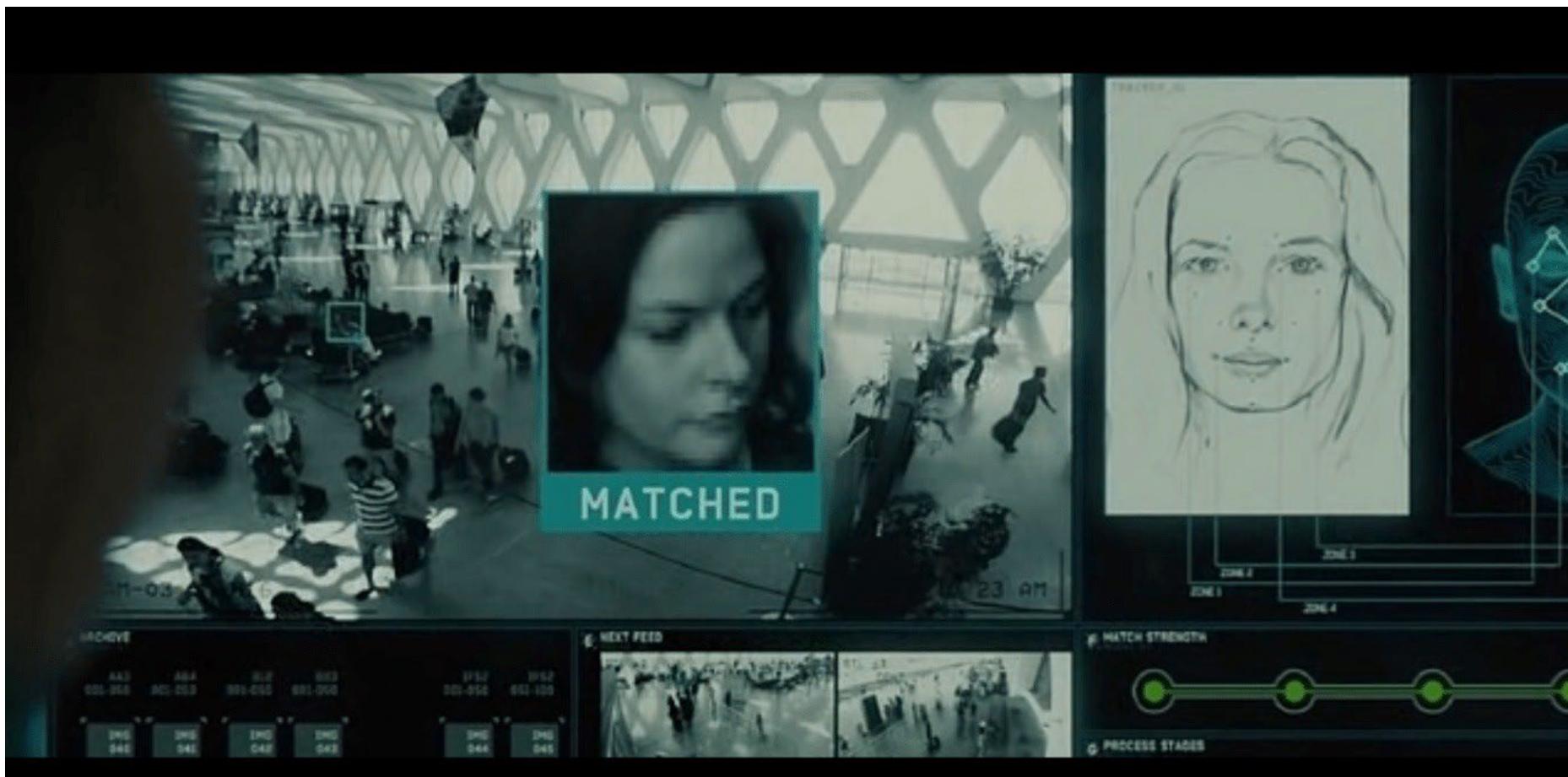
Almost all CCTVs are passive (merely record)

Still a very challenging (unsolved) problem

Distinctiveness
Universality
Permanence
Sensor
User
Environment

Surveillance

CSI fiction

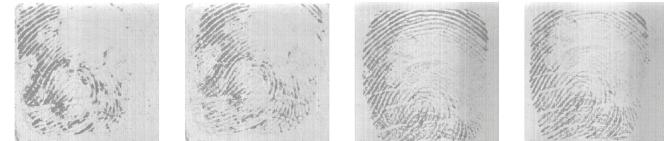


Limitations of Biometrics: Summary

Distinctiveness: number of distinguishable patterns



Non-universality: failure to enroll



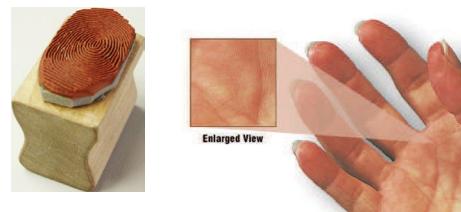
Permanence: aging

Unconstrained scenarios

- Sensing: noise, maintenance
- Intra-user variations: variations in interaction, behaviour, environment



Spoof attacks: circumvent the system by imitation or using artificial traits
(topic of another lecture)



Acceptance of Biometrics

Numerous large-scale deployments of biometrics worldwide.
At the same time, privacy concerns and debates about social
and ethical acceptance have emerged

Acceptance is mostly dictated by human factors (and by
legislation)

ZERO effort: users don't want to change their behaviour,
don't expect them to do anything differently!

- Ease and **comfort** in the interaction leads to better acceptance
- Reluctance to **physical contact** with the sensor?
- Convenience if **no cooperativity** is needed (e.g. face)
 - but the user could be captured without knowledge (**privacy**)

<https://nordic.businessinsider.com/china-guiyang-using-facial-recognition-to-arrest-criminals-2018-3>

Privacy

What else is revealed in a biometrics signal?

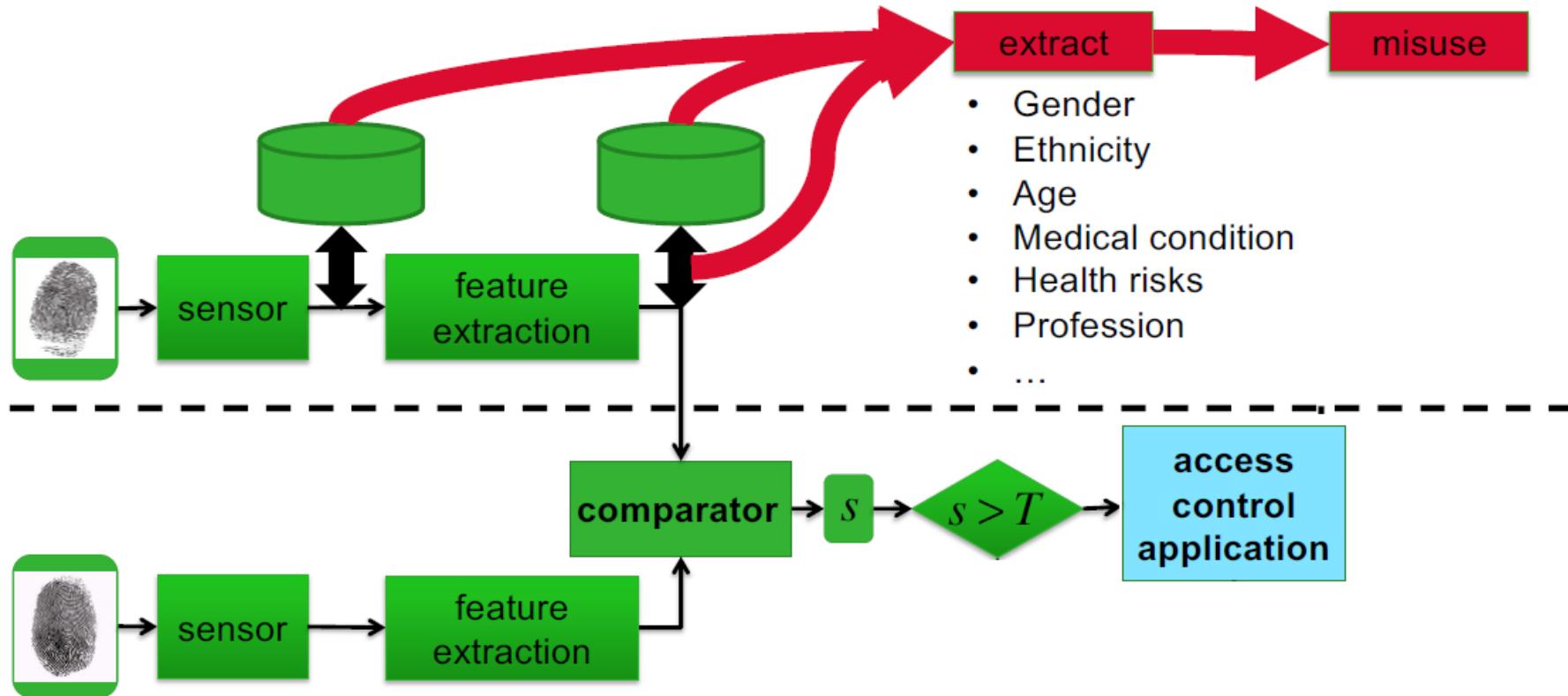


Image credit: R. Veldhuis (University of Twente)

Privacy

Linking and tracing across applications and databases

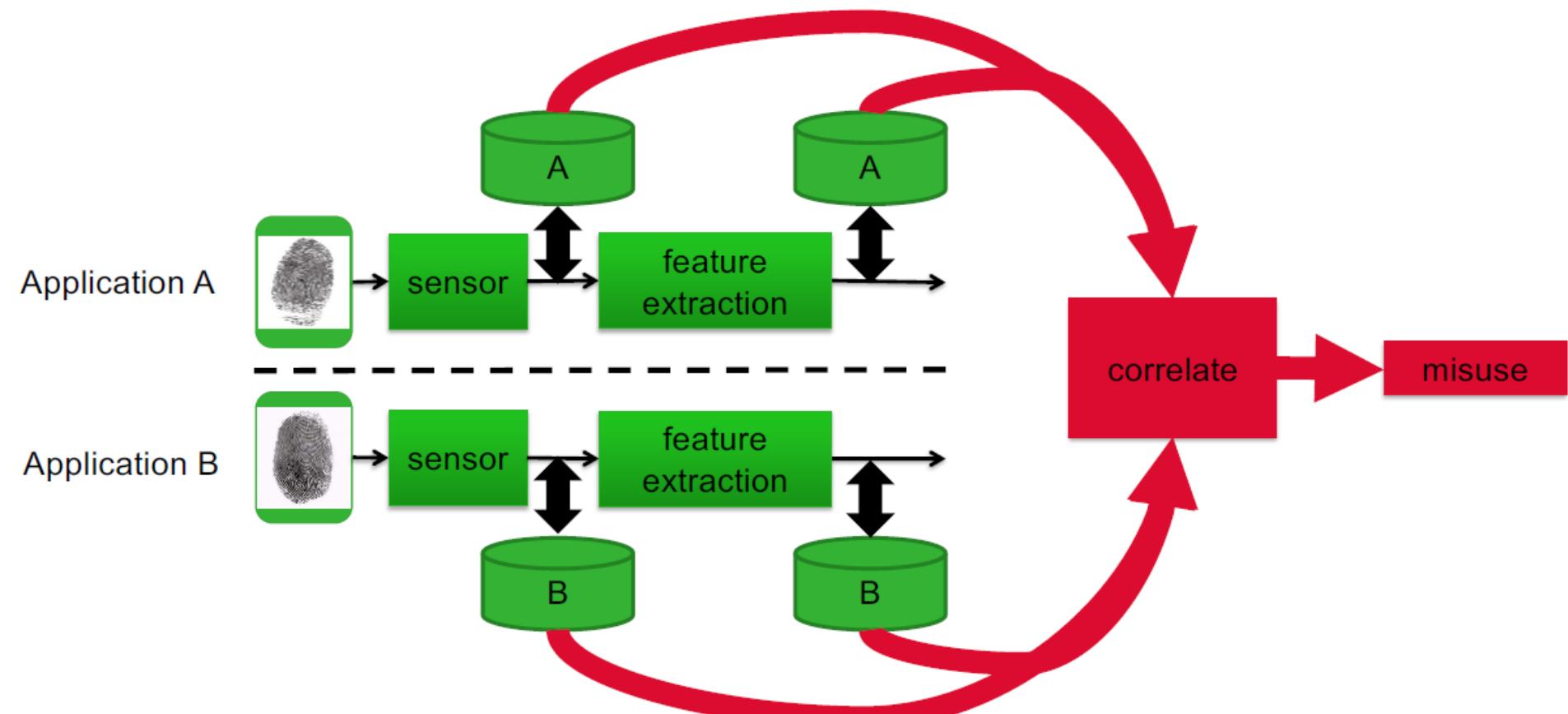
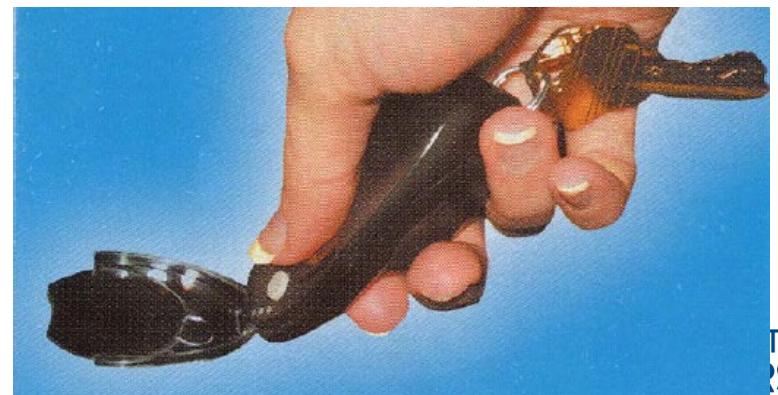


Image credit: R. Veldhuis (University of Twente)

Acceptance: Smart Cards

Biometric data stored in a
personal (smart) card

- Do not store raw data, but only **features** (this is in general, even if we use a centralized database)
- Recognition in the **own card** (processing chip) or in the sensor
- The only answer is a decision of acceptance/rejection, **no biometric data travels** through the network



Acceptance: Smart Cards



**MASTERCARD
IDENTITY CHECK**
PUSHING DIGITAL PAYMENTS FORWARD
WITH BIOMETRICS

**TOUCH, TAP,
BLINK!**

MASTERCARD IDENTITY CHECK
is already allowing consumers to authenticate digital payments using facial, iris scan and fingerprint recognition.

AS OF APRIL 2019
biometric solutions will be offered by all banks working with Mastercard.

CONSUMER PREFERENCE:
93%
of consumers prefer biometrics over passwords

CONSUMER EXPERIENCE:
70%
less abandonment rates with biometrics

Mastercard Identity Check:
Digital biometric solution for the digital age

www.newsroom.mastercard.com | @MastercardNews | @MastercardEU

The advertisement for Mastercard Identity Check features a central figure of a person holding a smartphone with a fingerprint icon on the screen. Below the figure are four circular icons representing safety, speed, ease, and personalization. The background is orange and red, with the Mastercard logo at the top right.



Design Considerations

Multiple factors to consider

- **Performance** of the biometric trait?
- **Sensor, Environment & User** factors (previous slides)
- **Back-end**: transmission speed, storage, processing?
- **Database**: size?
- **Working mode**: Identification or verification?
- **Privacy**: transparent recognition? protection measures?



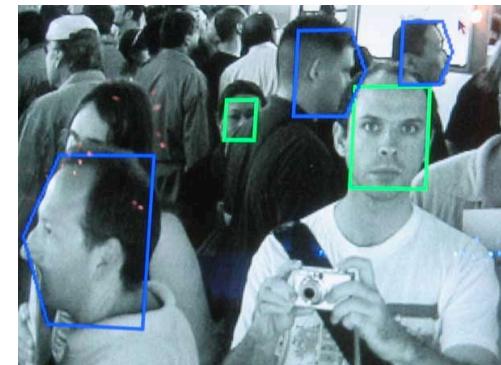
Design Considerations: Forensics

Forensics has some particularities

- We cannot determine **in advance** which evidence (trait) we will employ
- **Quality** of the evidence (sample) is typically lower (non deliberately deposited)
- We cannot ask the individual to produce **another** sample
- Involves **manual** collection and examination (which can lead to personal interpretation)



Latent fingerprint



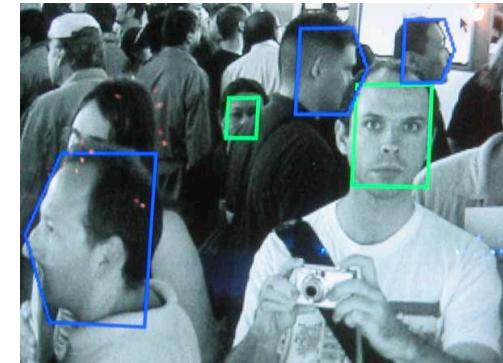
Design Considerations: Forensics

Forensics has some particularities

- **Real-time** is not a requirement
- **False non-match** is highly undesirable, since it can exclude the perpetrator from further consideration (at the risk of increasing false matches)
- Outcome often needs to be communicated **verbally** to a jury or a judge



Latent fingerprint



Introduction to Biometric Technologies and Applications (III)

Fernando Alonso-Fernandez (F510)
ITE School

Email: feralo@hh.se

Course: Biometric Recognition
DI4025