Biometrics - Blessing or Curse?

Jürgen Kühn
Senior Consultant

Frankfurt, 27.4.2016

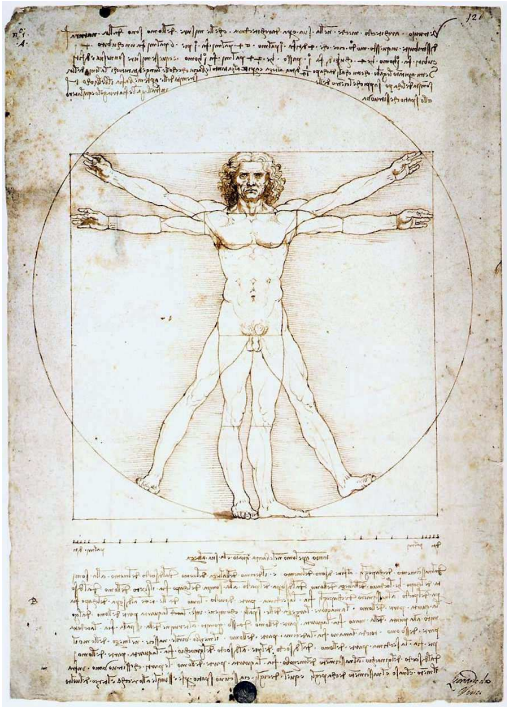
Personal

Jürgen Kühn

Senior Consultant

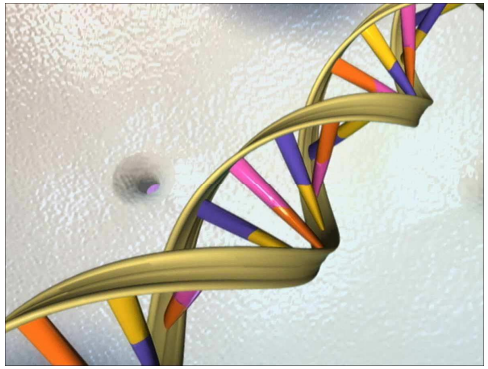
Dipl.-Ing. Nachrichtentechnik UNI Duisburg
Identity and Access Management
Single Sign-On
Smartcards
Biometrics
PKI
IT Security
Database Security

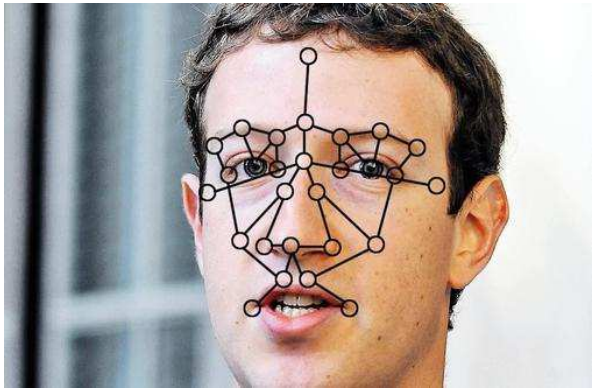
Agenda



- Basics
- Fingerprint
- Iris scan
- Face recognition
- Hazards
- Discussion

Biometrics in everyday life





What is Biometrics

- "Science of counting and [body] measurements on living organisms "
- From Greek
- Bios = Life
- Métron = Measure

- Biometrics is a technique for identification and authentication of persons based on specific physical characteristics

Source: DUDEN - Das große Fremdwörterbuch

Features of biometric characteristics

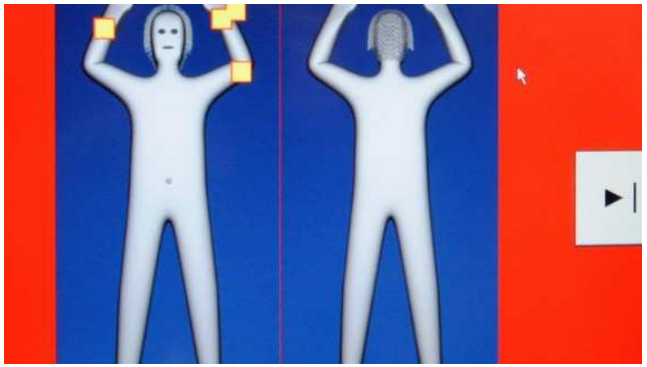
Universality

Uniqueness

Permanence

Detectability

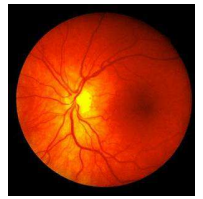
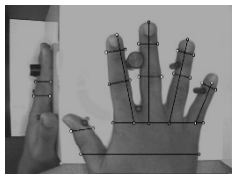
Features of biometric characteristics

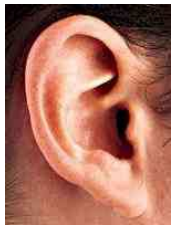
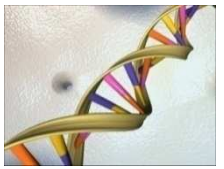


Characteristics for biometric identification

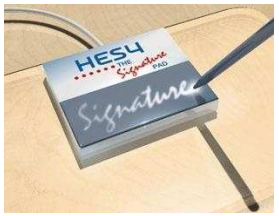
- Physiological features
  - Fingerprint
  - Face
  - Iris
  - Retina
  - Hand geometry
  - Vein pattern
  - Ear geometry
  - DNA

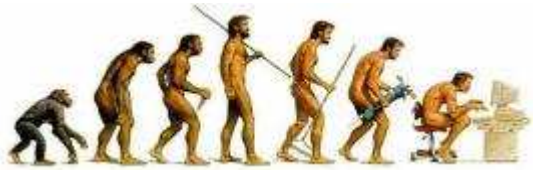


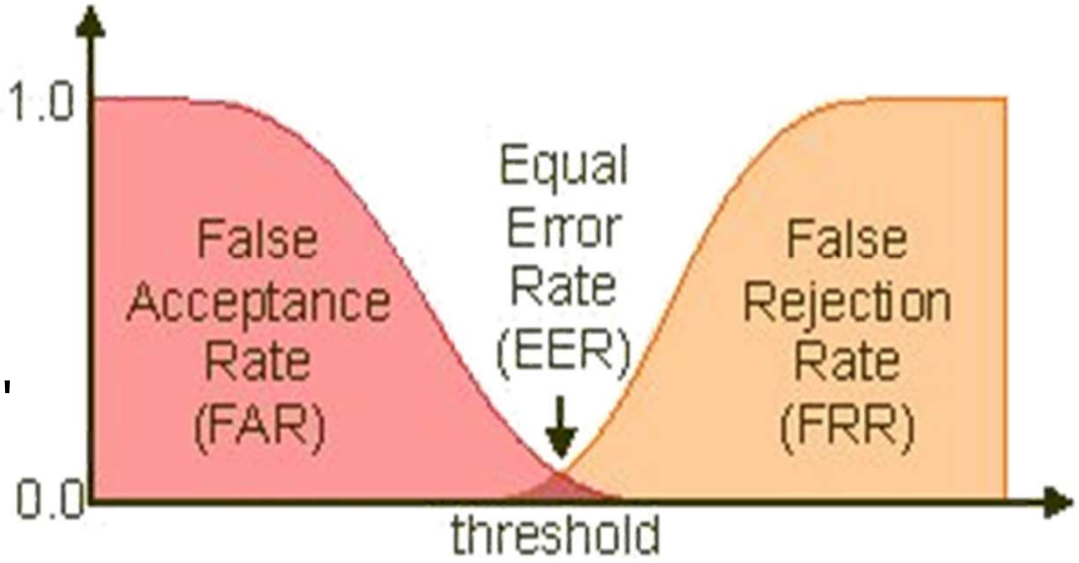
- Behavior-based features
  - Signature (dynamic / static)
  - Gestures / facial expressions while speaking
  - Walk
  - Lip movement
  - Voice / speech behavior
  - Keystroke at the keyboard



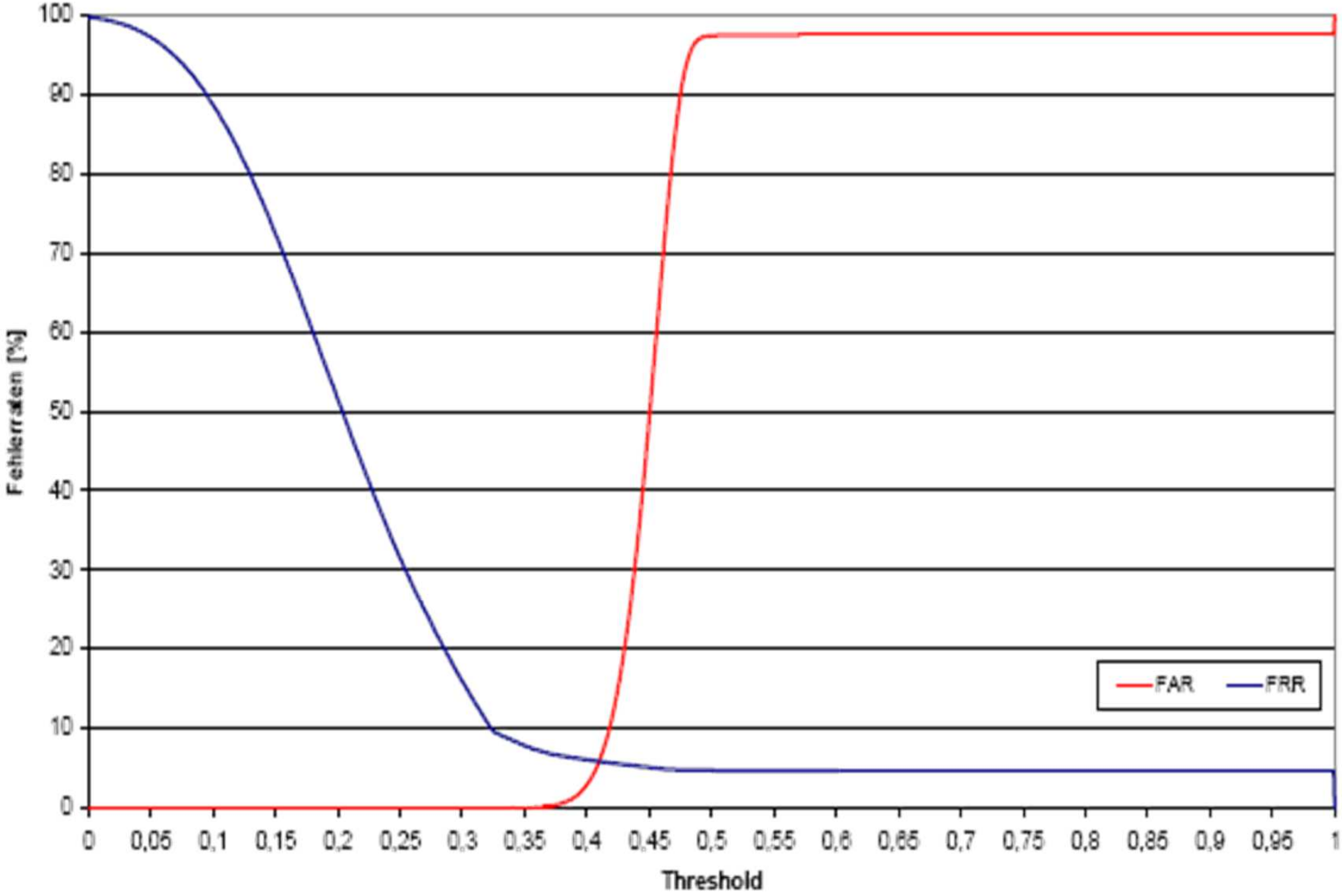
FAR und FRR (1)

- Only a probability of correspondence
- False Acceptance Rate FAR
  - Rate of unjustified accepted persons
- False Rejection Rate FRR
  - Rate of unjustified rejected persons
- Equal Error Rate ERR
  - FAR = FRR
- Threshold determines whether the system is "secure" or "comfortable"



FAR und FRR (2)

- Reality



Verification and Identification

- Verification
  - Check against only one reference
- Identification
  - Check against any number of references
  - Probability of false detection increases exponentially with the number of references
- Several attempts at one reference
  - 2 attempts and FAR = p

    $P(2) = p + (1-p)*p$
  - n attempts and FAR = p

    $P(n) = p + (1-p)*p + (1-p)*(1-p)*p + \ldots = 1 - (1-p)^n$

FAR = 0,002
N = 200, P(N) = 32%
N = 2000, P(N) = 98%
N = 10000, P(N) = 99.999%

Agenda

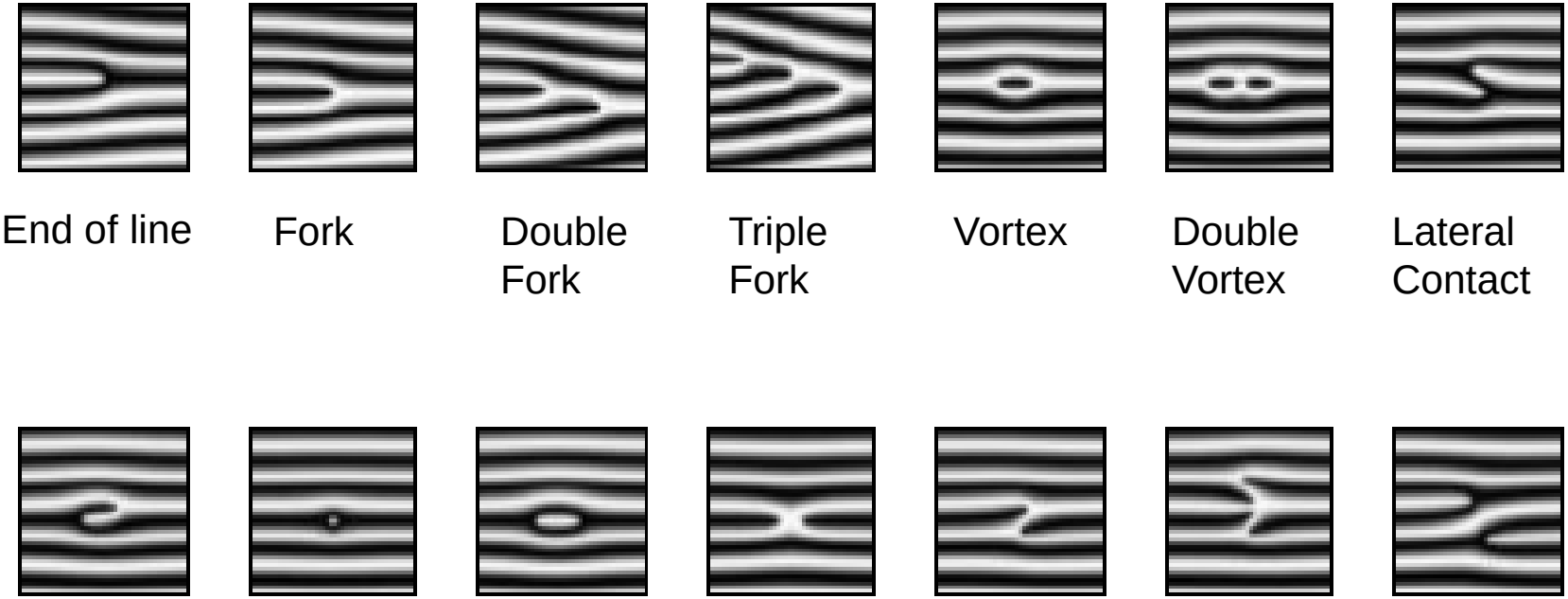
- Basics
- Fingerprint
- Iris scan
- Face recognition
- Hazards
- Discussion

Fingerprint: Operation (1)

- Sensor types
  - Optical
  - Capacitive
  - Thermal
  - Ultrasonic
  - Pressure
- Process
  - Minutiae
  - Pattern matching over the whole image
  - Follow the papilla segments
  - Position of sweat pores
- 20-30 Characteristics

Fingerprint: Operation (2)

- Minutiae



Source: BSI, „Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger“, öffentlicher Abschlussbericht

Fingerprint: Liveness Detection

- Measurement of the blood oxygen content by determination of the hemoglobin concentration ratios on the basis of the different absorption of different wavelengths of infrared light
- Pulse
- Electrical resistance of the skin
- Temperature
- Reflection properties in the ultrasonic range
- Blood flow

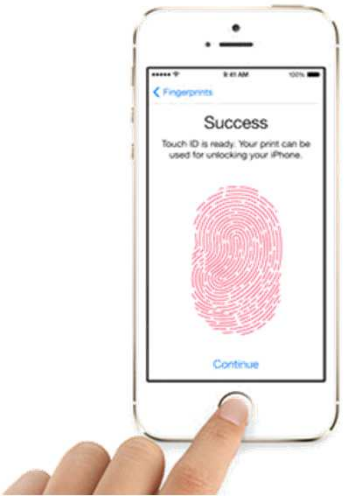
Fingerprint: Reader

Entrance door

Ultrasonic

capacitive

capacitive



optical

Fingerprint: Vulnerabilities (1)

- Latent image reactivation
  - Breathe on
  - Graphite powder
  - Color powder
- Use of latent images
  - Graphite powder and Tesa

- Build a fingerprint hardcopy
  - Gelatin
  - Wood glue
- Incorrect driver software
  - Access to passwords stored in the Windows registry
  - Preinstalled by leading notebook manufacturers

Fingerprint: Vulnerabilities (2)

- Video "Authentication to computer"

Source: Kopfball

Fingerprint: Advantages and Disadvantages

- Very well-researched methods
- High degree of uniqueness
- Cheap sensors
- Suitable for identification

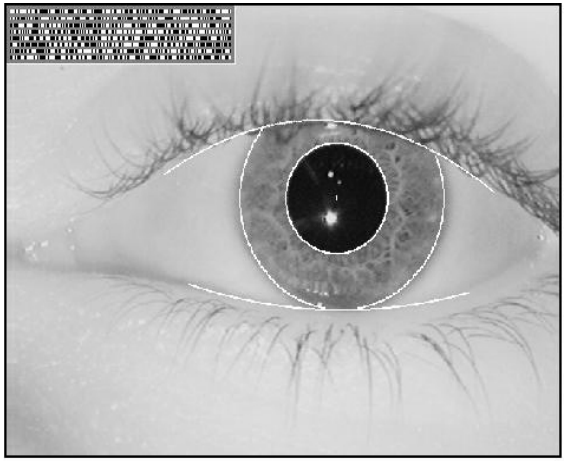
- Good Life recognition is relatively costly
- Hygienic concerns
- 5% of people have no really usable fingerprints
- Not tamper-proof

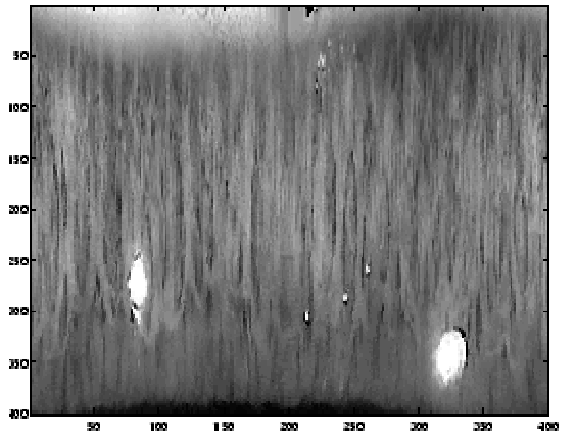
Agenda

- Basics
- Fingerprint
- Iris scan
- Face recognition
- Hazards
- Discussion

Iris Scanner: Operation (1)

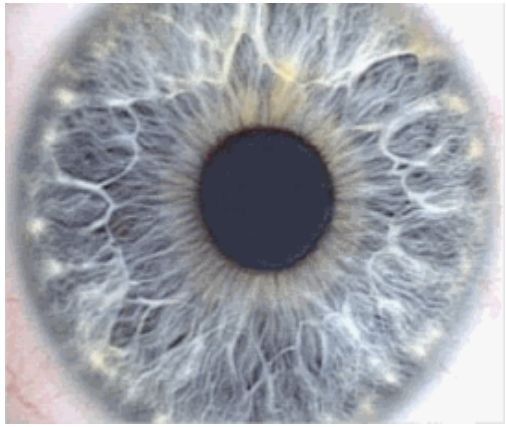
- Illuminating with infrared light
- Macro shot of the eye in the near infrared wavelength (680-850 nm)
- Photographic extraction of iris
- Dividing the iris in 8 circular cutouts
- Detection of remarkable patterns (Corona, crypts, fibers, stains, scars, radial furrows, stripes)
- Generation of iris code
  - Gabor Wavelet transformation
  - 244 measures
  - 512 bytes





Iris Scanner: Operation (2)

- One globally used algorithm
  - John Daugman, University of Cambridge
- Fast recognition
- Very good FAR and FRR
- Liveness detection
  - Irradiation and reflection
  - Pupillary reflex
- No detection of disease or drug use possible
- Iris indistinguishable after 25 years
  - According to Kevin Bowyer, the error rate changes after 2 years



Iris Scanner: Reader

Mobile phone

Computer access

Kiosk system

Building access

eGate

Iris Scanner: Vulnerabilities

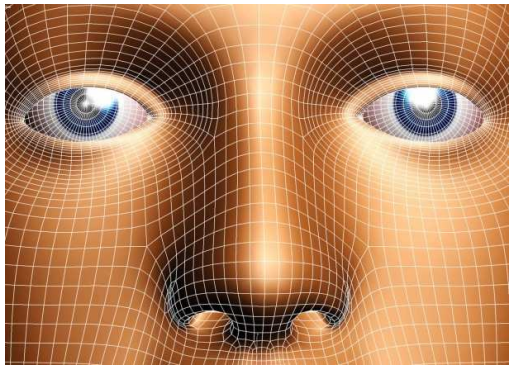
- Outwitting with photo or inkjet print
- Presentation of a video sequence
- Contact lens with printed or hand-painted iris
- Contact lens with iris hologram
- Hard to outwit if liveness detection is active

Iris Scanner: Advantages and Disadvantages

- High degree of uniqueness
- High temporal constancy
- Simple liveness detection by pupillary reflex
- Suitable for identification

- Change of characteristics due to illness
- Lighting, glasses, contact lenses
- Costs
- User acceptance
- User behaviour in front of active systems

Agenda

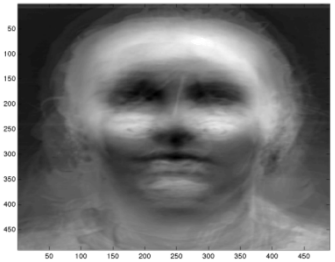


- Basics
- Fingerprint
- Iris scan
- Face recognition
- Hazards
- Discussion

Face recognition: Operation

- Based on characteristics
  - Extraction of individual characteristics
  - Classification based on these characteristics
  - Elastic Bunch Graph Matching
  - Detection using geometric characteristics

- Holistic approach
  - Observation of the entire face
  - Template Matching
  - Fourier transformation
  - Eigenface method

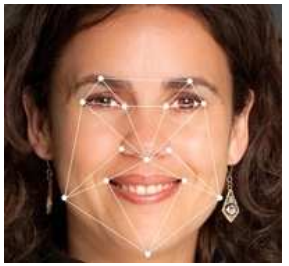


- Combination of the above methods

Source: Automatische Gesichtserkennung: Methoden und Anwendungen, Dominikus Baur, Universität München

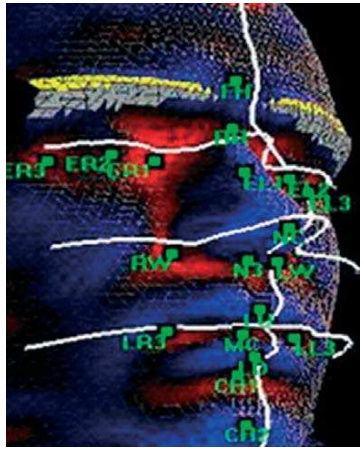
Face recognition

- Primarily used are features of the face that are not constantly changing due to the facial expressions
  - upper edges of the eye sockets
  - areas around the cheekbones
  - side panels of the mouth



- Normalization with the aid of prominent points on the face
  - e.g. nose, eyes, mouth, chin
  - Rotation
  - Translation
  - Scaling of the head

- 3D face recognition
  - Stripe projection
  - Systems available since 2010



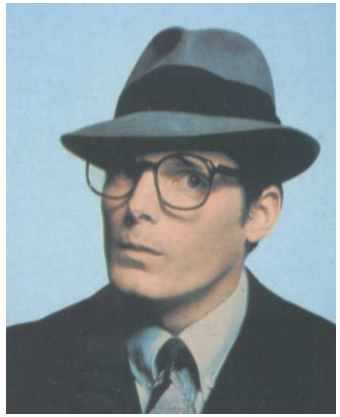
Source: Interflex

- Interoperability according to ISO/IEC 19794-5

- Todays FRR of 1 % is acceptable
  - Poor 79% in 1993

Face recognition: Vulnerabilities

- Disguise
  - Makeup artist
  - Sunglasses
  - Glasses
- Photo
- Video sequence
- Artificial head



- Poor lightning
- „Grimaces“

Face recognition: Advantages and disadvantages

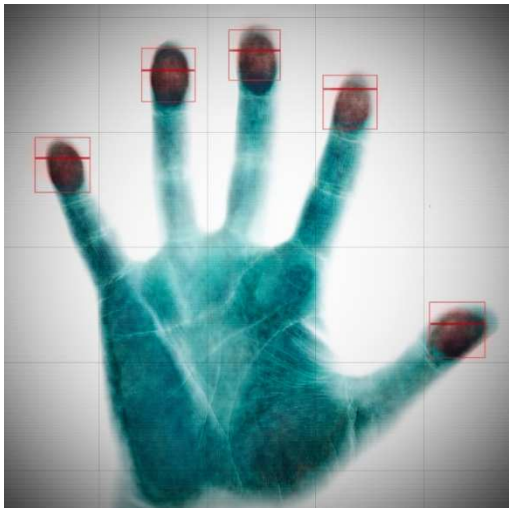
- High usability
- High user acceptance
- Face is always (at least partially) visible
- Can be generated and reviewed without notice

- Low relative constancy
- Low uniqueness
- No cooperation necessary
- Can be generated and reviewed without notice

Comparison of Technologies

Item	Fingerprint	Iris Scan	Face Recognition
Uniqueness	?	10e-78	?
FAR	0,01 - 0,2 % 1:10.000-1:500	0,0001 % 1:1.000.000	0,1 % 1:1000
FRR	0,1 - 5 %	1 %	1 % (1993: 79%)
Characteristics	25	244	22
Acceptance	-	- -	+ +

Agenda



- Basics
- Fingerprint
- Iris scan
- Face recognition
- Hazards
- Discussion

Fiktion ?

- Video "Fingerprint as evidence"

Hazards (1)

- Loss of a biometric characteristic
- Fingerprint
  - Security
  - Unique
  - Not tamper-proof
  - Burden of proof
  - Forensic consequences
  - Legal consequences

Ein Tatrichter, der seine Überzeugung von der Täterschaft des Beschuldigten auf das Beweisanzeichen der an den Tatorten festgestellten und nach den wissenschaftlichen Grundsätzen der sogenannten Daktyloskopie sorgfältig ausgewerteten Fingerabdrücke des Täters stützt, begeht damit keinen Verstoß gegen Rechtsnormen des Strafrechtes oder gegen allgemeine Erfahrungssätze der Wissenschaft

- Faith in technology
  - Fingerprint of Wolfgang Schäuble
  - Murders deposit foreign DNA at the crime scene (study)

Hazards (2)

- Video "Shopping with fingerprint"

- „ Economics of Crime“

FAR = 0,002
N = 200, P(N) = 32%
N = 2000, P(N) = 98%
N = 10000, P(N) = 99.999%

Source: Planetopia 25.1.2009

ePass (1)

- Stored in optically machine readable zone
  - Given names and surname
  - Issuing state
  - Pass number
  - Gender
  - Date of birth
  - Expiration date

- Stored in the contactless chip of the passport
  - Photo
  - Two fingerprints as compressed images
- No storage at registry offices
  - Different from the proposal of former German Interior Minister Otto Schily

ePass (2)

- The exact usage and storage of the data read out at boundaries is unclear
- Unencrypted wireless transfer of data
- Wireless chips allow unnoticed monitoring and tracking of individuals
- Increase in counterfeit security could be realized even without storage of personal data
- A Study of the BSI showed the immaturity of the technology in biometrics in everyday life
  - Rejection rate of 3 to 23 percent
  - Separate examination of rejected people
  - Unsustainable staffing overhead

ePass (3)

- Left Party criticized biometrics strategy of the Federal Government

  According to the Left Party in the Bundestag, the Federal Government has acknowledged that biometric methods can be at best used as secondary early detection of suspected terrorists (13.01.2009)

- EU Parliament agrees on a compromise proposal for biometric passports

  The European Court of Human Rights has set a limit on the national governments with his decision against the British government (Marper vs. UK) recently. Therein, the ECJ declared the storage of DNA data and fingerprints are disproportionate and incompatible with Article 8 of the European Convention on Human Rights. Any national laws to biometric databases would find here their EU legal limit (15.1.2009)

Source: www.heise.de

Strange (1)

- Cat Stevens
  - If a file ends up times ...
- Phantom of Heilbronn
  - 40 Crime scenes with identical DNA traces
  - “Different DNA results of 'acquaintances female person' (UWP) in relation to facts that were not plausible from a criminological perspective“
  - Contamination of cotton swabs used for receiving samples of DNA by an employee

- Biometric face recognition for laptops hacked
  - The system has been tricked with a photo of a registered user
  - With fake facial images by generating a large number of images
  - Security experts required the laptop manufacturers to remove biometric authentication from the devices and to warn all users before using the function

Strange (2)


Wieso?
Weshalb?
Warum?
Wir entdecken unseren Körper
Knochen sind das Gerüst unseres Körpers.
... und von dir.
Nur Zwillinge sehen sich zum Verwechseln ähnlich. Oft haben sie sogar die gleiche Art zu sprechen und sich zu bewegen.
Ferse
ANNA
TIBO
HELEN
Kein Mensch auf der Welt hat genau die gleichen Fingerabdrücke wie du. Wie sieht dein Daumenabdruck aus?

Wish List

Wikileaks 30.11.2010

- US Secretary of State Hillary Clinton is said to have given their ambassadors in July 2009 secret directives ... to collect biometric data of important UN officials.
- On Clinton's wish list were amongst others passwords and encryption keys used by high-level UN staff for official communication, as well as credit card and frequent flyer numbers.
- Moreover, US diplomats in the DRC, Uganda, Rwanda and Burundi should even collect fingerprints, DNA samples and iris scans of specific target persons from UN circles.

Source: www.heise.de

FBI Biometric Database (1)

FBI takes largest biometrics database piecemeal in operation (25.3.2011)

- The "Next Generation Identification" system have reached the first phase of "operational usability".
- Replaces the Integrated Automated Fingerprint Identification System (AFIS) of the US Police.
- The system is initially fed with fingerprints.
- Later to be captured are iris scans, voice samples, pictures of handprints, tattoos, scars and facial shapes.

Source: www.heise.de

FBI Biometric Database (2)

FBI provides biometric database completed (16.9.2014)

- With Rap Back, authorized sites may automatically receive updates about conflicts of staff with the law. This would include employees who are dependent in their work on trust, such as teachers.
- In addition, national prosecutors can now access the facial recognition system IPS (Interstate Photo System).
- The FBI said that the images of suspects are compared only with photos of convicted criminals.
- Internal information suggested that other photos may be used, such as shots of crowds or Facebook photos.
- The face recognition system has been criticized massively by civil rights activists.

Source: www.heise.de

FBI Biometric Database (3)

- In the FBI office in Clarksburg in the State of Virginia on average around 168,000 fingerprints are being daily analyzed and identified.
- In future, the system should enable 18,000 law enforcement agencies around the clock an automated search for fingerprints, a real-time matching and associated information exchange. Investigators on site will in future be equipped with handheld scanners.
- The Department of Homeland Security (DHS) has in parallel built a private system for fingerprinting and iris scans of travelers entering the United States at airports.
- For the US civil rights activist Barry Steinhardt of the data protection organization Privacy International, there is no question that biometric systems are an important component of future government surveillance projects. He warns that an "Always on" – surveillance society will be possible due to reconcile abilities. The Californian futurologist Paul Saffo warns in this context against that biometric features, unlike some credit card numbers, clang to an individual for it’s life. Errors in government databases could therefore have serious consequences.

Source: www.heise.de

FBI Biometric Database (4)

FBI massively extends their biometric database (22.9.2015)

- Storage of job applicant's fingerprints that employers must send to the FBI for a background check in many professions.
  - Engineers, doctors, brokers, stockbrokers, lawyers, or architects
- Employers and other authorities can additionally send facial images to the FBI.
- The EFF is concerned that these are then used to track the movement of people between different locations.
- According to EFF, confusion with the physical characteristics resulted in innocent persons migrating to jail.

Source: www.heise.de

EU-Project E-Border Control

EU-Project: Federal police testing e-border control with ten fingerprints (17.3.2015)

- Frankfurt airport runs a trial where up to ten fingerprints are taken from volunteers.
- The German MP Andrej Hunko called on "to avoid absolutely" the tests because they paved the way for a "huge border police data retention of travel profiles".
- The Left Party called the entire package of "smart borders" a "stimulus plan for the defense and biometrics industry."
- It was actually launched to control migrants who overdraw their visa.
- However, the Federal Government sees the high level of investment justified only if police authorities have access to the collected facial and fingerprint data and could monitor travelers in general more intensively.

Source: www.heise.de

Voluntary

Léon de los Aldamas, Central Mexico (31.10.2010)

- Global Rainmakers Iris-Scanner "HBox"
- Recognizes up to 50 moving persons per minute.
- Offenders are automatically recorded in an iris database.
- Innocent citizens can register voluntarily.
  - Global Rainmakers promises a number of benefits.
  - Pay by iris scan – the system just looks into a customer's eye, identifies him, and debits money from his bank account.
  - Passports or train tickets will become obsolete in the long term.
- „In the future, everything you want to open - one's own house, the car, the door to the office – will be accessible with a single key: the iris“ (Jeff Carter, CEO of the biometrics company).
- „At a certain point, it is striking to refuse than to participate. Everyone will participate.“
- „In ten years every person, every place, and every object will be linked”.

Source: www.heise.de, Die Welt

Tourists pay by fingerprint

Japan (14.2.2016)

- Foreign tourists will be able to pay by fingerprint soon.
- Tourists need to register their fingerprint at the airport as well as store additional data, e.g. credit card accounts.
- Until the 2020 Olympic Games in Tokyo, the system is supposed to work nationwide.
- Data collected when using the system will be made anonymous and managed by a panel under administrative management.
- Because the data allow a deep insight into the spending habits of visitors, it is expected to be used for the domestic tourism industry too.

Source: www.heise.de,

Wrong Analysis (1)

Deadly temptation at FBI (19.4.2012)

- Since the 90s, the US government had knowledge of significant sources of error in the investigation laboratories of the FBI.
- Blatant errors in the analysis of hair samples and skin residues in murder and homicide cases.
- The results in 2004 were passed neither to wrongly imprisoned inmates which have been imprisoned for years not to their attorneys.
- Only the prosecutors involved were informed. They retained the partly exculpatory evidence largely for themselves.
- Hundreds of cases of miscarriages of justice and unjustified penalties
- Wrongly convicted persons were not rehabilitated.
- The Justice Department is refusing to publish the names of those people.

Source: http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html

Wrong Analysis (2)

- The 17-year Santae Tribble was convicted of capital murder, although several witnesses testified under oath that Tribble was with them at the time of the crime.
- The core of the argument of the prosecutor were hair samples that were assigned to Tribble.
- As it turned out at the internal audits, the FBI evidence objects in truth have been dog's hair.
- A forensic scientist has apparently committed multiple fatal errors especially in hair analysis.
- "FBI experts repeatedly "came to unscientific conclusions" that were a great disadvantage for the accused."
  - Bombing of Oklahoma 1995
  - Murder trial against the former football star O.J. Simpson
  - First attacks to the World Trade Center in New York 1993

Source: http://www.derwesten.de/panorama/hunderte-justizirrtuemer-toedliche-vertuschung-beim-fbi-id6569273.html

Last but not least

Quote of an online publication

„As biometric data can not be modified or passed on to other people, an extremely high security against forgery is given.“

Conclusion

- Biometric systems can increase security
- Prerequisite is an exemplary implementation
- Biometric systems can be bypassed
- Saved biometric data arouse desires
- Strength of evidence be challenged legally

„We are not only responsible for what we do but also for what we do not"

(Voltaire)

Many Thanks!