Biometrische Verfahren und automatisierte Gesichtserkennung

#### **Christoph Busch**

more information at: https://christoph-busch.de latest news at: https://twitter.com/busch\_christoph video at: https://www.youtube.com/watch?v=9\_WT\_aTdILw

HAWtech on September 22, 2021







# **Biometric Characteristic**

#### **Biometric activities**

- Lecturer in Darmstadt, Gjøvik and Copenhagen
- Convener of the Working Group 3 on Biometric Data Interchange Formats in ISO/IEC JTC1 SC37
- Board-member European Association for Biometrics
- Chair of the TeleTrusT working group on Biometrics
- Co-Chair of the Norsk Biometri Forum

#### Recent projects related to Biometrics

- Hochschule Darmstadt:
  - HWMK/BMBF ATHENE https://ngbs.athene-center.de/
  - BSI DIRECT-PAD
  - EU H2020 iMARS, TReSPAsS
- NorwegianBiometricsLab@NTNU:
  - EU H2020 iMARS https://imars-project.eu/
  - eu-LISA https://christoph-busch.de/projects-euLISA
  - IKTPLUSS SWAN https://www.ntnu.edu/iik/swan





## **Access Control**

Authentication can be achieved by:

- Something you know: Password, PIN, other secret
- Something you own: SmartCard, USB-token, key
- Something you are: Body characteristics

Something you know or own you may loose, forget or forward to someone else, with biometrics this is more difficult.



# Definition

• International Organization for Standardization defines:

Biometrics:

"automated recognition of individuals based on their behavioural and biological characteristics"

Remark: behavioural has to do with the function of the body biological / anatomical has to do with the structure of the body



# Landmark Oriented Approach

#### Landmarks represent essential properties

- Detection of geometric landmarks
- Features
  - Relationship between Length of Nose versus Eye basis
  - Additional features at landmark positions

Combination and processing of local texture features in one hand-crafted feature vector



[King2009] D. E. King. "Dlib-ml: A Machine Learning Toolkit." In: Journal Machine Learning, (2009)

Biometrische Verfahren

# Border Control in Frankfurt - EasyPASS

#### Automated but supervised Control

Survey by control personnel

Project goals:

- Proof of Concept "Self-Service to increase throughput"
- **Operation started 2009** 
  - Procedure for travellers
    - No registration needed
    - Use of ePassport/Face
    - Limited for EU/Schengen-Citizen (18+ years old)



Source: BSI

# **Presentation Attack Detection**

#### Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- making appearance similar to the reference
- artefact presentation



https://www.youtube.com/watch?v=9\_WT\_aTdlLw

### Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose



evade face detection



Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

# What is Morphing?

In our real world morphing can become a threat

- with a criminal and an accomplice as actors
- take the criminal
- and the accomplice
- morphing can transform one face image into the other
- and you can stop half way in the transformation



**Biometrische Verfahren** 

# **Problem: Morphing Attacks**

#### Is it a really problem ? - YES!

- In September 2018 German activists
  - used a morphed images of Federica Mogherini (High representative of the European Union for Foreign Affairs and Security Policy) and a member of their group
  - and received an authentic German passport.





Image source: https://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html

Biometrische Verfahren

# **NIST-FRVT-MORPH**

### NIST IR 8292 report presented September, 2021

### FRVT-MORPH

https://pages.nist.gov/frvt/html/frvt\_morph.html

- results for MAD algorithms from four research labs:
  - Hochschule Darmstadt (HDA)
  - Norwegian University of Science and Technology (NTNU
  - University of Bologna (UBO)
  - University of Twente (UTW)

#### **NISTIR 8292 DRAFT SUPPLEMENT**

Face Recognition Vendor Test (FRVT) Part 4: MORPH - Performance of Automated Face Morph Detection

> Mei Ngan Patrick Grother Kayee Hanaoka Jason Kuo Information Access Division Information Technology Laboratory

This publication is available free of charge from: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing



# **NIST-FRVT-MORPH**

### NIST IR 8292 report presented September, 2021

- Performance of Automated Face Morph Detection https://pages.nist.gov/frvt/reports/morph/frvt\_morph\_report.pdf
- results for high quality morphs versus print and scanned
  - note the low number of print and scanned images



Christoph Busch

# **Makeup Presentation Attacks**

#### Severe alterations

- Makeup for impersonation
- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply



[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Detection of Makeup Presentation Attacks based on Deep Face Representations", in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020)

# **Demographic Effects**

#### Algorithm bias in the media

- Movie Coded Bias
- Press information

Nov 4, 2020, 08:10am EST | 621 views

#### Biometrics Aren't Inherently Biased — We're Training Them Wrong



Stephen Ritter Forbes Councils Member Forbes Technology Council

> Machines learn that Brussels writes the rules: The EU's new AI regulation Mark MacCarthy and Kenneth Propp - Tuesday, May 4, 2021

Gende



ECHTANK

Editor's Note: This post originally appeared on the Lawfare blog.

he European Union's <u>a proposed</u> artificial intelligence (AI) regulation, released on April 21, is a direct challenge to Silicon Valley's common view that law should leave emerging technology alone. The proposal sets out a nuanced regulatory structure that bans some uses of AI, heavily regulates high-risk uses and lightly regulates less risky AI systems.

### WEAPONS OF Math Destruction



HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY



#### Biometrische Verfahren

TECHTANK

## Contact

