Biometrics
Face recognition

PV181 Laboratory of security and applied cryptography
Seminar 29. 12. 2023

Agáta Kružíková, kruzikova@mail.muni.cz
Katarína Galanská, galanska@mail.muni.cz

CROCS
Centre for Research on Cryptography and Security

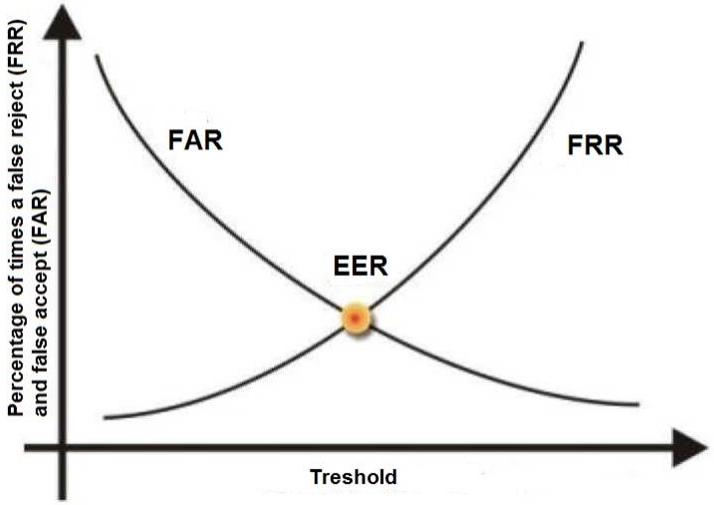
Lecture structure

1. Lecture
   - Face recognition theory
   - Practical examples
   - Selected attacks
2. Seminar activity
   - SWOT analysis
3. Homework
   - Face detection

Biometrics – introduction

- Authentication based on:
  - something I know (e.g. password)
  - something I have (e.g. access card)
  - **something I am (e.g. fingerprint)**

- Never 100% match
  - FAR (false acceptance rate)
  - FRR (false rejection rate)



Face recognition

Theory and examples

Project Citizen K.

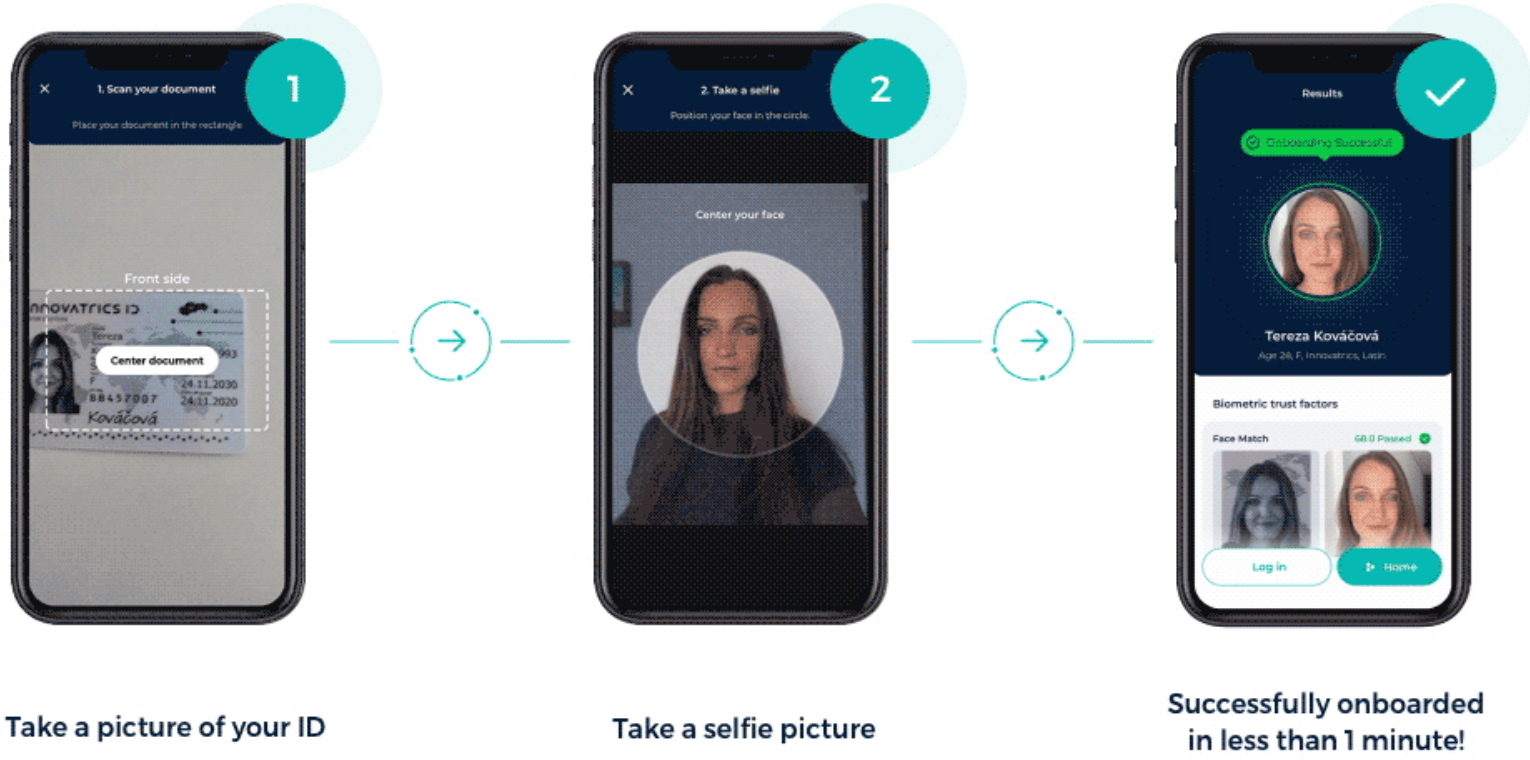
- 2010 “art” project by ZTOHOVEN
- 12 people had their Czech ID cards re-issued with morphed photographs
  - Similar haircut & style
  - Photos 50% themselves, 50% someone else
  - In 2010 you brought your own photo for the ID card

- Using someone else's identity for several months
  - Wedding, gun licence, pilot licence, bank operations, out-of-Schengen travel, elections, ...

PS: Czech documentary can be legally streamed for 60 Kč

Used for smartphone unlocking

Bank registration



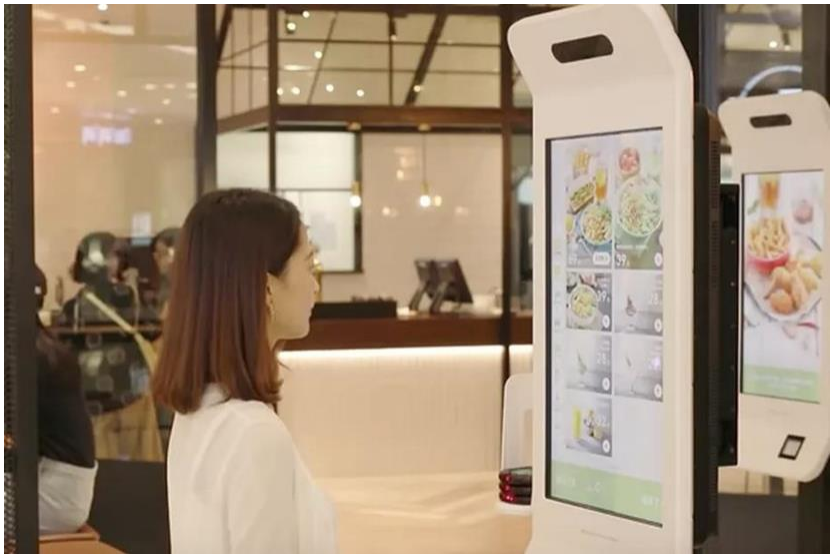
Take a picture of your ID

Take a selfie picture

Successfully onboarded in less than 1 minute!

Source: https://developers-old.innovatrics.com/digital-onboarding/docs/use-cases/onboarding/

KFC AliPay

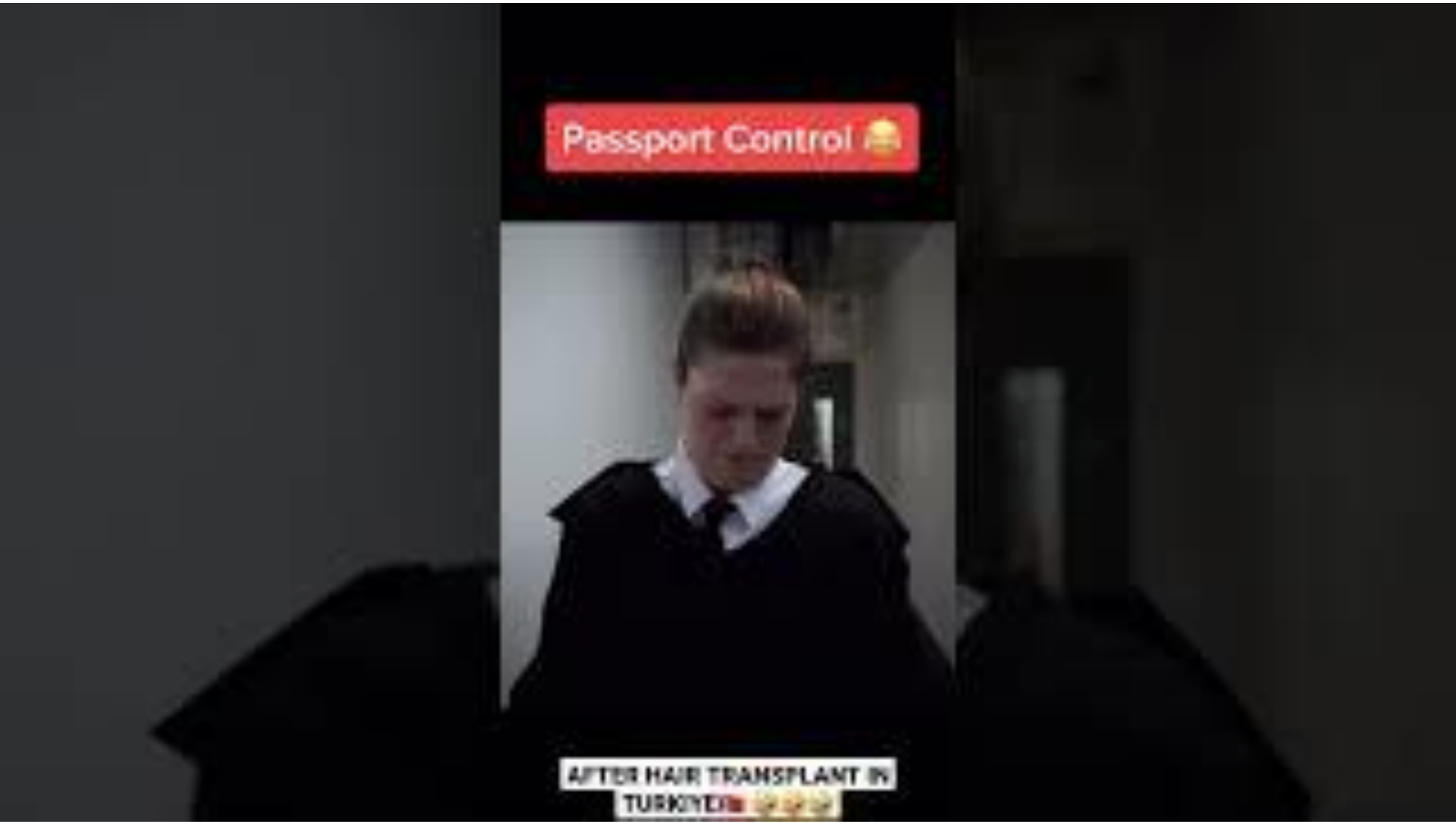


- Introduced 2015
- Only one KFC in China
- Liveness detection
  - 3D camera
- 2017: login in Alibaba services
- See AliPay promo video at https://www.theverge.com/2017/9/4/16251304/kfc-china-alipay-ant-financial-smile-to-pay

Biometric passports

- “Smart card”, contain NFC chip
- Two security levels:
  - BAC: Reading your photo+personal information (Try Android app Passport reader)
  - EAC: Reading your biometrics
    - Fingerprint, Face and Iris support

Passport control?


Passport Control
AFTER HAIR TRANSPLANT IN

Automatic passport control

The future of travel

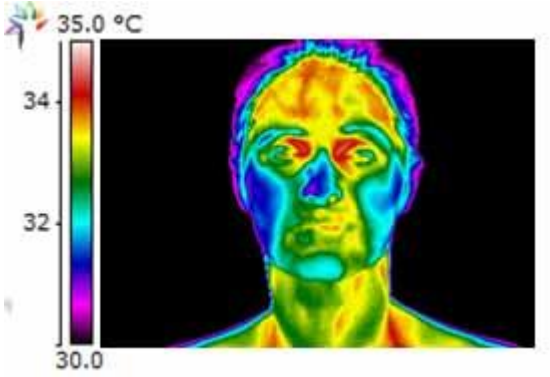
This world-class airport will soon go passport-free

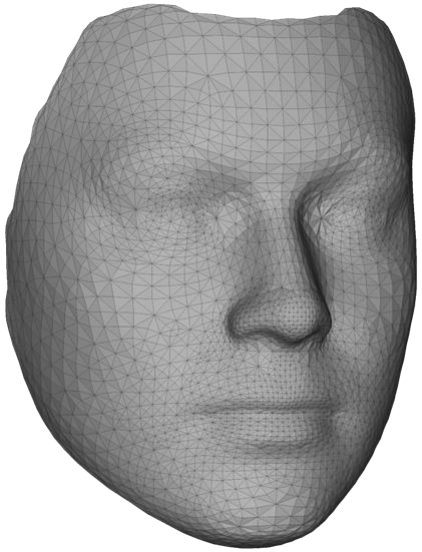
By Heather Chen, CNN

3 minute read · Published 3:24 AM EDT, Wed September 20, 2023

Face recognition – Input

- Single picture
- Video sequence
- 3D image
- Facial thermograms



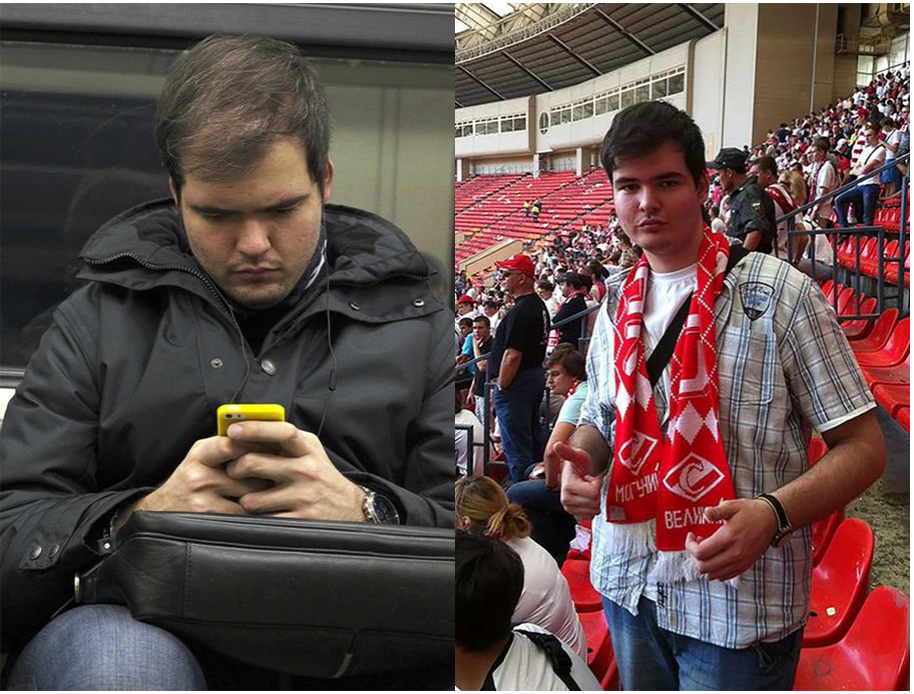


Face recognition: The automatic way

- Statistical
  - Eigenface, PCA, LDA, ...
- Neural networks
  - Microsoft: Face API
  - Facebook: DeepFace
  - VK: FindFace *(“best results” in MegaFace comp.)*
  - Google: FaceNet

FindFace – example

Subway photo (left), social network photo (right)



Face recognition overview (OpenFace)

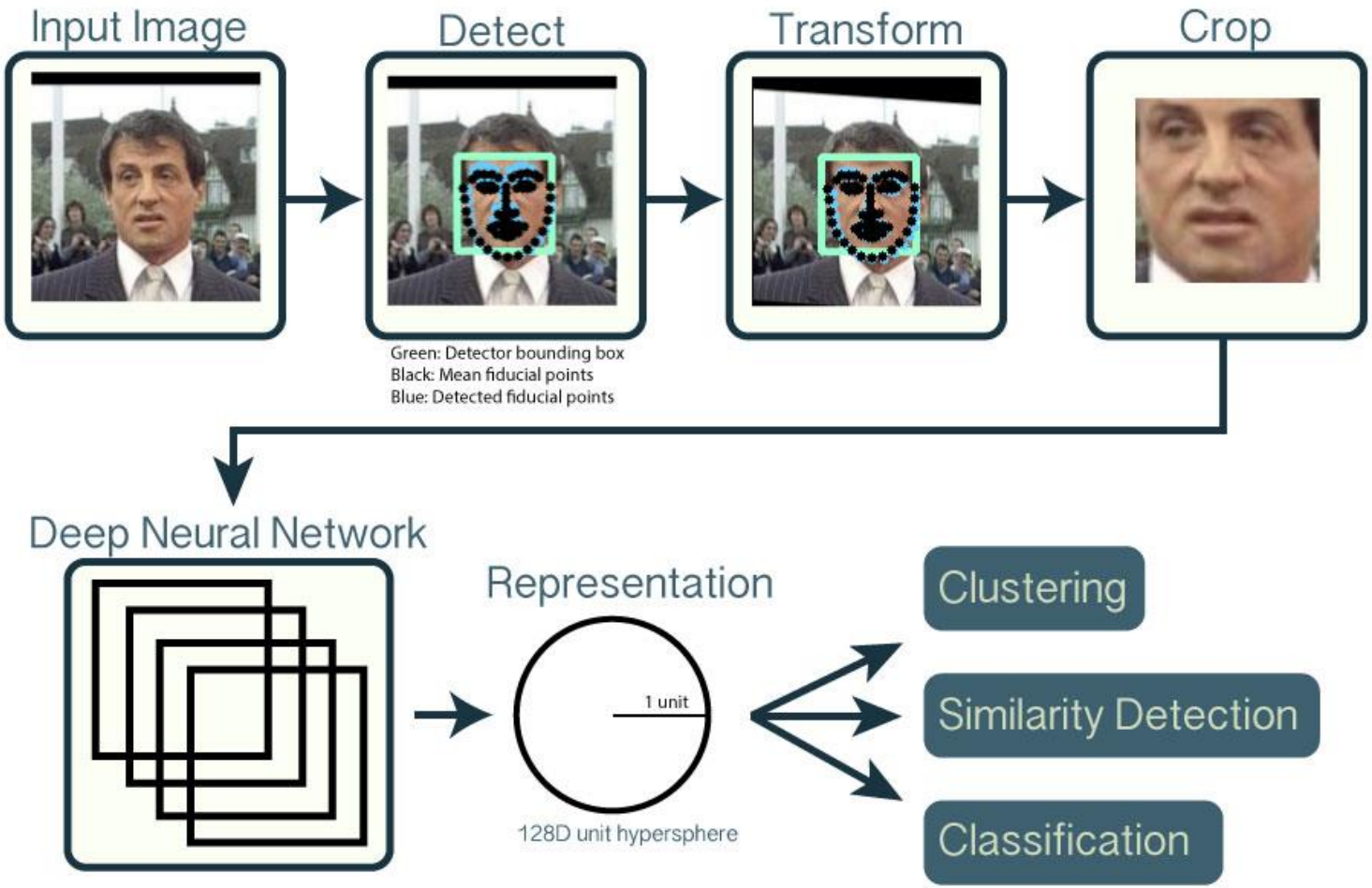
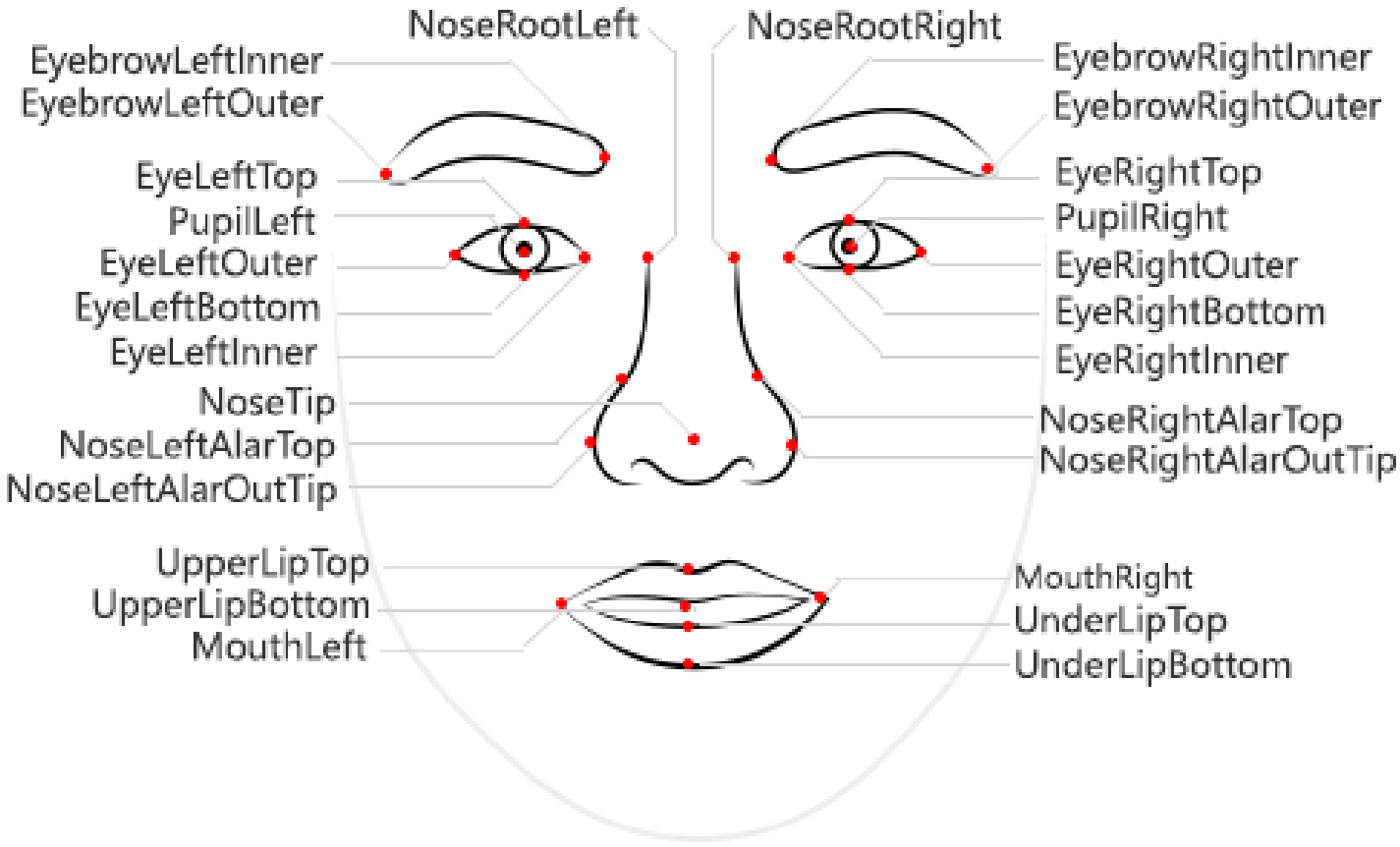


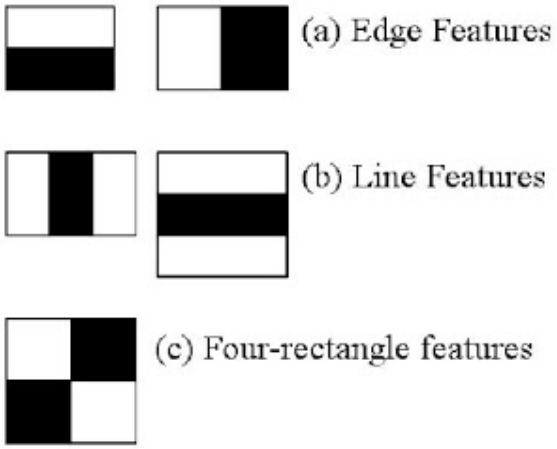
Photo © The OpenFace project, cmusatyalab.github.io/openface

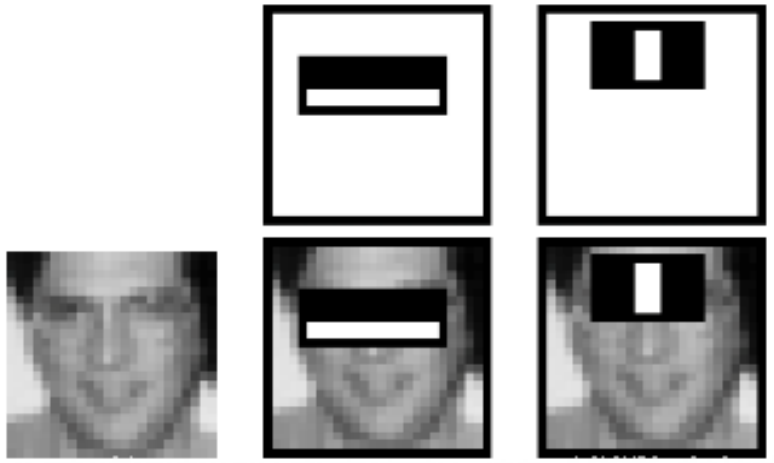
Microsoft: Face API



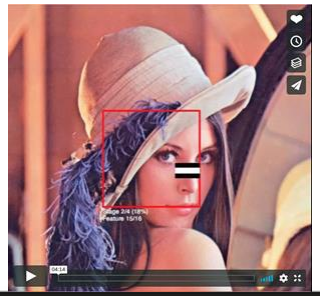
Face detection: Haar cascades

- Machine learning based approach based on comparing pixel intensities in adjacent regions





- *Face Detection: Visualized*
  https://vimeo.com/12774628



Challenges in face recognition

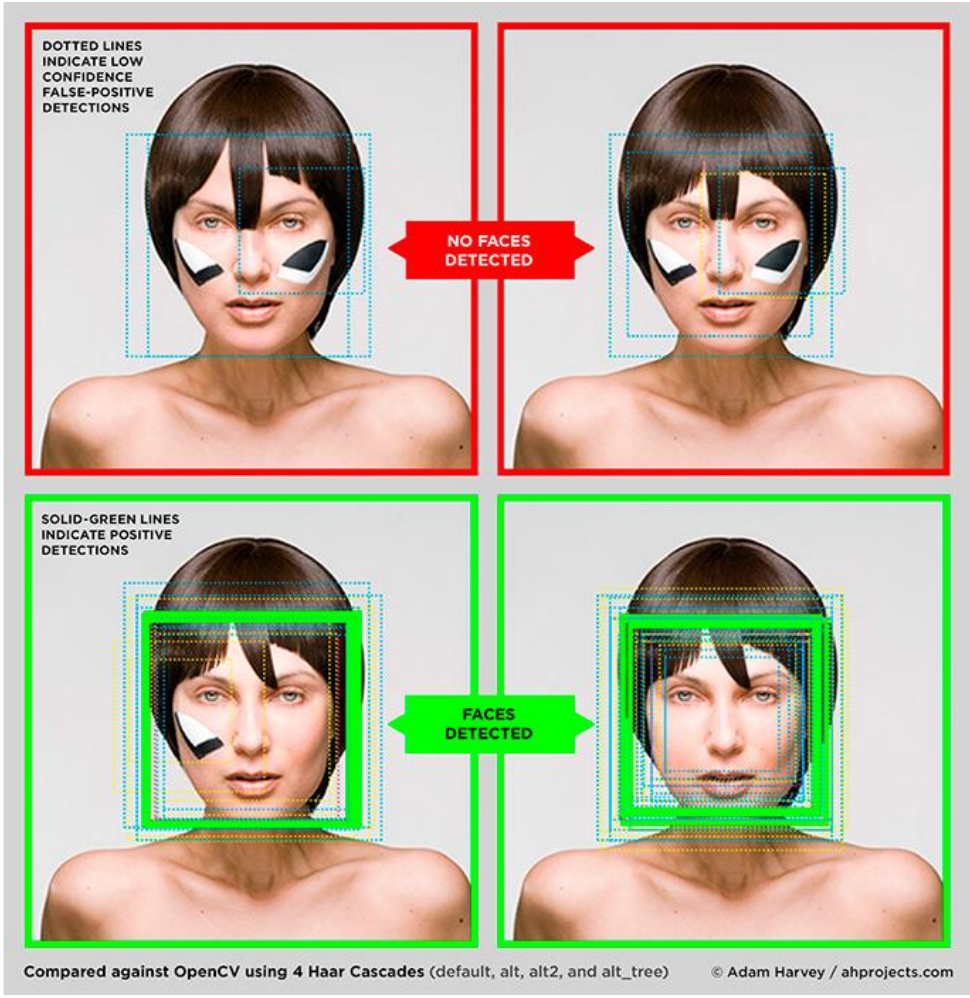
- Illumination
- Pose
- Environment
  - Noisy background
- Aging
- Feature occlusion
  - Hats, glasses, hair, ...
- Image quality
  - colour, resolution, ...

Covid challenge in face recognition...

- NIST study on the effects of face masks
  - Error rates 5–50% on face masks
  - Nose and mask color matter
- NtechLab: “Even balaclava is OK.”
  - Focus (even more) on eyes

CV Dazzle: Anti face-detection

Photo © 2010-2016 Adam Harvey, CV Dazzle



CV Dazzle: Anti face-detection

Photo © 2010-2016 Adam Harvey, CV Dazzle

Face impersonation

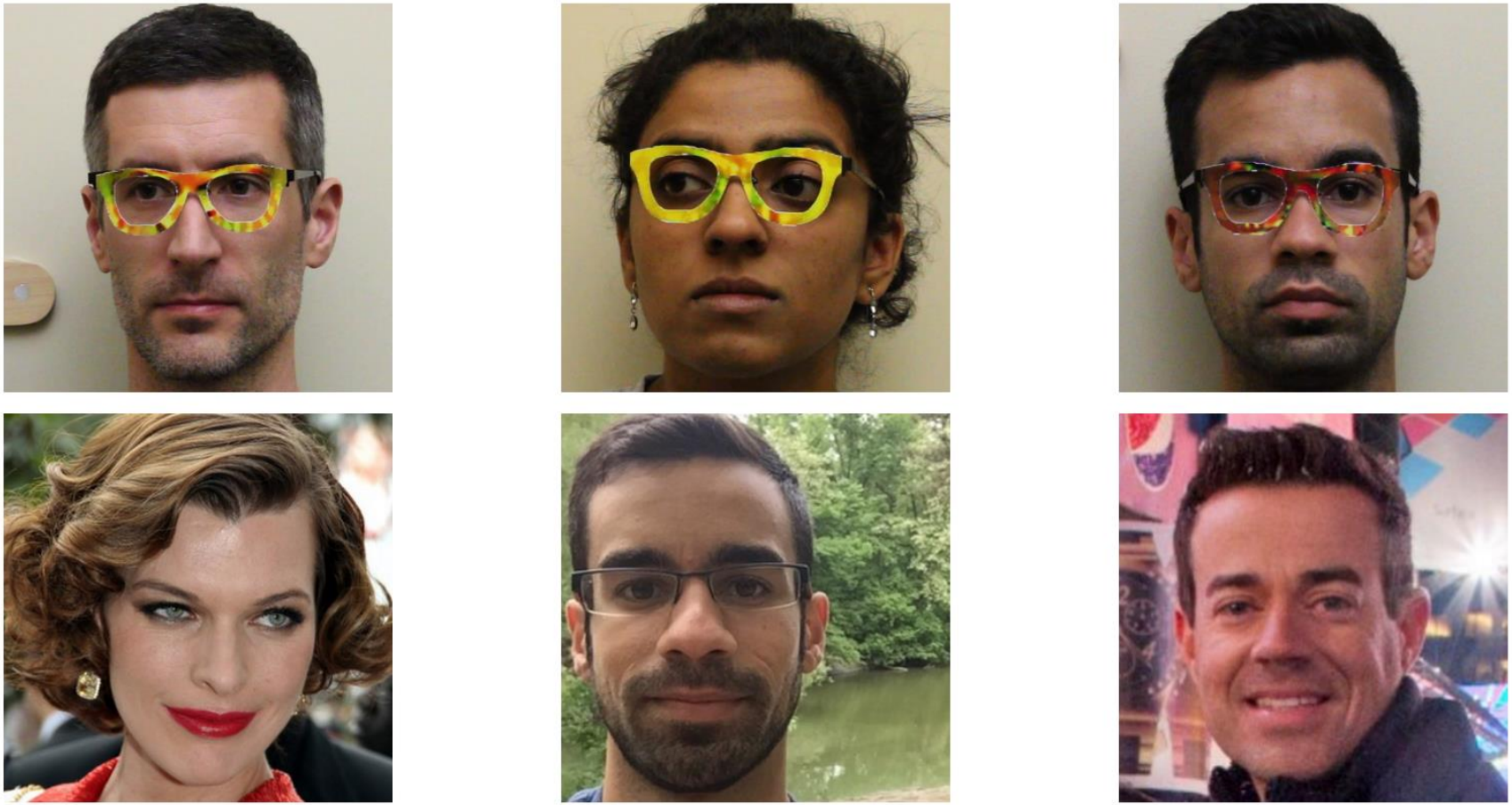


Photo © 2016 Carnegie Mellon University, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*

Face impersonation

- Fooling deep-neural-networks-based face recognition systems (e.g. Face++)
  - Over 90% success rate
  - The principle is more general
- *"physically realizable and inconspicuous"*

Sharif, Mahmood, et al. "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.

Liveness detection

- Protection against: spoofs (digital replicas), photos, videos, masks (physical replicas)
- Liveness detection:
  - AI in real time
  - Passive
    - E.g., eye movements, skin structure
  - Active
    - User asked to do something
- Combination of liveness checks

Liveness Detection in Face Recognition: Evolution of Biometrics

Liveness detection: other resources

Facia Unveils How It Will Defend Against $24B Identity Thefts: From Paper Masks to Deepfakes

Can I unlock it with my photo? Face ID vs Windows Hello vs Samsung Facial Recognition

iPhone X Review: Testing (and Tricking) FaceID

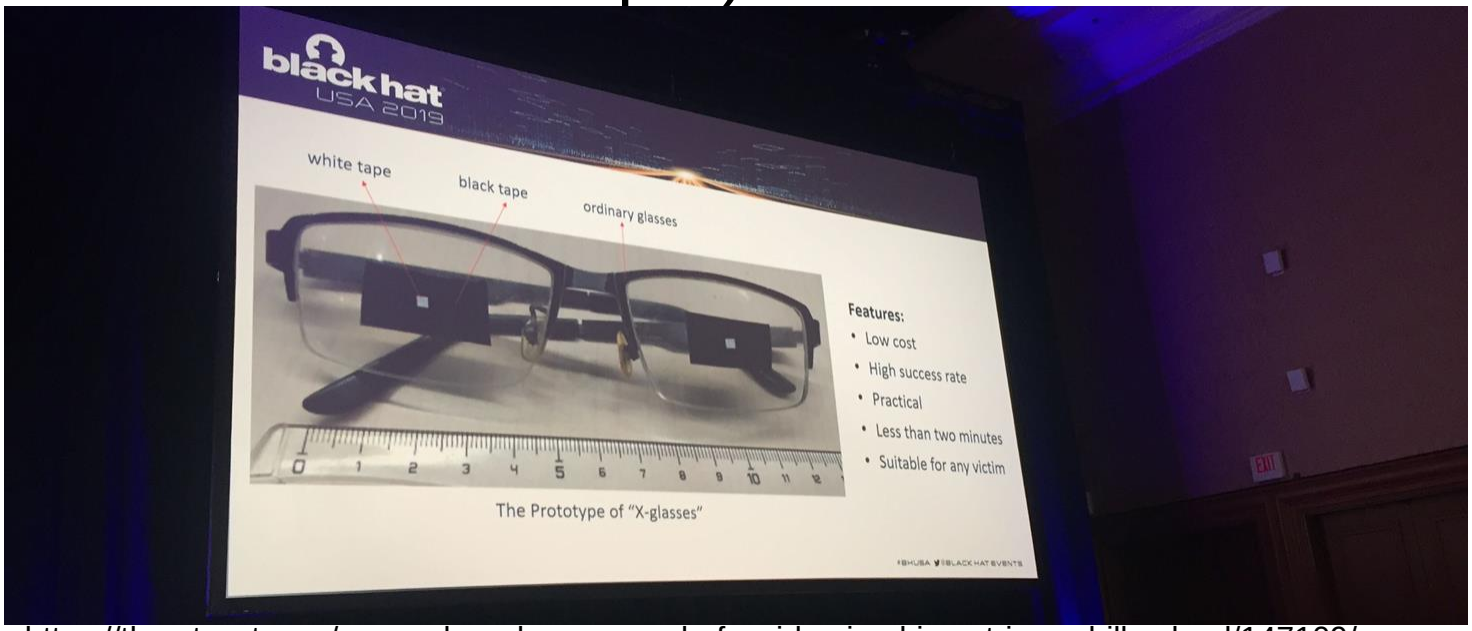
iPhone X Face ID fooled with mask, claims hackers

https://support.apple.com/en-us/102381

E. Lavens, D. Preuveneers, and W. Joosen. 2023. Mitigating undesired interactions between liveness detection components in biometric authentication. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). ACM, New York, NY, USA, Article 141, 1–8. https://doi.org/10.1145/3600160.3604992

Apple FaceID hacked

- Liveness detection feature hacked in 2019
- Researchers used a pair of modified glasses
- A victim has to sleep :-)



Soucce: https://threatpost.com/researchers-bypass-apple-faceid-using-biometrics-achilles-heel/147109/

Face recognition

Privacy issues

Detecting sexual orientation from faces

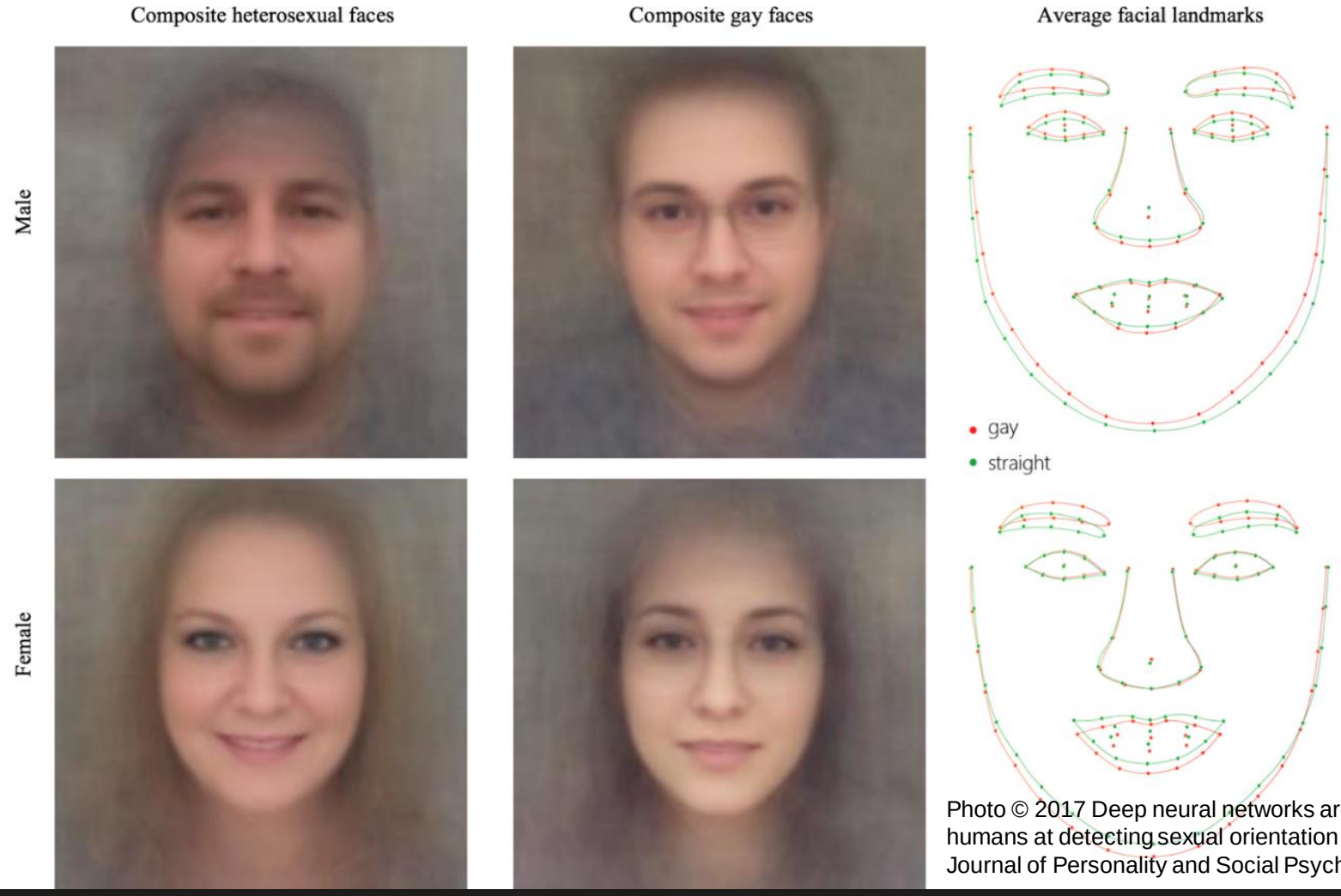


Photo © 2017 Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology

Detecting sexual orientation from faces

- Classifying sexual orientation (straight vs. gay) on men/women photos
  - Human success: 61% / 54%
  - Neural networks: 81% / 71%
  - Neural networks (5 images): 91% / 83%
- May be a privacy issue!

Wang, Y., & Kosinski, M. (in press). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 2017.

Mugshots

BUDDSJD_10

CAUGHMANMD_3

CLYMANNS_1

DELAROSAJ_2

CHEWEYSR_22

CLARKJ_6

DELOACHAM_1

GILLEYNK_1

Face recognition ban in San Francisco

- *"Threat to civil liberties"*
  - Ban for government agencies (city police and sheriff)
  - Federal agencies not affected
- Reason: discrimination, privacy issues
  - Less accurate at people of colour!
- Suppliers see it as a step back
- See more at www.banfacialrecognition.com

Gregory Barber, *San Francisco Bans Agency Use of Facial-Recognition Tech*. 2019, Wired.

Ethical use of technology?

Code of Ethics (ACM)

1. Society and human well-being
2. No harm for participants & risk analysis
3. Honesty (transparency)
4. No plagiarism
5. Respect privacy
6. Confidentiality
7. High quality & standards (competence)
8. Professional review
9. Inform society

ACM Code of Ethics and Professional Conduct., Online [2019]: acm.org/code-of-ethics

Detour: SWOT analysis

- A.k.a. “SWOT matrix”
- From 1960s
- Strategic planning technique related to business competition or project planning
- Widely applicable

SWOT example: Passwords

Strengths

- Well understood
- Legacy
- Intuitive usage
- Possibility of high entropy

Weaknesses

- Often low entropy
- Infinite ways to implement
- Policy differences
- Sticky note syndrome
- Threats related to storage

Opportunities

- FIDO 2.0 system
- Integration of OPT and Push-to-Approve

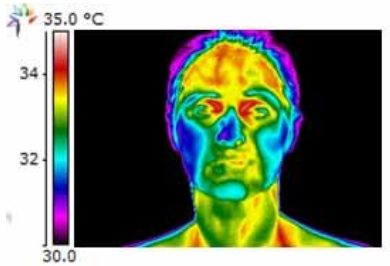
Threats

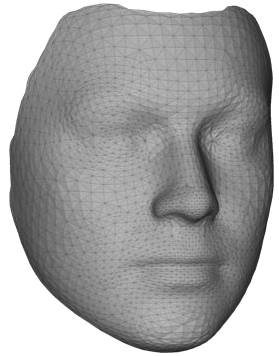
- Bad attack understanding
- Long tail of replacement
- Usability issues
- The dark web

Example inspired by the RSAC 2018 talk *Passwords and fingerprints and faces – Oh my! Comparing old and new authentication* by Jackson Shaw

Seminar task

- Do a SWOT analysis for a use case on face recognition biometrics, work in groups of three
- Use cases:
  a. Face authentication
     on border crossing (passports)
  b. “Pay by a smile”
     for Internet card payments
  c. 3D face authentication
     for accessing bank vaults
  d. Thermal face scans
     securing nuclear power plant





Homework

Exploring automatic face detection

Homework: Overview

- Explore what influences face detection
  - Use deep learning modules from OpenCV
    github.com/crocs-muni/biometrics-utils
  - Use a webcam or your own picture(s)
    - Your pictures will not be shared
  - Test real-live modifications or digital touch-up
- Submit to IS MUNI **a single ZIP file** with
  - Report (PDF) with proper methodology (see next slide)
  - Used adjusted images
- Deadline: 6. 12. 2020 8:00

Homework: Overview

Step 1: State the hypotheses.

E.g., obstructing eyes decreases face detection accuracy significantly more than obstructing other face parts.

Step 2: Set the criteria for a decision.

Set baseline (no obstructions) and test different settings, do *multiple* small changes (progressively obstructing eyes, mouth, ...).

Step 3: Interpret the results.

Summarize the results, reject the hypothesis if appropriate.

Homework: Hypotheses

- Measurable (we can make observations)
  - *NOT: "There are invisible creatures all around us."*
- **Falsifiable** (if it's false, we can show it)
  - *NOT: "There are other planets in the universe where life exists."*
- **Precise** (can be made into experiment)
  - *NOT: "Candles repel mosquitoes."*
- Reproducible (others can verify it)
  - *NOT: "Putting an African bush elephant on the top of the Leaning tower of Pisa will crash it."*
- Useful enough (predictive, not too general, ...)
  - *NOT: "A Škoda Superb car with (...specification...) will drive more than 2 km with 20 l of petrol."*

Note: Hypothesis is always a statement, not a question

Task: Formulating Hypotheses

Formulate possible good hypotheses based on these sentences:

1. Do people like iris eye readers?
2. 256b AES keys are secure.
3. PV181 is the best course at FI MU.
4. You can make a lock that opens with three different keys.
5. Closing the browser deletes the cookies.

Task: Formulating Hypotheses

Possible nice hypotheses:

1. Non-IT university students consider using fingerprint readers more usable than iris eye readers for day-to-day authentication.
2. You cannot successfully break 256b AES encryption in CBC mode in one hour on machine XYZ.
3. Among all bachelor students at FI MU, the average self-reported satisfaction with PV181 is significantly higher than for IB000.
4. You cannot make a lock that opens with three different keys.
5. All non-permanent cookies are removed after closing Google Chrome 89.0.4389.114 (Official Build) (64-bit).

Homework: Report

- Write a summarizing report
  - Your hypotheses and how you tested them
  - Test at least 5 distinct features
- Concentrate on:
  - Having a formulated hypotheses for each feature
  - Having several images supporting/falsifying your idea
- Avoid:
  - Many changes in the face at once
  - Radical changes (deleting half the face)
  - Overgeneralization

Homework: Scoring

- Up to 10 points awarded
  - Scoring rubric available in the Information system
  - The rubric can help you understand what is important in the task!