# Biometrics 2
## Face recognition

**PV181 Laboratory of security and applied cryptography**
**Seminar 27. 11. 2019**

Agáta Kružíková, 409782@mail.muni.cz
Martin Ukrop, mukrop@mail.muni.cz

CRoCS
Centre for Research on
Cryptography and Security

# Lecture structure

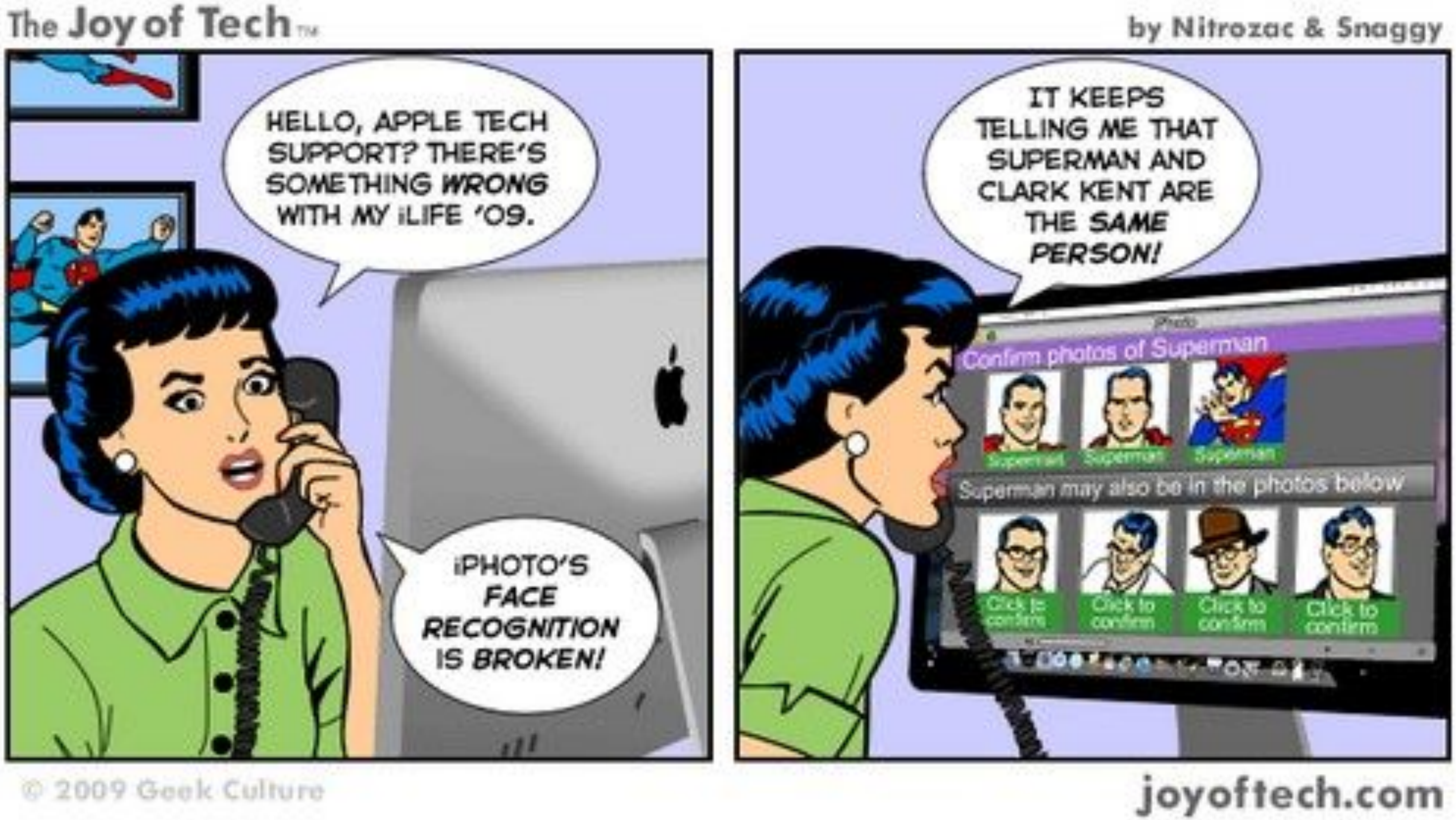
## Seminar 1

1. Introduction
2. Fingerprints
3. Seminar activity
   - Fake fingerprints
4. Homework
   - Report on selected biometric system

## Seminar 2

1. Face recognition
2. Seminar activity
   - Face biometric SWOT analysis
3. Homework
   - Age estimation

# Real-life example

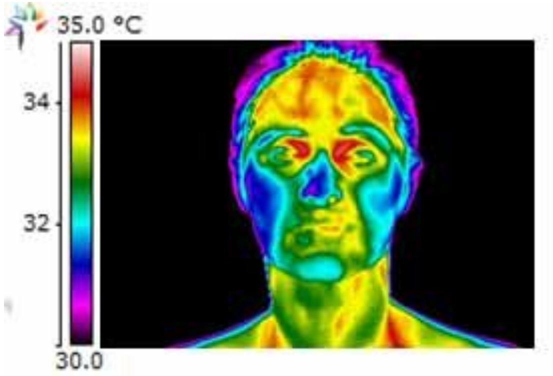

HELLO, APPLE TECH SUPPORT? THERE'S SOMETHING WRONG WITH MY iLIFE '09.
iPHOTO'S FACE RECOGNITION IS BROKEN!
IT KEEPS TELLING ME THAT SUPERMAN AND CLARK KENT ARE THE SAME PERSON!
iPhoto
Confirm photos of Superman
Superman
Superman
Superman
Superman may also be in the photos below
Click to confirm
Click to confirm
Click to confirm
Click to confirm

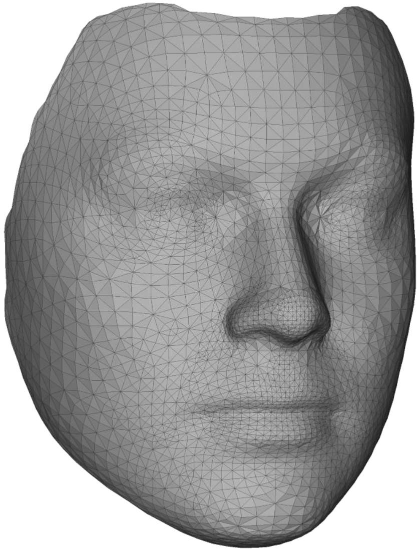
The Joy of Tech™ by Nitrozac & Snaggy

© 2009 Geek Culture joyoftech.com

# Face recognition – Input

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





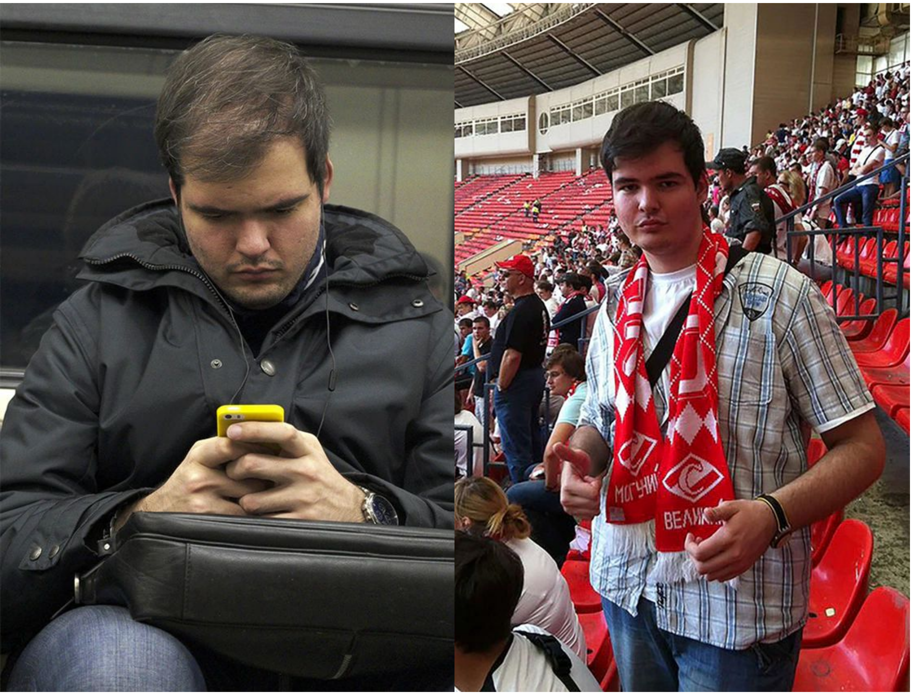
# Face recognition: The manual way

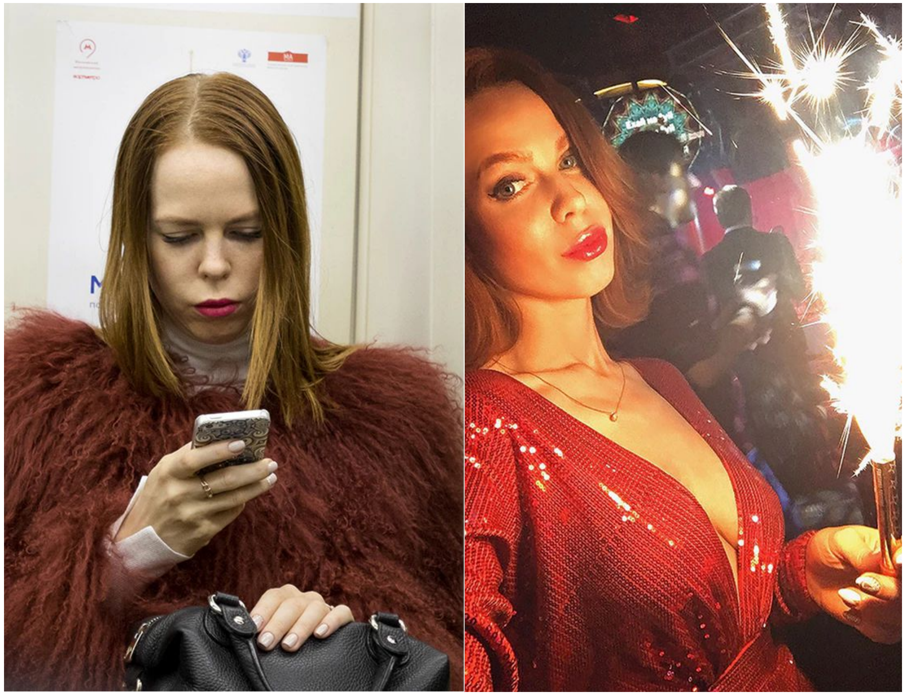
# Face recognition: The automatic way

- 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)





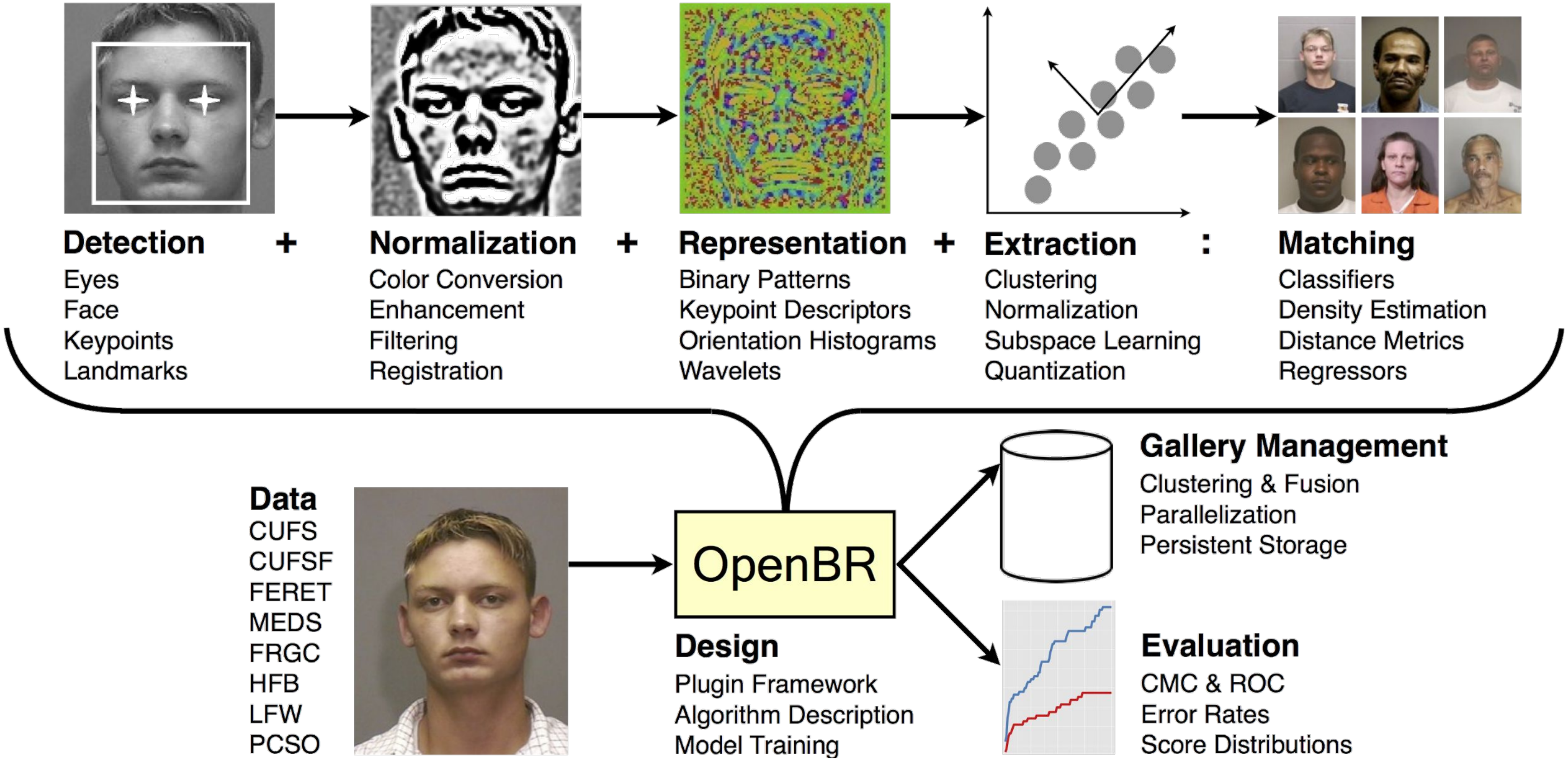
# Challenges in face recognition

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

# Testing sets (databases)

- Many databases: http://www.face-rec.org/databases/
- Covering:
  - Aging
  - Ilumination
  - Pose
  - Expresion

# OpenBR: Face recognition overview



**Detection** +
Eyes
Face
Keypoints
Landmarks

**Normalization** +
Color Conversion
Enhancement
Filtering
Registration

**Representation** +
Binary Patterns
Keypoint Descriptors
Orientation Histograms
Wavelets

**Extraction** :
Clustering
Normalization
Subspace Learning
Quantization

**Matching**
Classifiers
Density Estimation
Distance Metrics
Regressors

**Data**
CUFS
CUFSF
FERET
MEDS
FRGC
HFB
LFW
PCSO

**Design**
Plugin Framework
Algorithm Description
Model Training

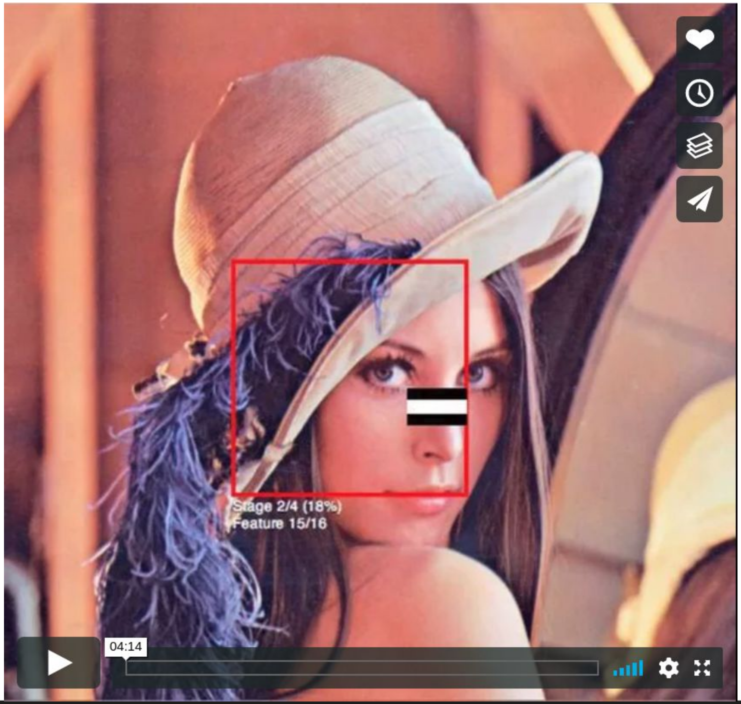
**Gallery Management**
Clustering & Fusion
Parallelization
Persistent Storage

**Evaluation**
CMC & ROC
Error Rates
Score Distributions

Photo © 2016 openbiometrics.org

# OpenBR face recognition – visualization

- Haar-cascade Detection
- Machine learning based approach where a cascade function is trained from a lot of positive and negative images.
- See video: *OpenCV Face Detection: Visualized* https://vimeo.com/12774628



# CV Dazzle: Anti face-detection

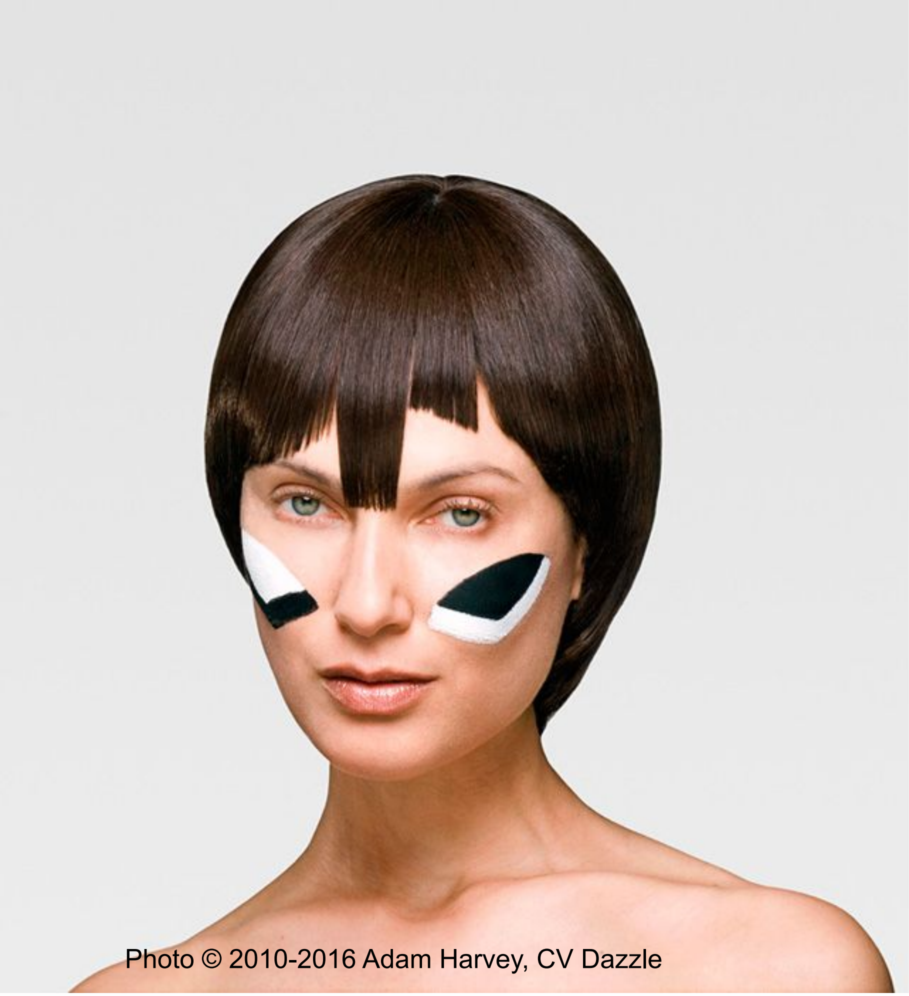
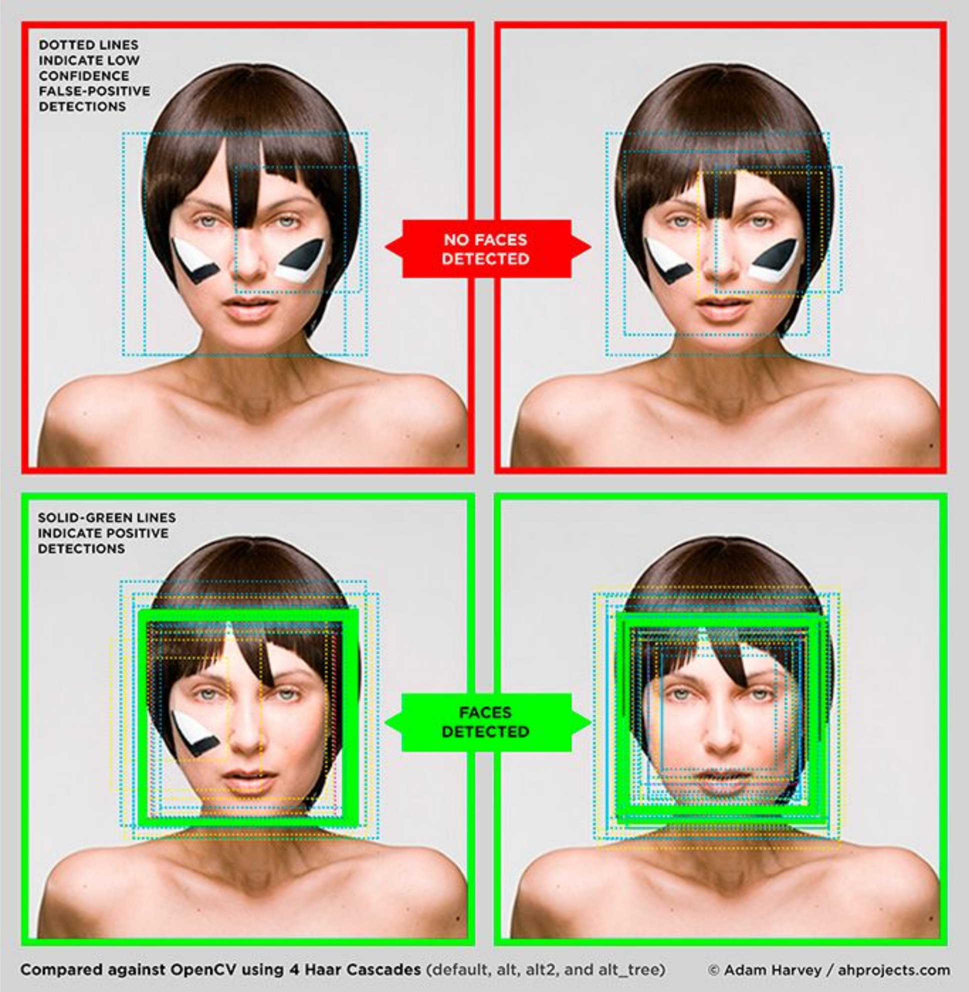


Photo © 2010-2016 Adam Harvey, CV Dazzle


DOTTED LINES INDICATE LOW CONFIDENCE FALSE-POSITIVE DETECTIONS
NO FACES DETECTED
SOLID-GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED

Compared against OpenCV using 4 Haar Cascades (default, alt, alt2, and alt_tree) © Adam Harvey / ahprojects.com

# CV Dazzle: Anti face-detection

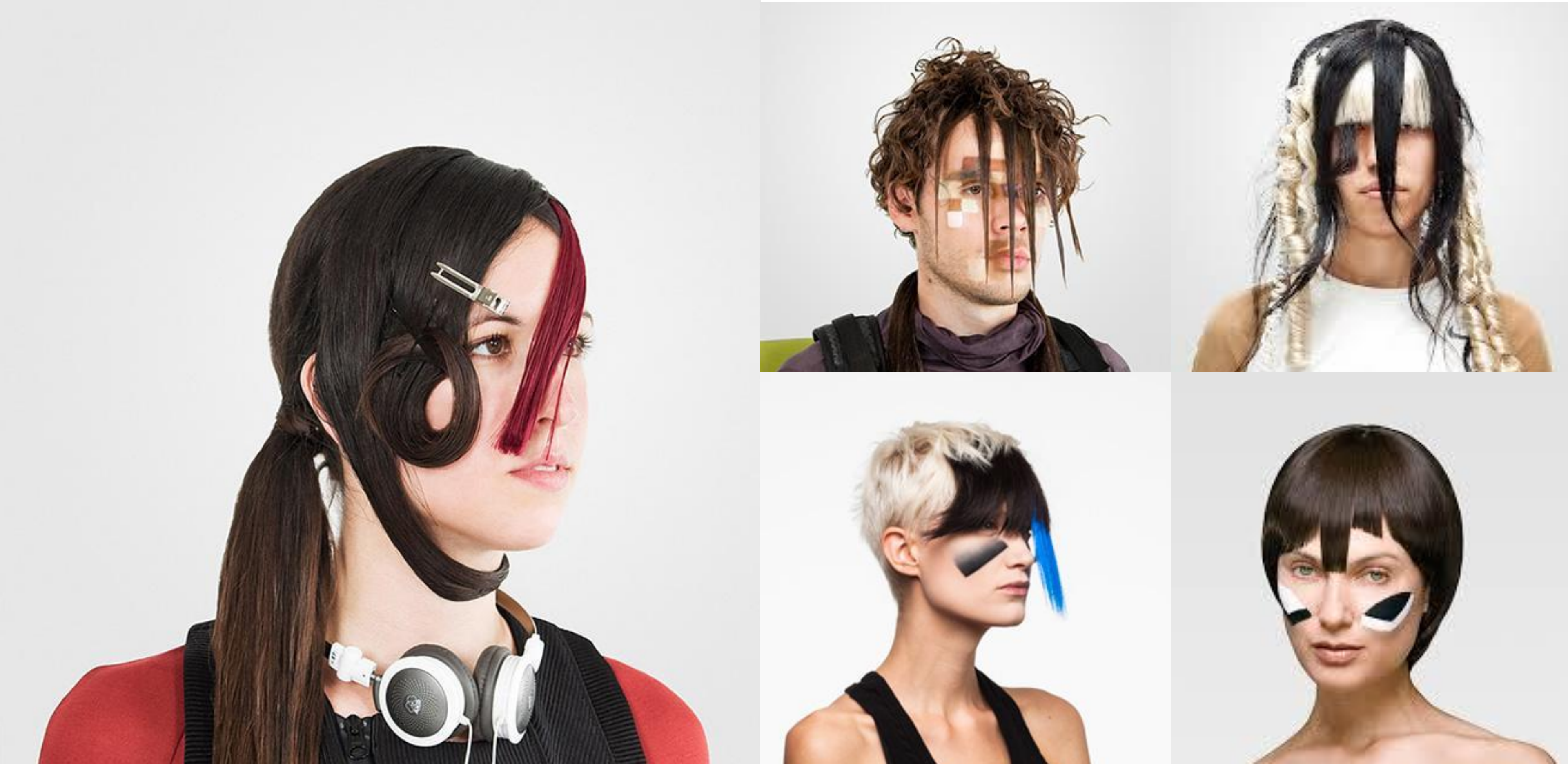
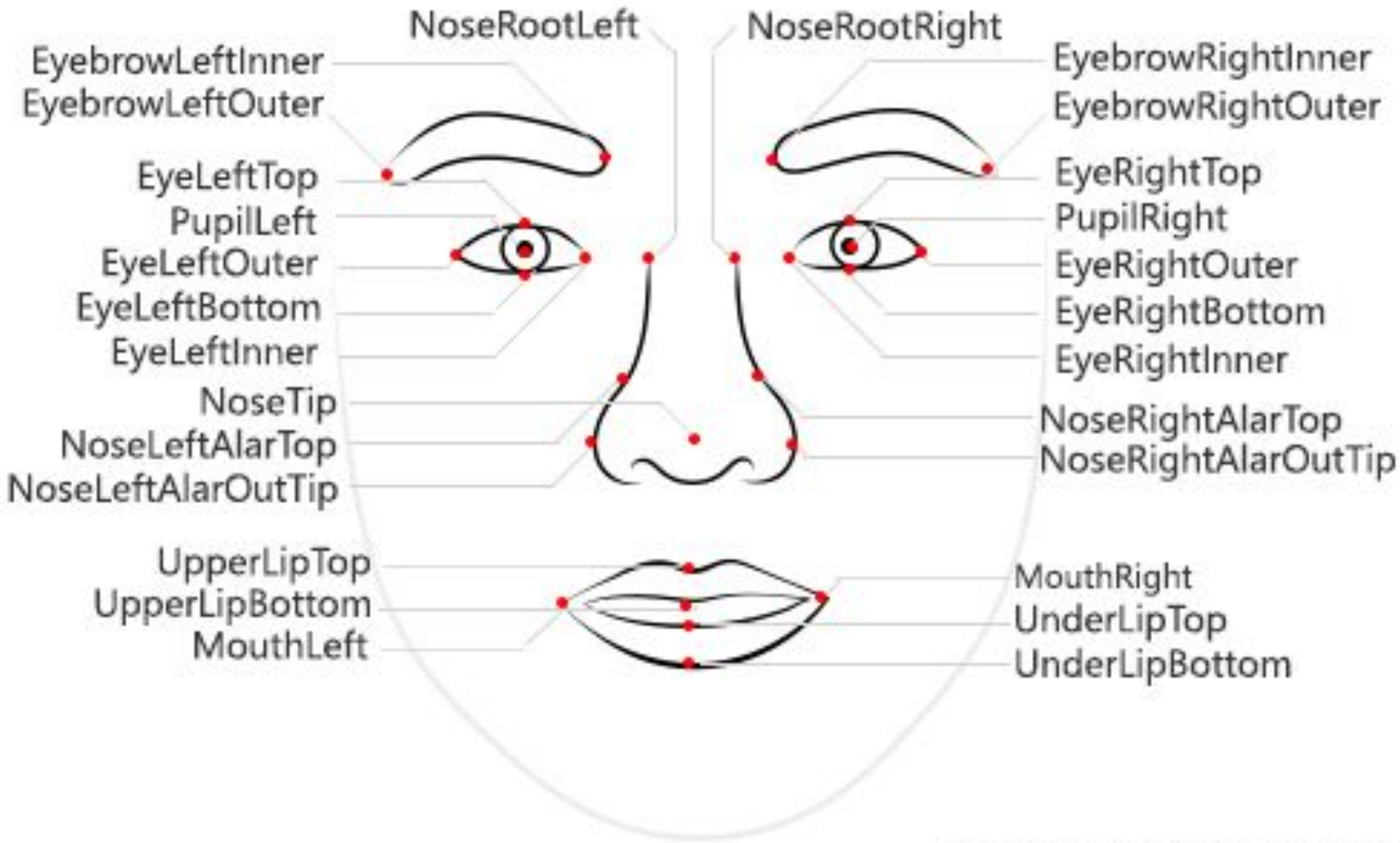


Photo © 2010-2016 Adam Harvey, CV Dazzle

# Microsoft: Face API



# Automatic passport control

# 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

# Face impersonation

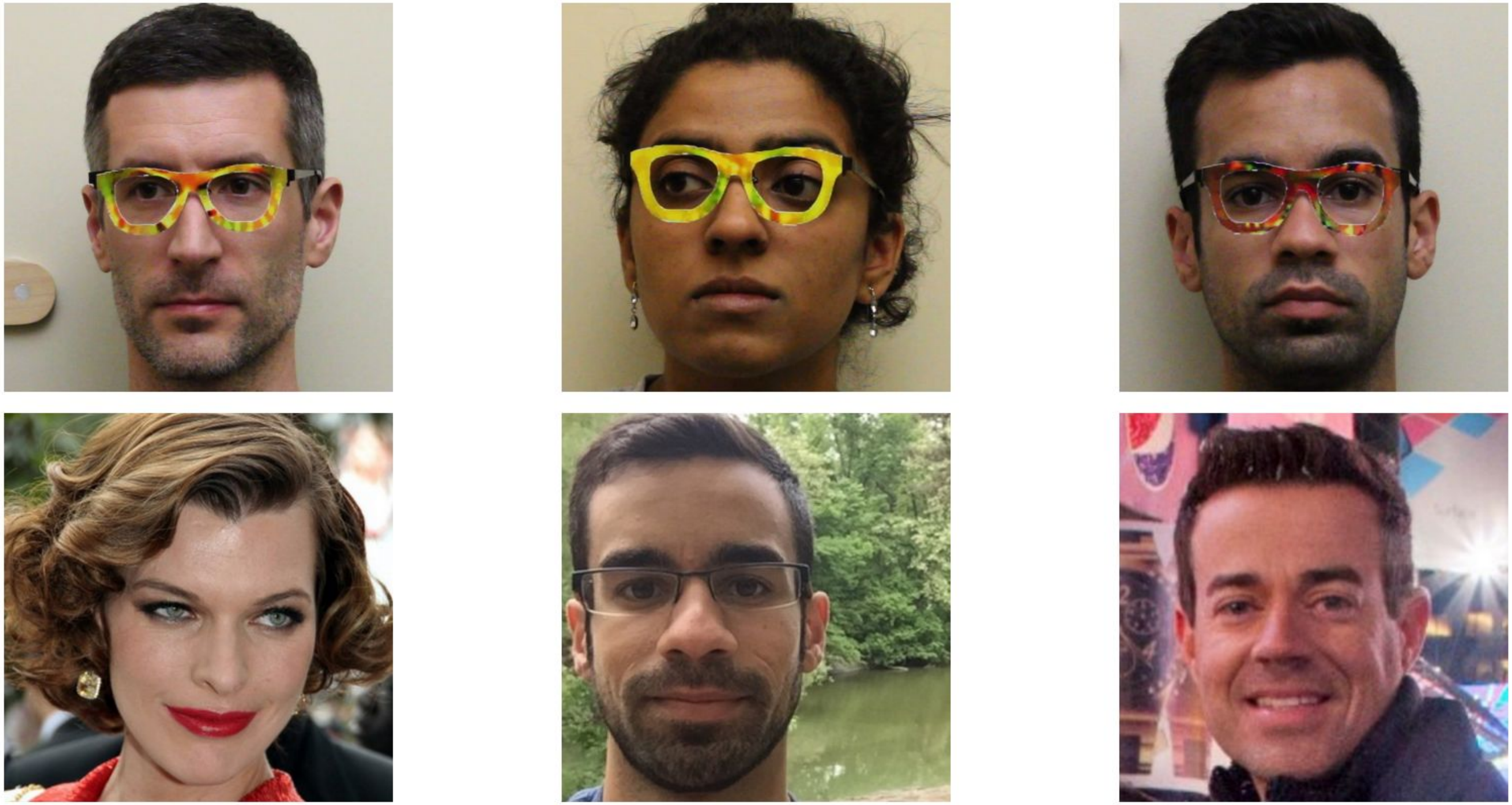


Photo © 2016 Carnegie Mellon University, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*

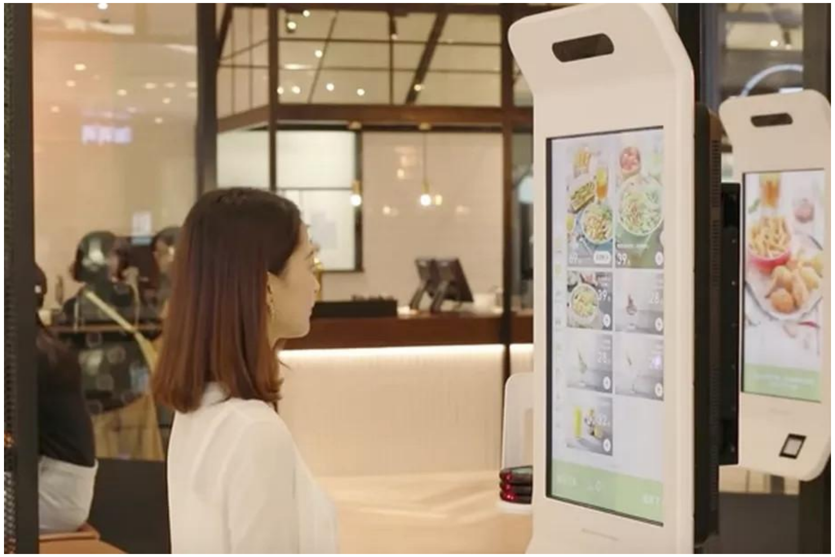
# Face impersonation

- 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.*

# KFC AliPay

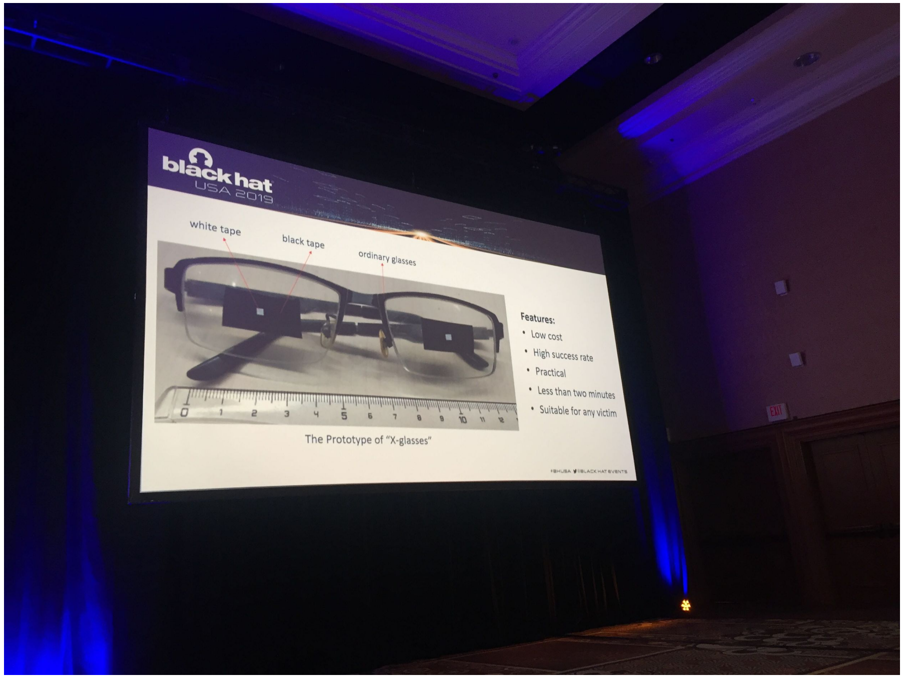
- Introduced 2015
- Only one KFC in China



- See AliPay promo video at https://www.theverge.com/2017/9/4/16251304/kfc-china-alipay-ant-financial-smile-to-pay

# Apple FaceID hacked

- Liveness detection feature
- In 2019 by researchers
- Hacked by usage of pair of modified glasses
- A victim has to sleep :-)



Features:

- Low cost
- High success rate
- Practical
- Less than two minutes
- Suitable for any victim

The Prototype of "X-glasses"

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

# Detecting sexual orientation from faces

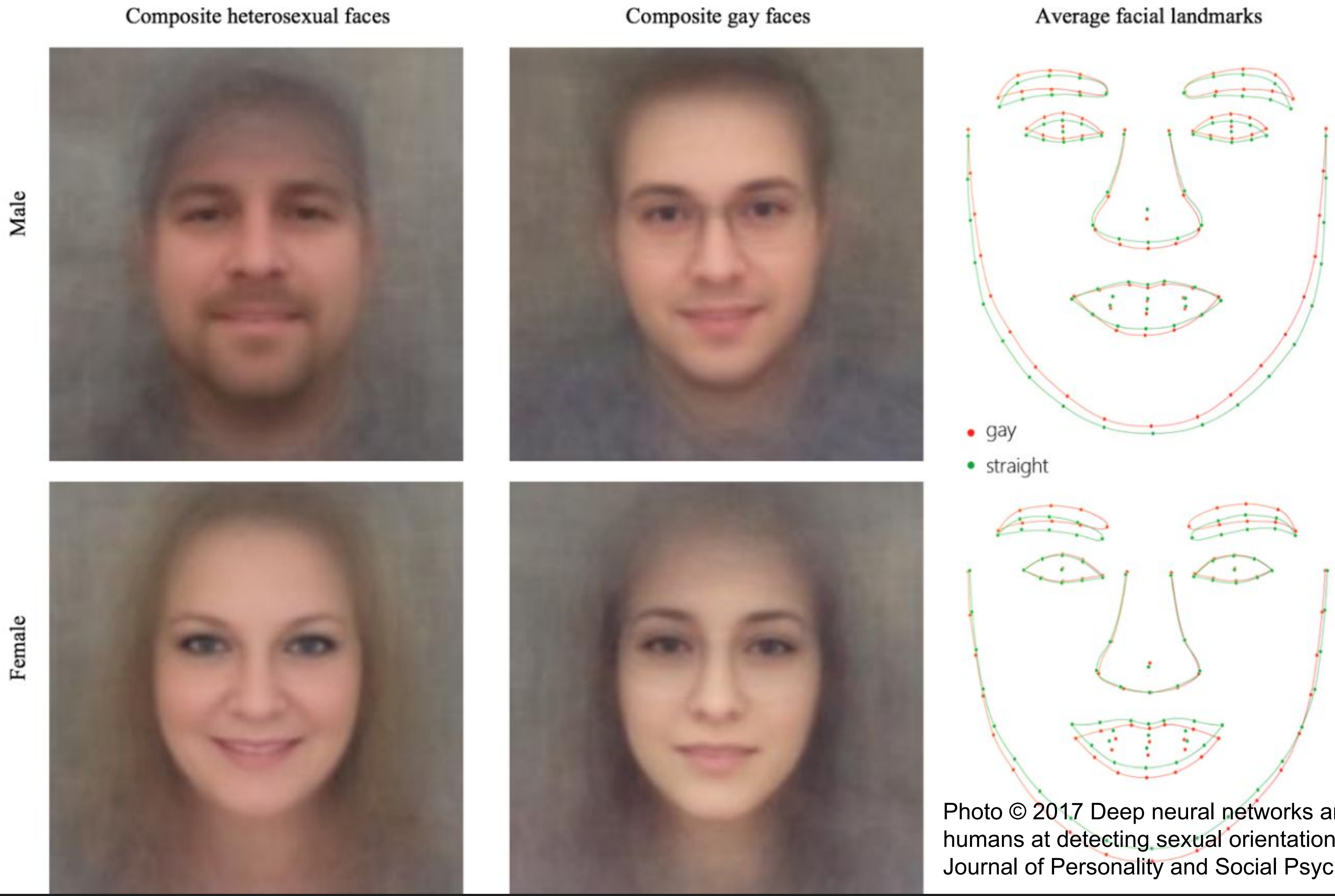


Photo © 2017 Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology

# 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

- San Francisco
- “Threat to civil liberties”
- Ban for government agencies (city police and sheriff)
- Federal agencies not affected
- Reason: privacy issue
  - Less accurate at people of colour
- For the supplier: step back
- www.banfacialrecognition.com

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

# 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

Advancing Computing as a Science & Profession, *ACM Code of Ethics and Professional Conduct. Online [2019]: acm.org/code-of-ethics*

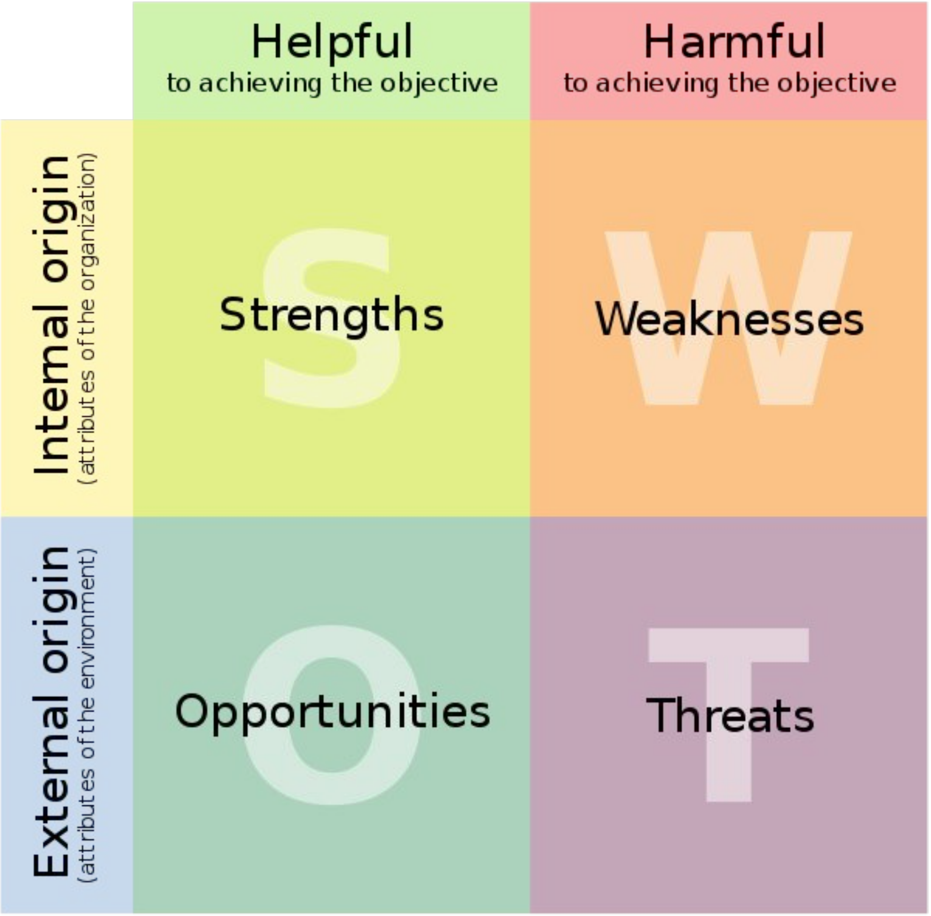
# Fun with biometrics

- InterSoB task
  - https://how-old.net/
  - Try to appear as old as possible

Photo © 2016 Dominika Krejčí, InterSoB

# Detour: SWOT analysis

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



| | Helpful<br>to achieving the objective | Harmful<br>to achieving the objective |
|---|---|---|
| Internal origin<br>(attributes of the organization) | S<br>Strengths | W<br>Weaknesses |
| External origin<br>(attributes of the environment) | O<br>Opportunities | T<br>Threats |

# 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 SMS/OPT and Push-to-Approve

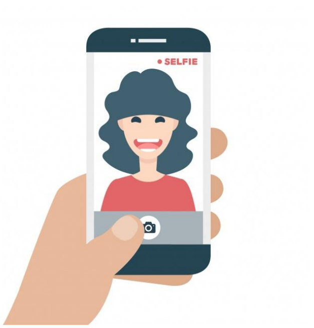
**Threats**

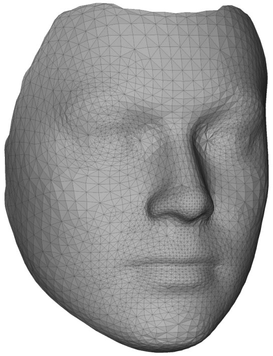
- Bad attack understanding
- Long tail of replacement
- Usability issues
- The dark web

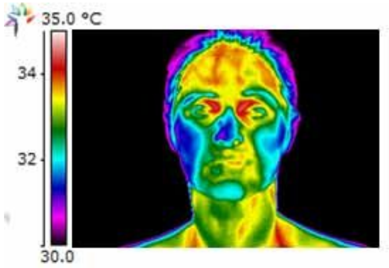
Example inspired by the RSAC 2018 talk *Passwords and fingerprints and faces – Oh my! Comparing old and new authentication* by Jackson Shaw

# 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 age estimation

# Homework: Overview

- Investigate what influences age estimation
  - In https://how-old.net/ (neural-networks based)
  - Adjust our pictures again
- Submit to IS MUNI **a single ZIP file** with
  - Report (PDF), see next slide
  - Used adjusted images
- Deadline: 4. 12. 2018 8:00

# Homework: Overview

**Step 1: State the hypotheses.**

E.g., Wrinkles around the tails of eyes increase the estimated age.

**Step 2: Set the criteria for a decision.**

Set baseline (no wrinkles) and repeat measurement for different wrinkles around tails of eyes.

**Step 3: Compute the test statistic (if you know how).**

In our simplistic case, take a look on measurements.
This is not necessary, if you don't understand statistics well.

**Step 4: Interpret the results.**

The hypothesis should not be regarded as true based on these data.

# Homework: Good methodology

**Measurements:**
Martin 1 - 27
Martin 2 - 27
Martin 3 - 27
Martin 4 - 27
Martin 5 - 27

# 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 (e.g. smoother skin decreases estimated age)
  - Having several images supporting/falsifying your idea
- Avoid:
  - Many changes in the face at once
  - Radical changes (deleting half the face)
  - Overgeneralization

# Homework: Methodology, 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!
- Have a look at old homework submissions with good methodology in the Study Materials.
  - Special thanks to Jan Kvapil and Rao Arvind for providing them.

# Homework: Bad methodology (but at least funny)