Biometrics 2
Face recognition

PV181 Laboratory of security and applied cryptography
Seminar 13, 12. 12. 2018

Vlasta Šťavová, vlasta.stavova@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

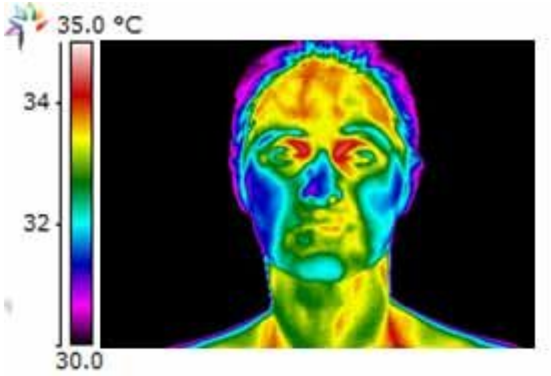
1. Face recognition
2. Seminar activity
   - Face biometric SWOT analysis
3. Homework
   - Age estimation

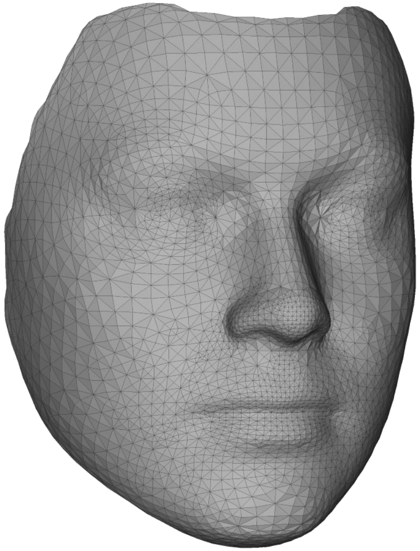
Real-life example

The Joy of Tech™
by Nitrozac & Snaggy
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
© 2009 Geek Culture
joyoftech.com

Face recognition – Input

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



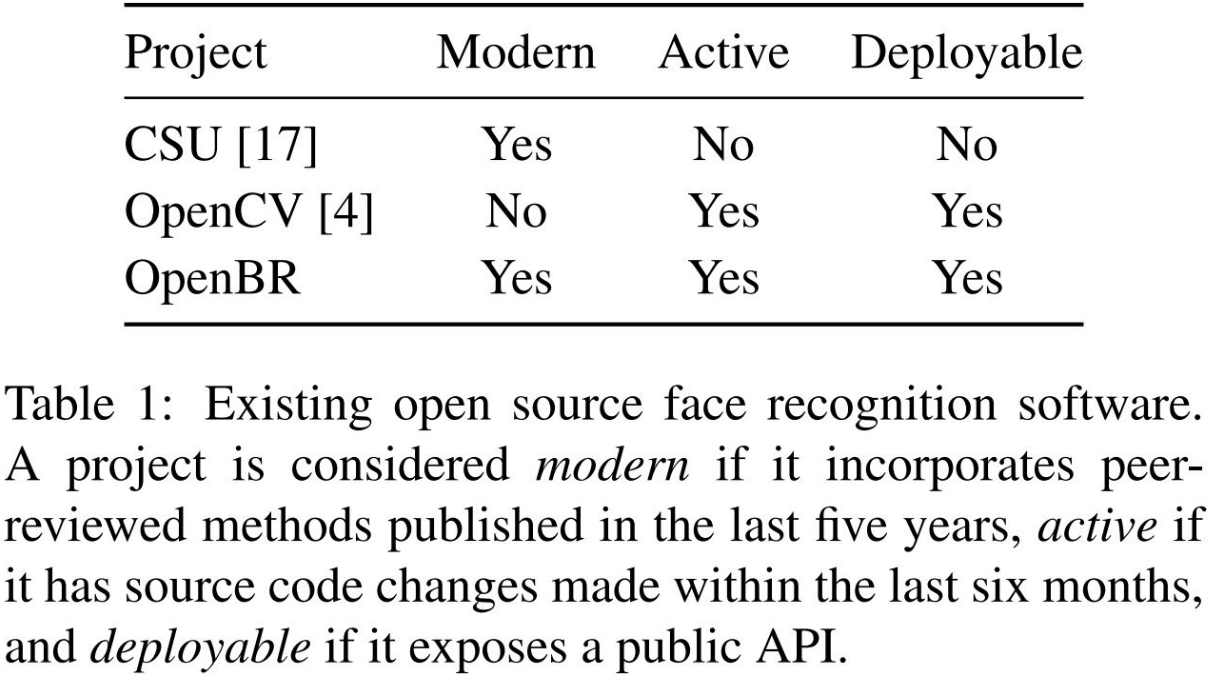


Face recognition: The manual way

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

Open source frameworks



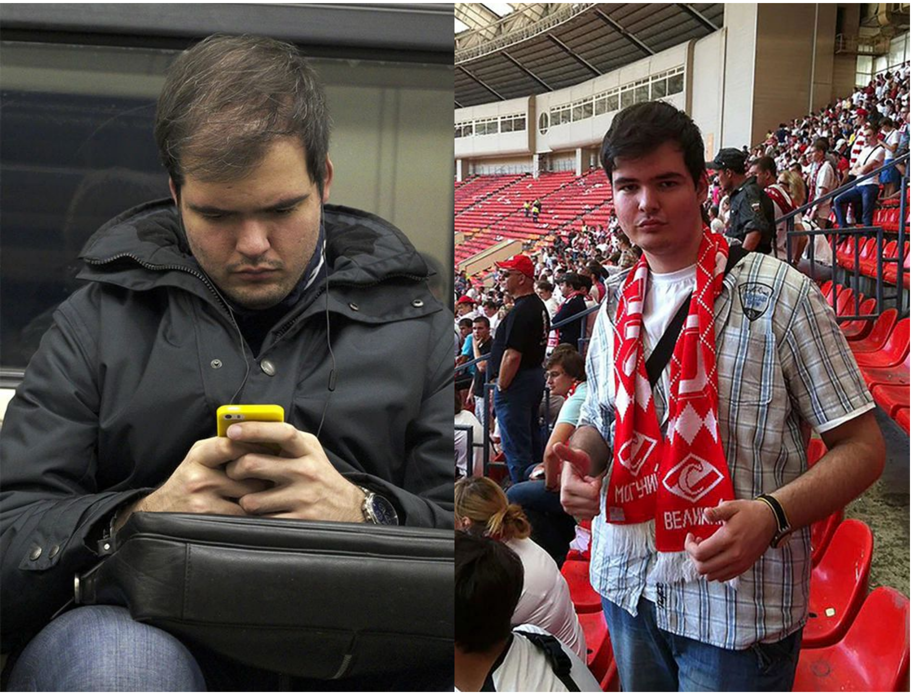
Project	Modern	Active	Deployable
CSU [17]	Yes	No	No
OpenCV [4]	No	Yes	Yes
OpenBR	Yes	Yes	Yes

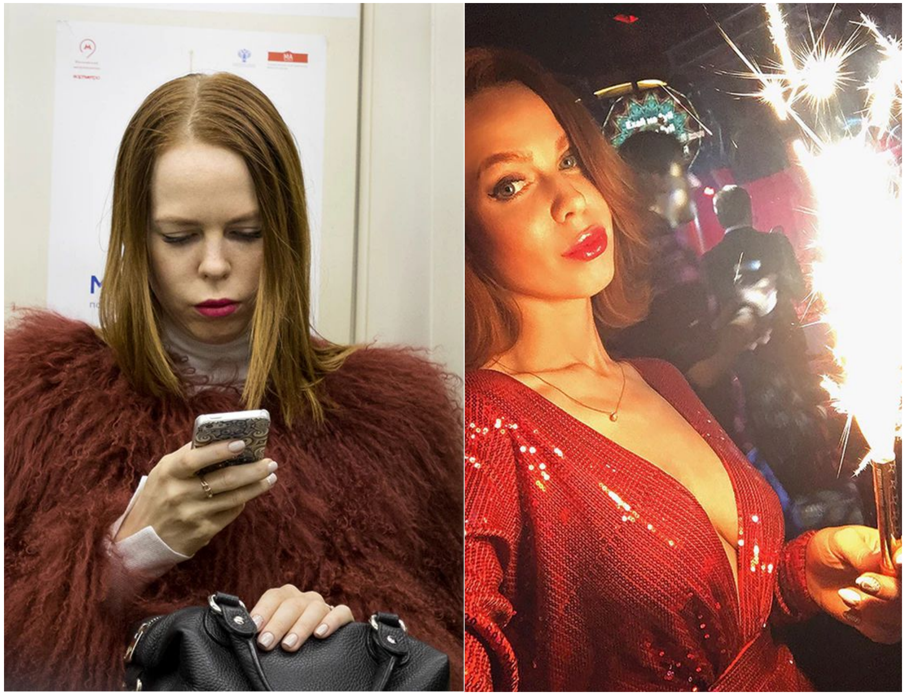
Table 1: Existing open source face recognition software. A project is considered *modern* if it incorporates peer-reviewed methods published in the last five years, *active* if it has source code changes made within the last six months, and *deployable* if it exposes a public API.

J. Klontz, B. Klare, S. Klum, A. Jain, M. Burge. "Open Source Biometric Recognition", Proceedings of the IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013.

FindFace – example

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

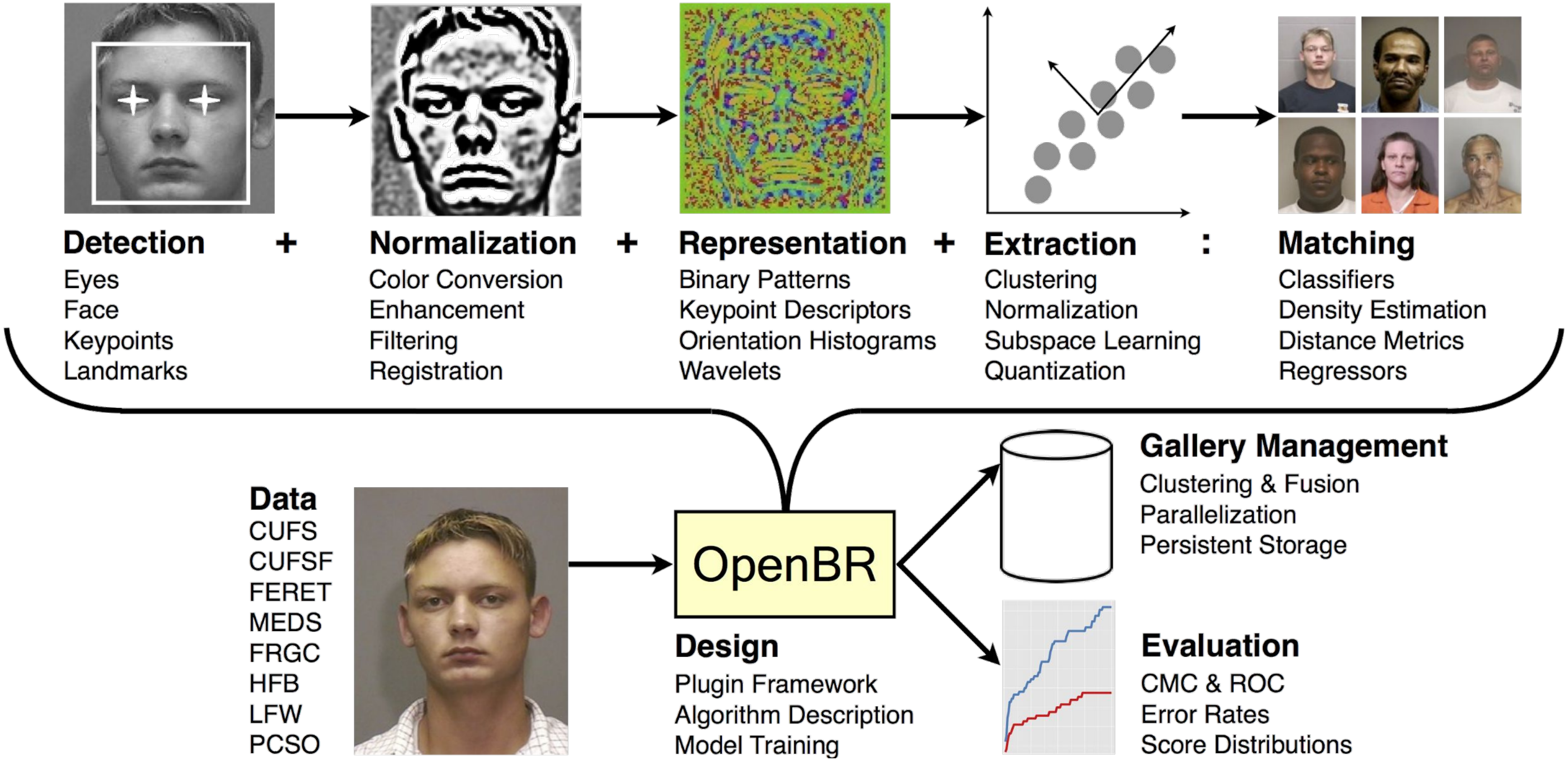




Challenges in face recognition

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

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

OpenBR

Design
Plugin Framework
Algorithm Description
Model Training

Gallery Management
Clustering & Fusion
Parallelization
Persistent Storage

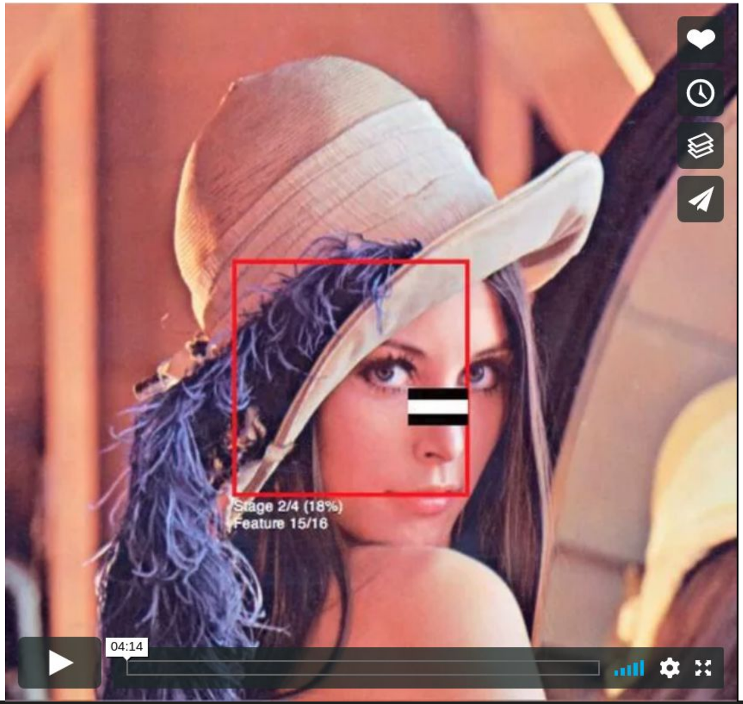
Evaluation
CMC & ROC
Error Rates
Score Distributions

Step 1 – Face detection

- Knowledge-based methods.
  - Ruled-based methods that encode our knowledge of human faces.
- Template matching methods.
  - These algorithms compare input images with stored patterns of faces or features.
- Appearance-based methods.
  - A template matching method whose pattern database is learnt from a set of training images.

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

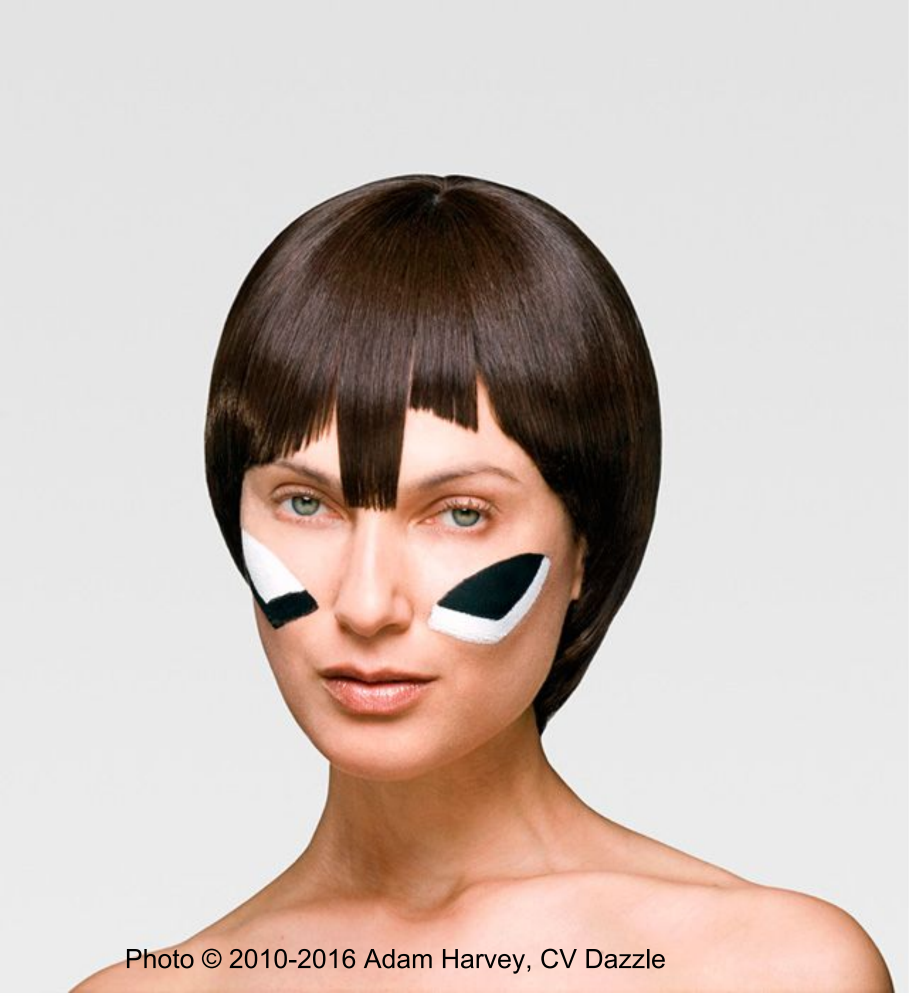
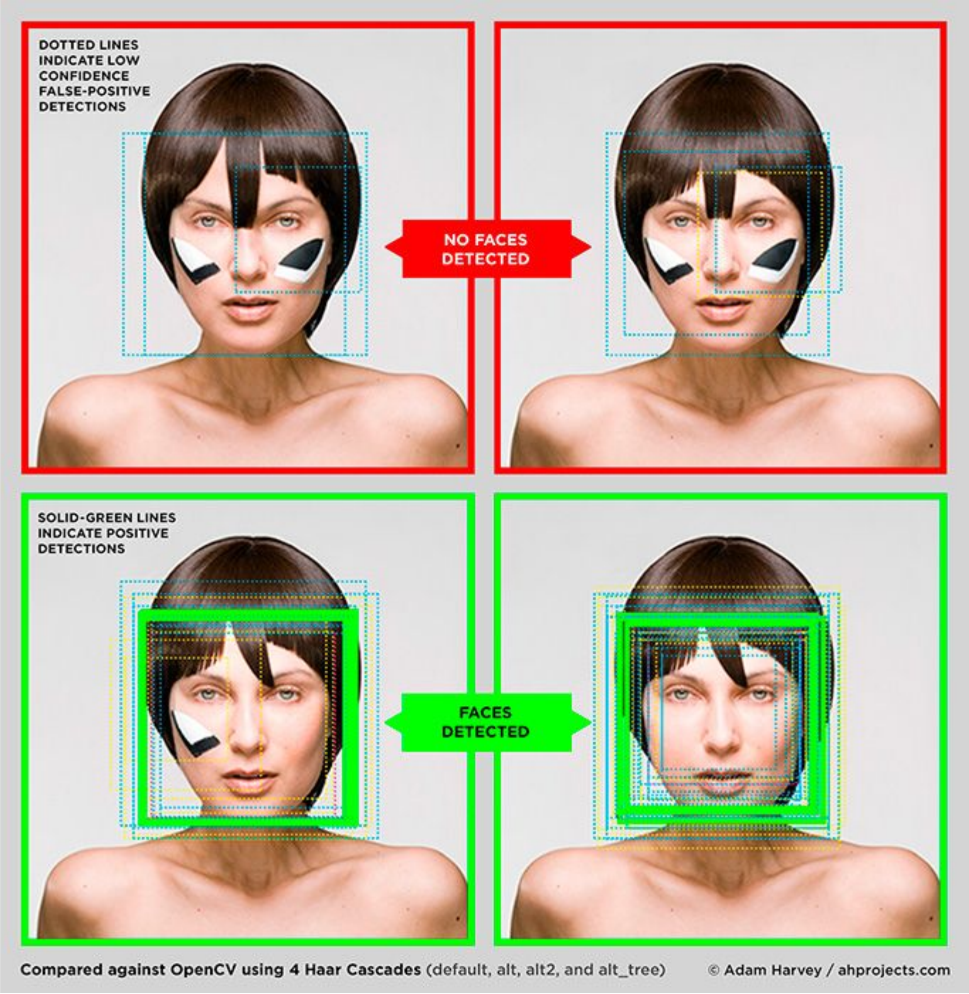


Photo © 2010-2016 Adam Harvey, CV Dazzle


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

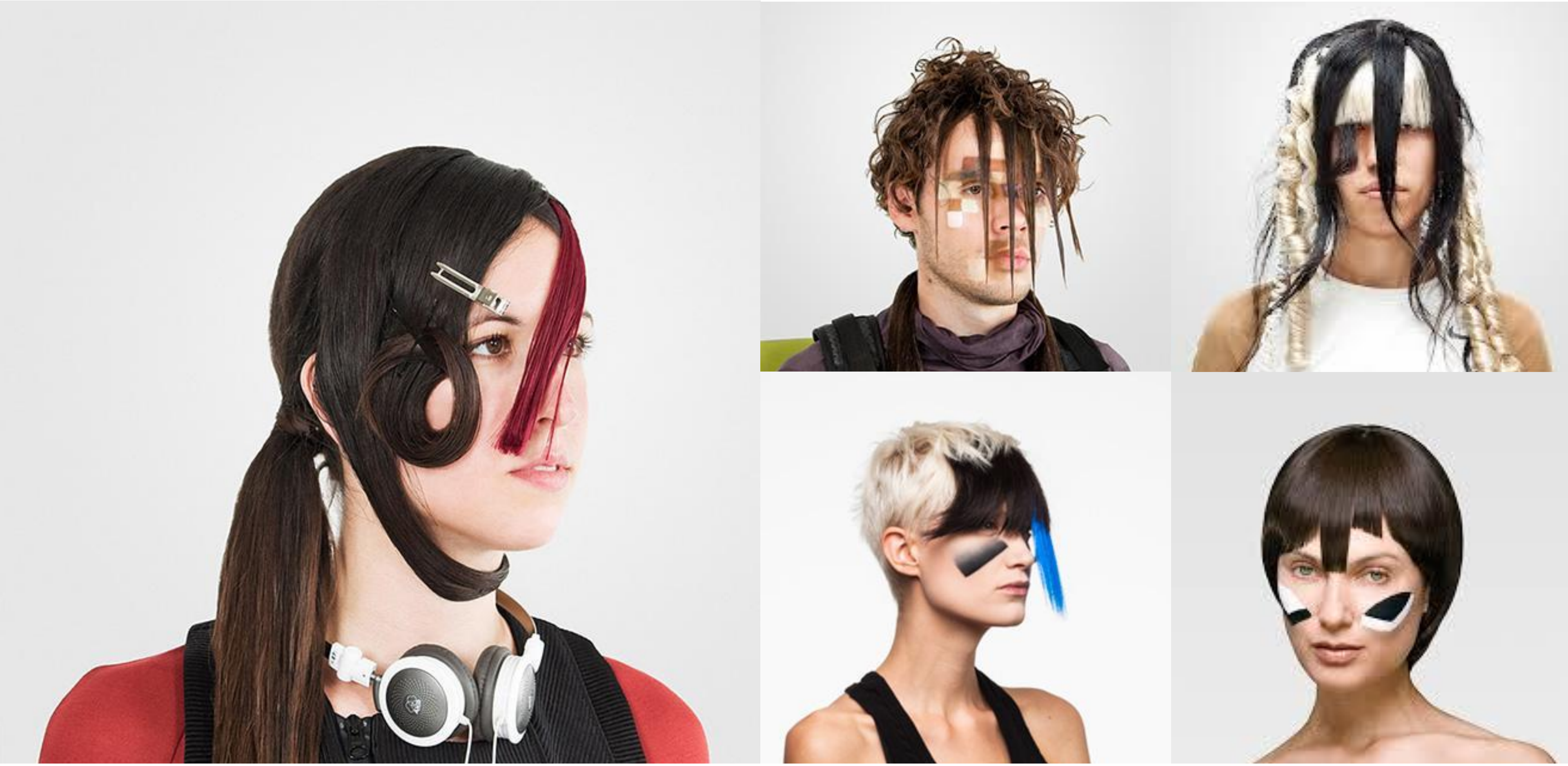


Photo © 2010-2016 Adam Harvey, CV Dazzle

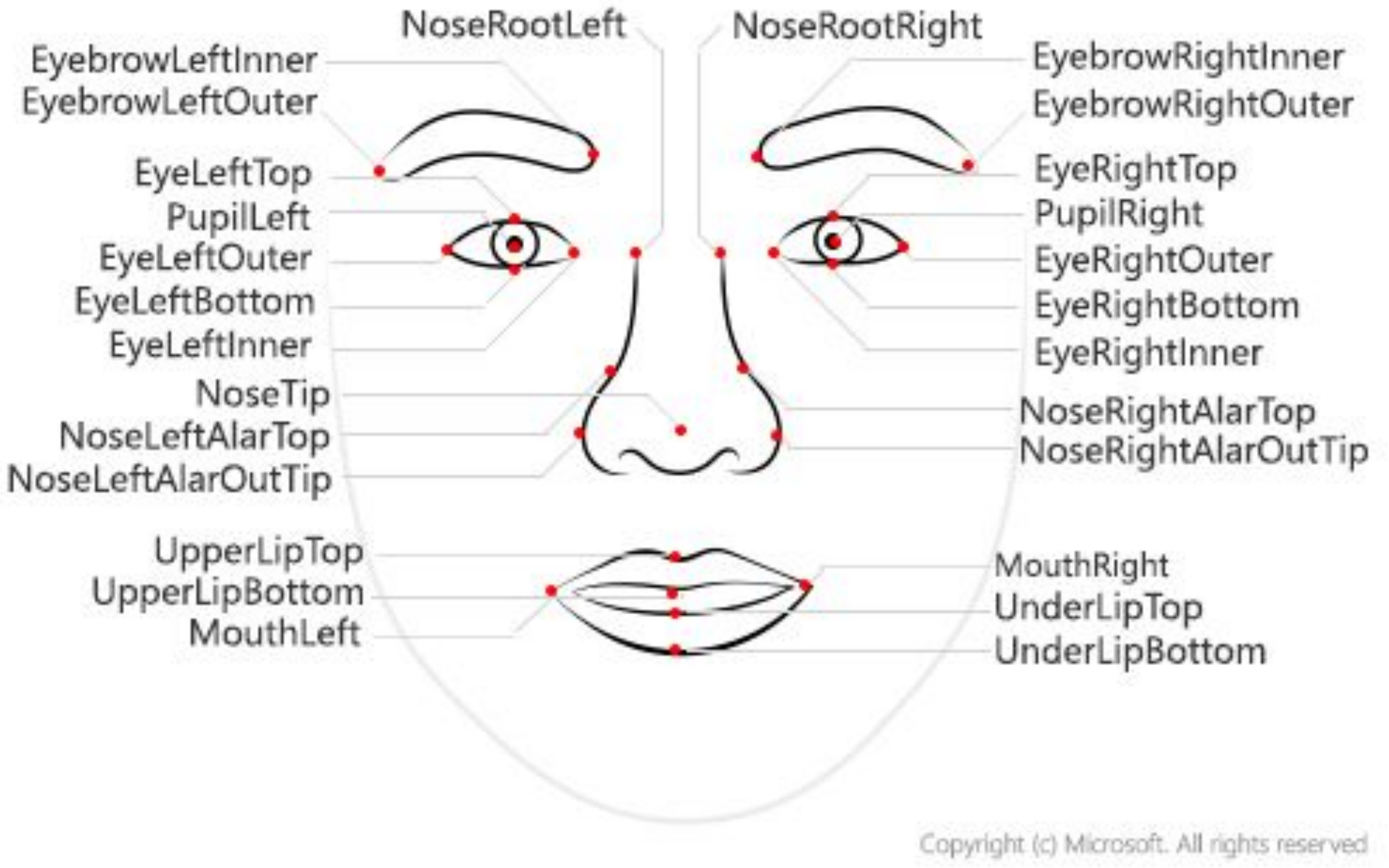
Step 2 – Normalization and Representation

- Picture preprocessing
- OpenBR approach (Eigenface):
  - Detects eyes in detected faces
  - Normalize the face with respect to rotation and scale using the eye locations
  - Converts the image to floating point format
  - Embeds the image in a PCA subspace trained on face images

Step 3 – Extraction

- Extracting relevant information from image
- Face color? Position of eyes, mouth, nose? Between eyes ratio? Width-length ratio?
- Information must be valuable to the later step of identifying the subject
- “Reducing dimension”

Microsoft: Face API



Step 4 – Matching

- Template matching
  - Patterns are represented by samples, models, pixels, curves, textures. The recognition function is usually a correlation or distance measure.
- Statistical approach
  - Patterns are represented as features. The recognition function is a discriminant function.
- Neural networks
  - The representation may vary. There is a network function in some point.

Step 5 – Output

- Confidence:
  - Euclidian distance as match measure
  - Interval 0 (=bad match) to 1 (=perfect match)
  - Cca >0.6 to detect similarity
- Similarity value for comparing two templates
  - The higher value the more likely the same
  - Computed as -log(distance+1) where distance is the sum of the Euclidean distances between two face images
  - Smaller distances (Euclidean) indicate higher similarity

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

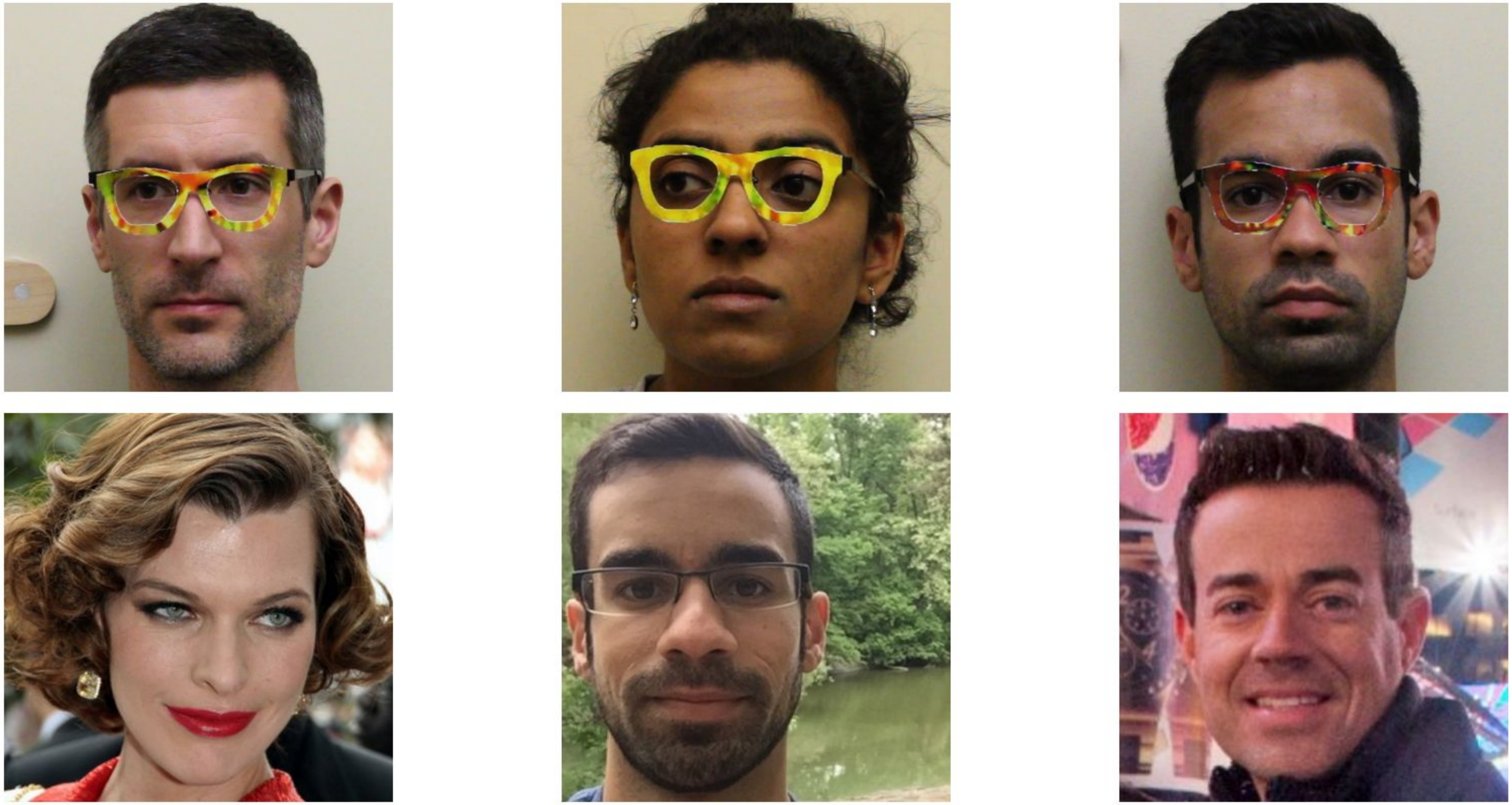


Photo © 2016 Carnegie Mellon University, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*

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.

Detecting sexual orientation from faces

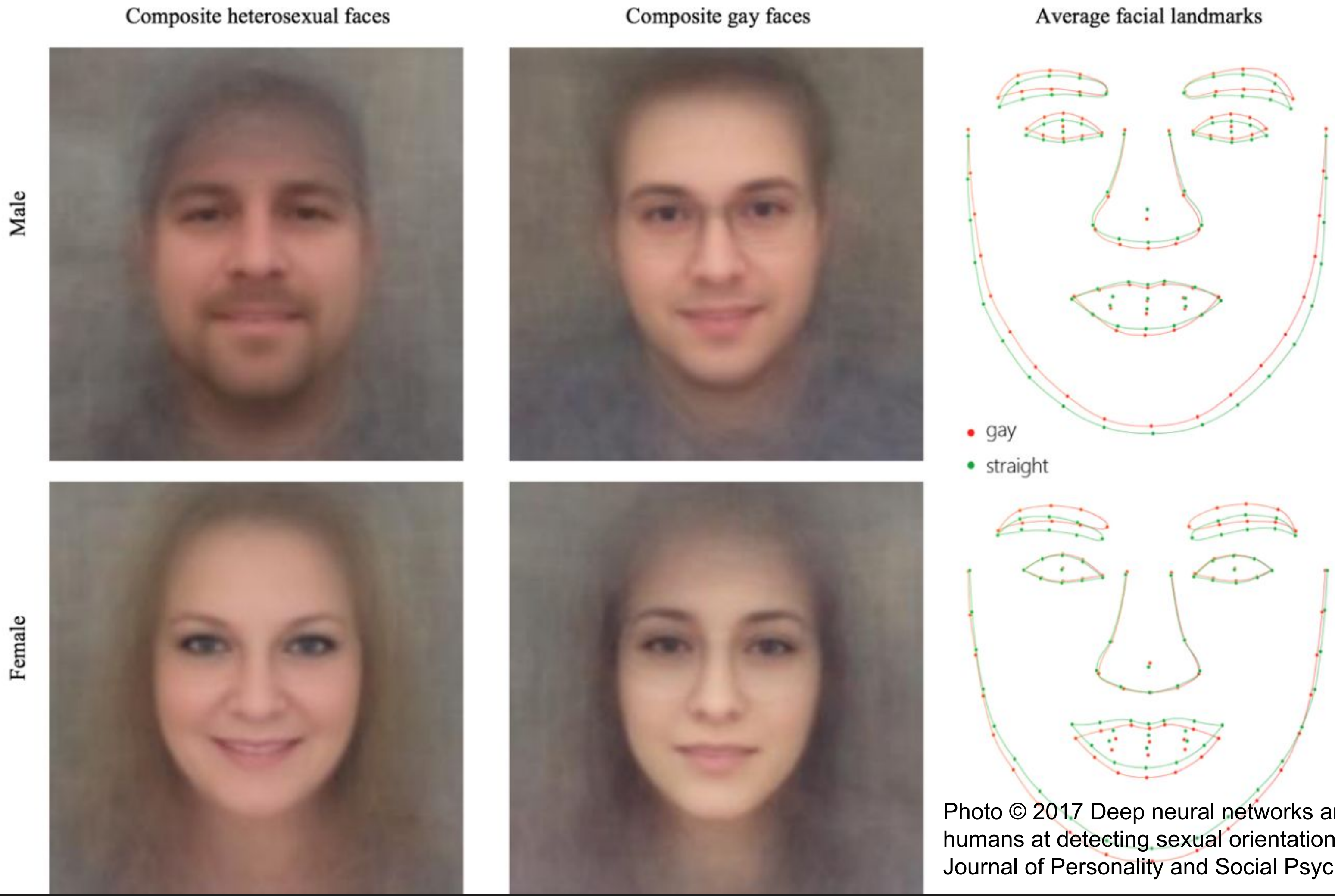


Photo © 2017 Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology

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.

Testing sets (databases)

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

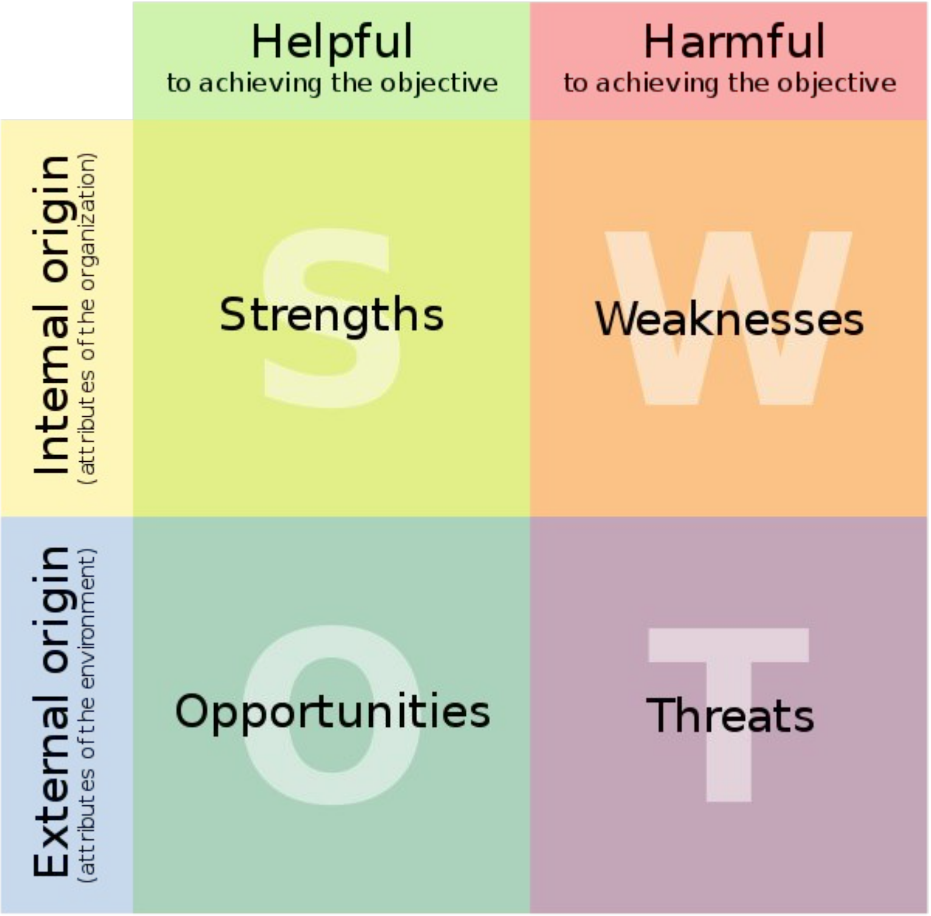
Fun with biometrics

- InterSoB task
  - https://how-old.net/
  - Try to appear as old as possible
- Attractivenes measurement
  - https://www.howhot.io/

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 to achieving the objective	Harmful to achieving the objective
Internal origin (attributes of the organization)	S Strengths	W Weaknesses
External origin (attributes of the environment)	O Opportunities	T 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

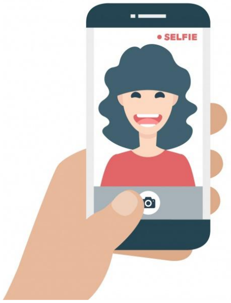
Threats

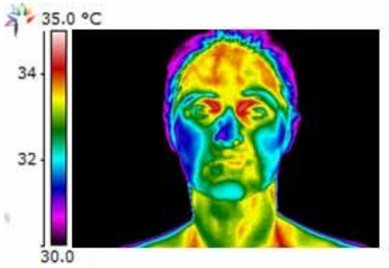
- Bad attack understanding
- Long tail of replacement
- Usability issues
- The dark web

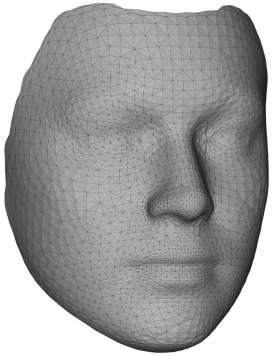
Example inspired by the RSAC 2018 talk *Passwords and fingerprints and faces – Oh my! Comparing old and new authentication* by Jackson Shaw

Seminar task

- Do a SWOT analysis for a given 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





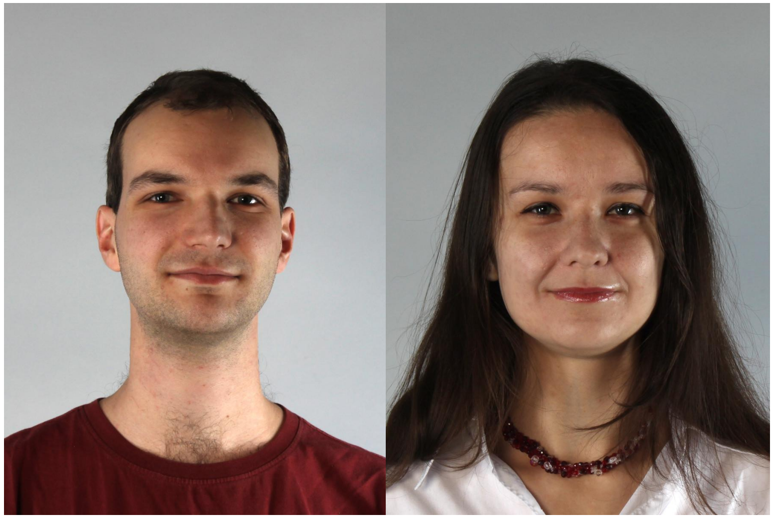


Homework

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: 20. 12. 2018 23:59



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 basics

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.

In our simplistic case, take a look on measurements.

Step 4: Make a decision.

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: Good methodology

Homework: Bad methodology (but at least funny)

Homework: Methodology basics

- Have a look at old homework submissions with good methodology in the Study Materials.
- Special thanks to Vláďa Sedláček, Kristýna Loukotová and Rao Arvind for providing them.