Biometrics 1

PV181 Laboratory of security and applied cryptography

Seminar 11

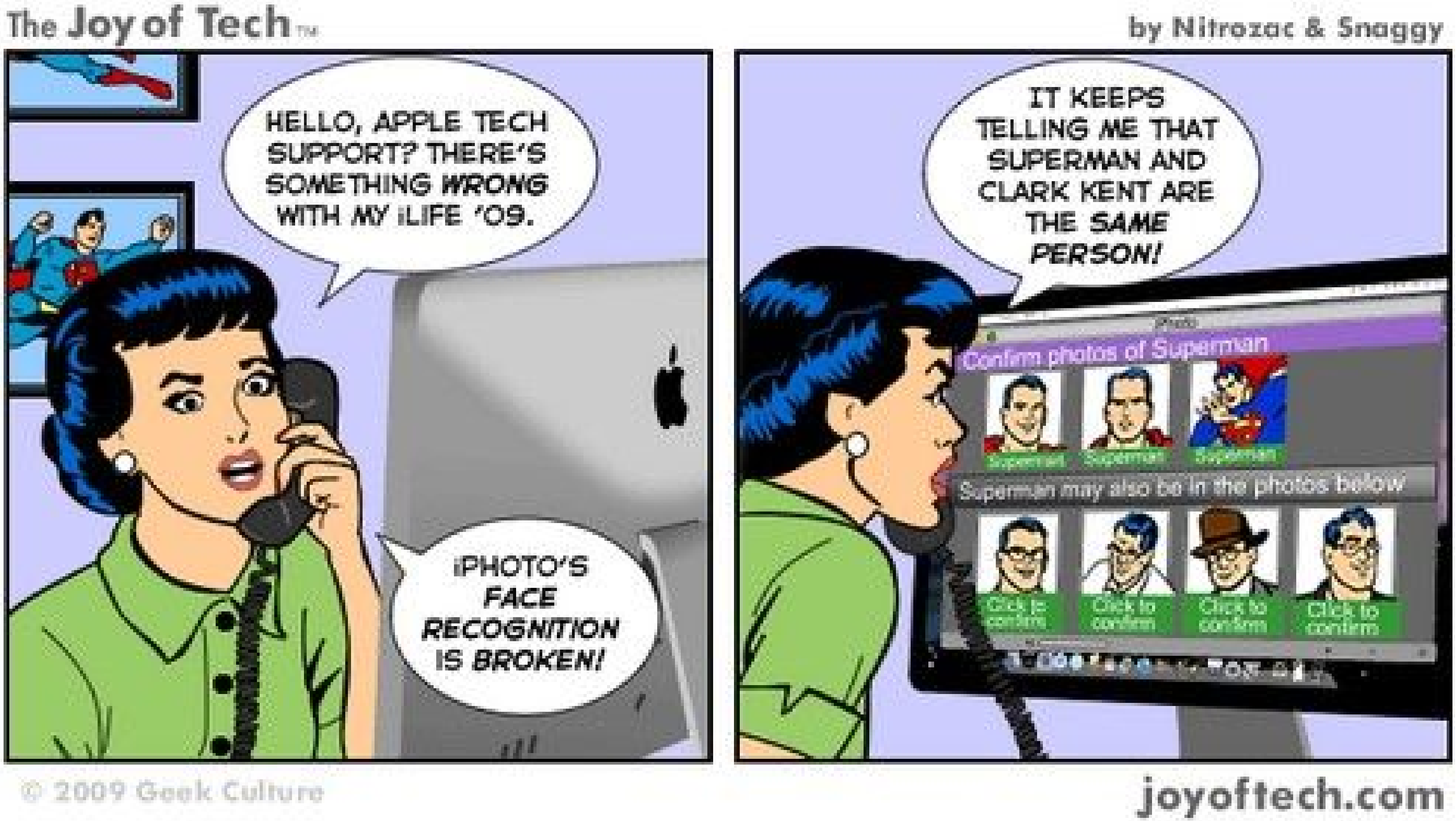
Vlasta Šťavová, vlasta.stavova@mail.muni.cz

Martin Ukrop, mukrop@mail.muni.cz

CROCS

Centre for Research on
Cryptography and Security

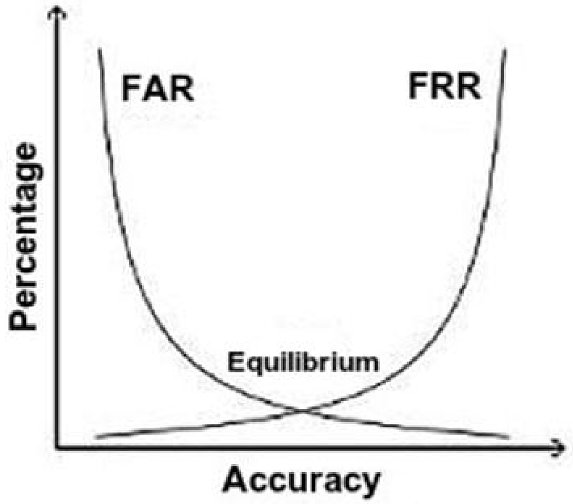
Real-life example


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!*
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

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)



Biometrics – introduction

- Physiological
  - Face
  - Fingerprint
  - Palm geometry
  - Hand vein pattern
  - Eye iris
  - Eye retina
  - DNA
- Behavioral
  - Keystrokes
  - Signature dynamics
  - Voice
  - Walking

Biometrics – basic problem?

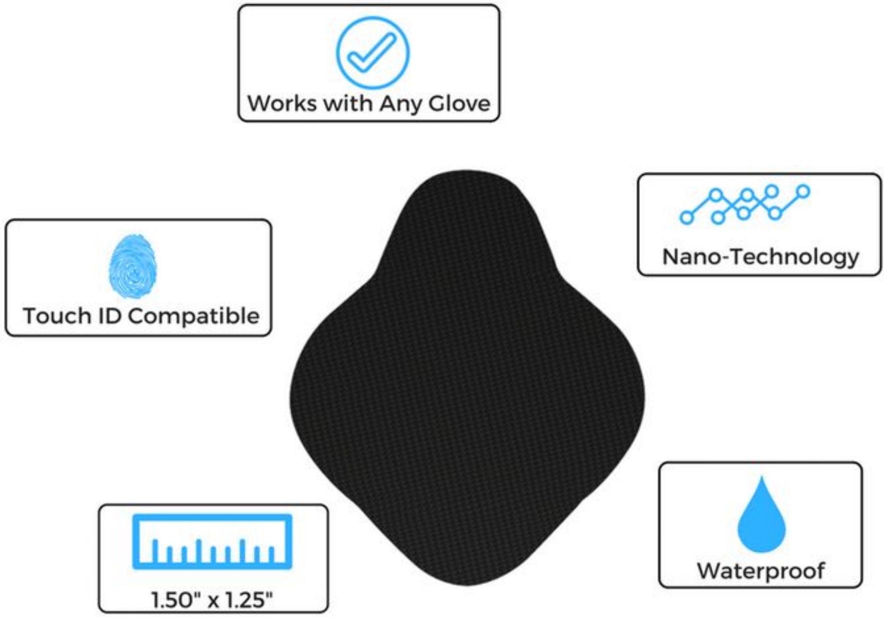
Biometrics are not secret!

And cannot be changed...

News – TAPS

- Touchscreen Sticker *with TouchID* (KickStarter)
- *Something I have* instead of *something I am*

Photo © 2016 TAPS Kickstarter campaign



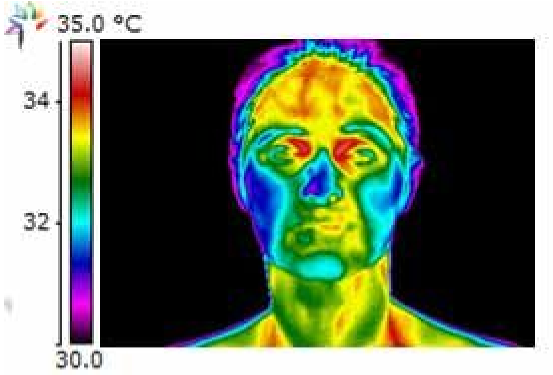
News – biometric payment authentication

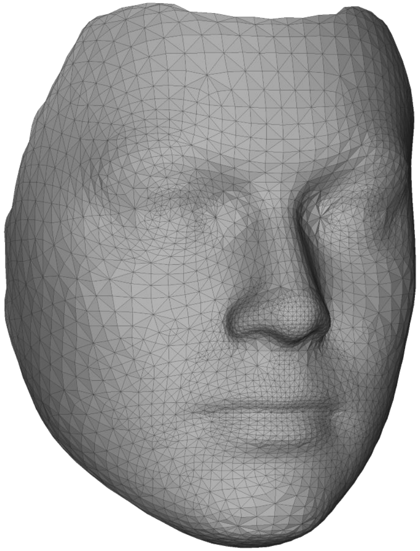
- MasterCard’s Identity Check Mobile
  - Prove holder’s identity by fingerprint/selfie
  - Blinking as liveliness testing.
  - Being introduced in 12 EU countries
  - Supported by Alibaba e-shop
- *Selfies to kill off passwords ‘in five years’*, says MasterCard.

http://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/

Input – Imaging

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

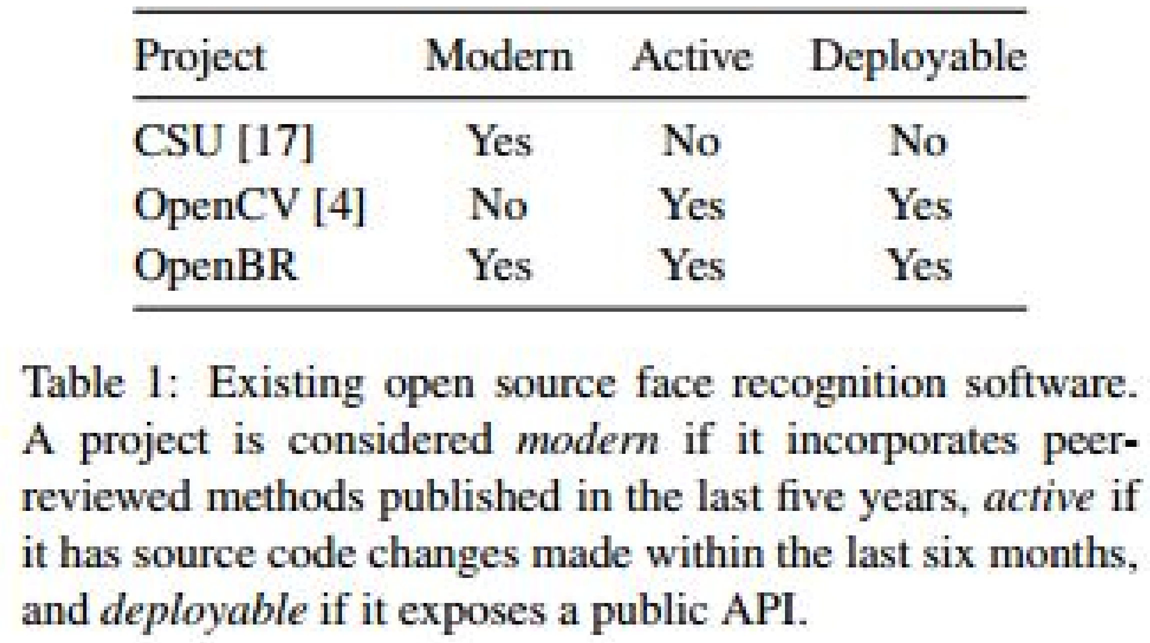




Face recognition

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

Open source frameworks



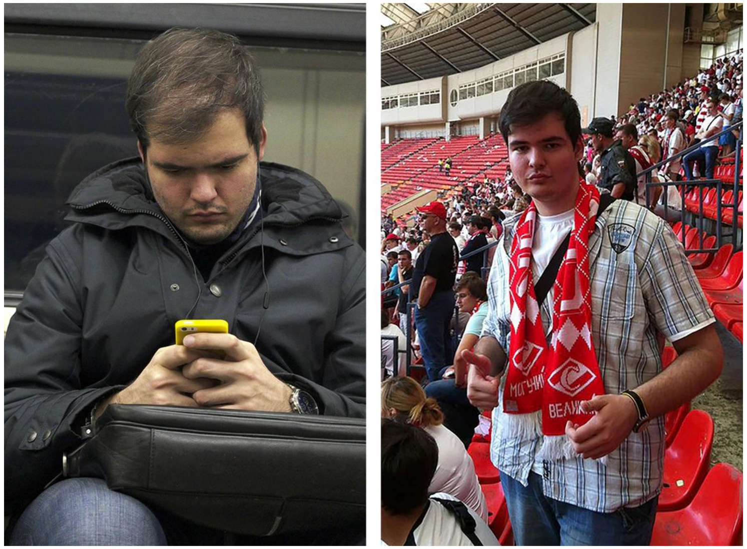
Project	Modern	Active	Deployable
CSU [17]	Yes	No	No
OpenCV [4]	No	Yes	Yes
OpenBR	Yes	Yes	Yes

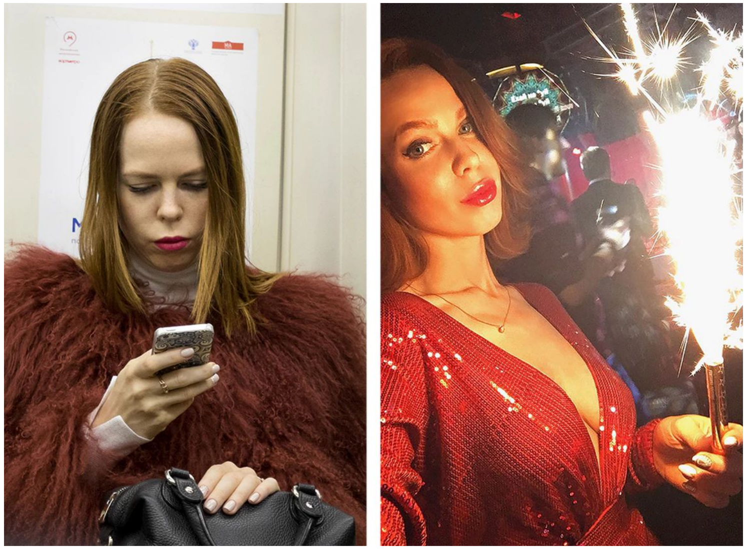
Table 1: Existing open source face recognition software. A project is considered *modern* if it incorporates peer-reviewed methods published in the last five years, *active* if it has source code changes made within the last six months, and *deployable* if it exposes a public API.

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

Left - photo from subway, right photo from VK

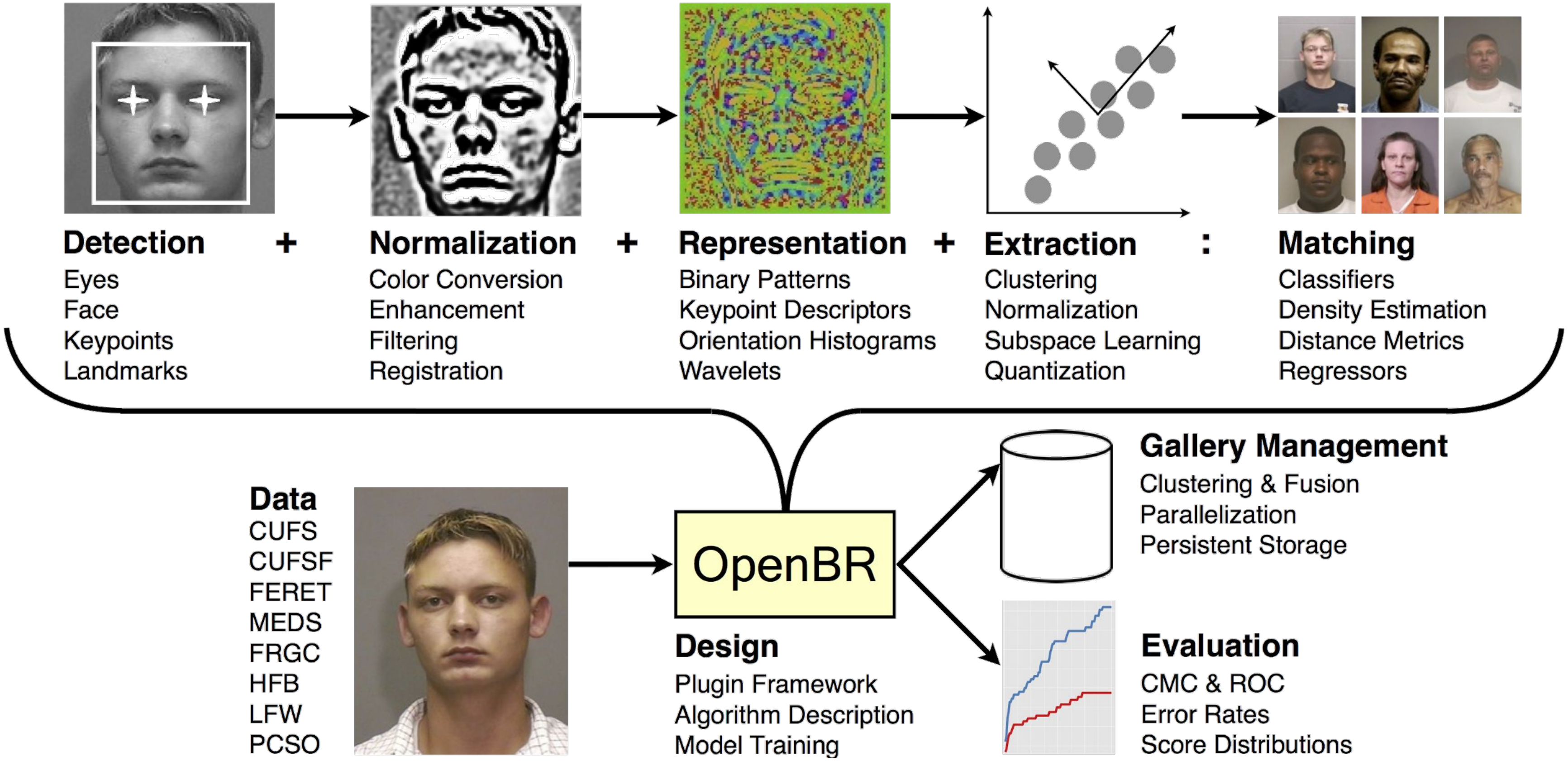




Challenges in face recognition

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

OpenBR: Face recognition overview



Detection + **Normalization** + **Representation** + **Extraction** : **Matching**

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

Photo © 2016 openbiometrics.org

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: https://vimeo.com/12774628

CV Dazzle: Anti face-detection

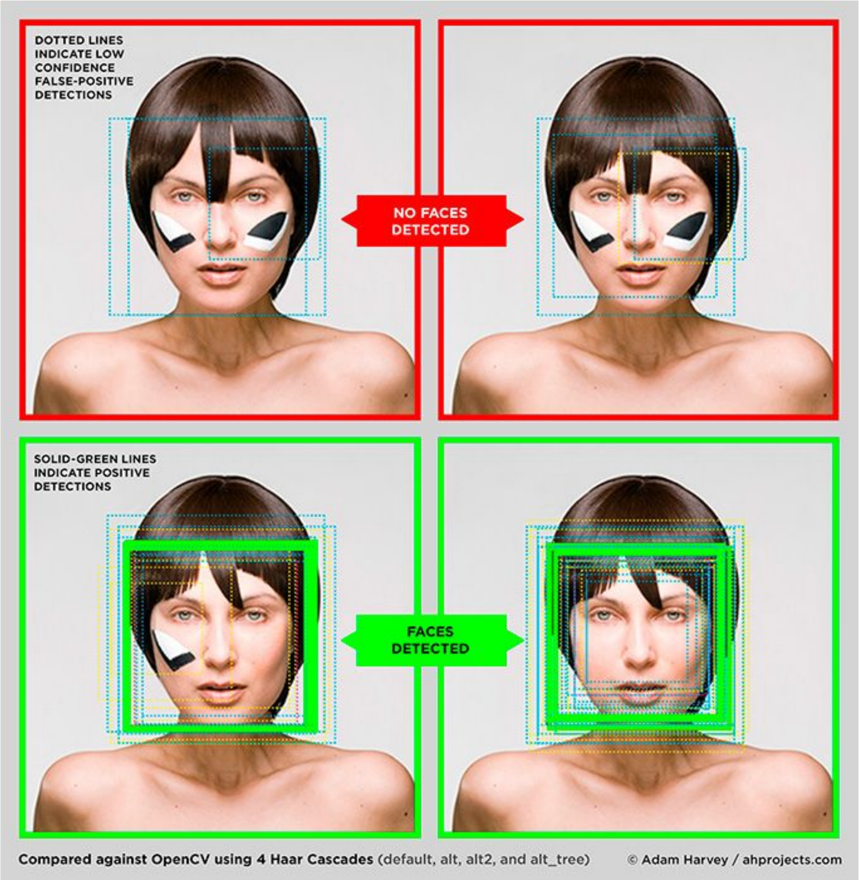

DOTTED LINES INDICATE LOW CONFIDENCE FALSE-POSITIVE DETECTIONS
NO FACES DETECTED
SOLID-GREEN LINES INDICATE POSITIVE DETECTIONS
FACES DETECTED
Compared against OpenCV using 4 Haar Cascades (default, alt, alt2, and alt_tree)
© Adam Harvey / ahprojects.com

Photo © 2010-2016 Adam Harvey, CV Dazzle

CV Dazzle: Anti face-detection

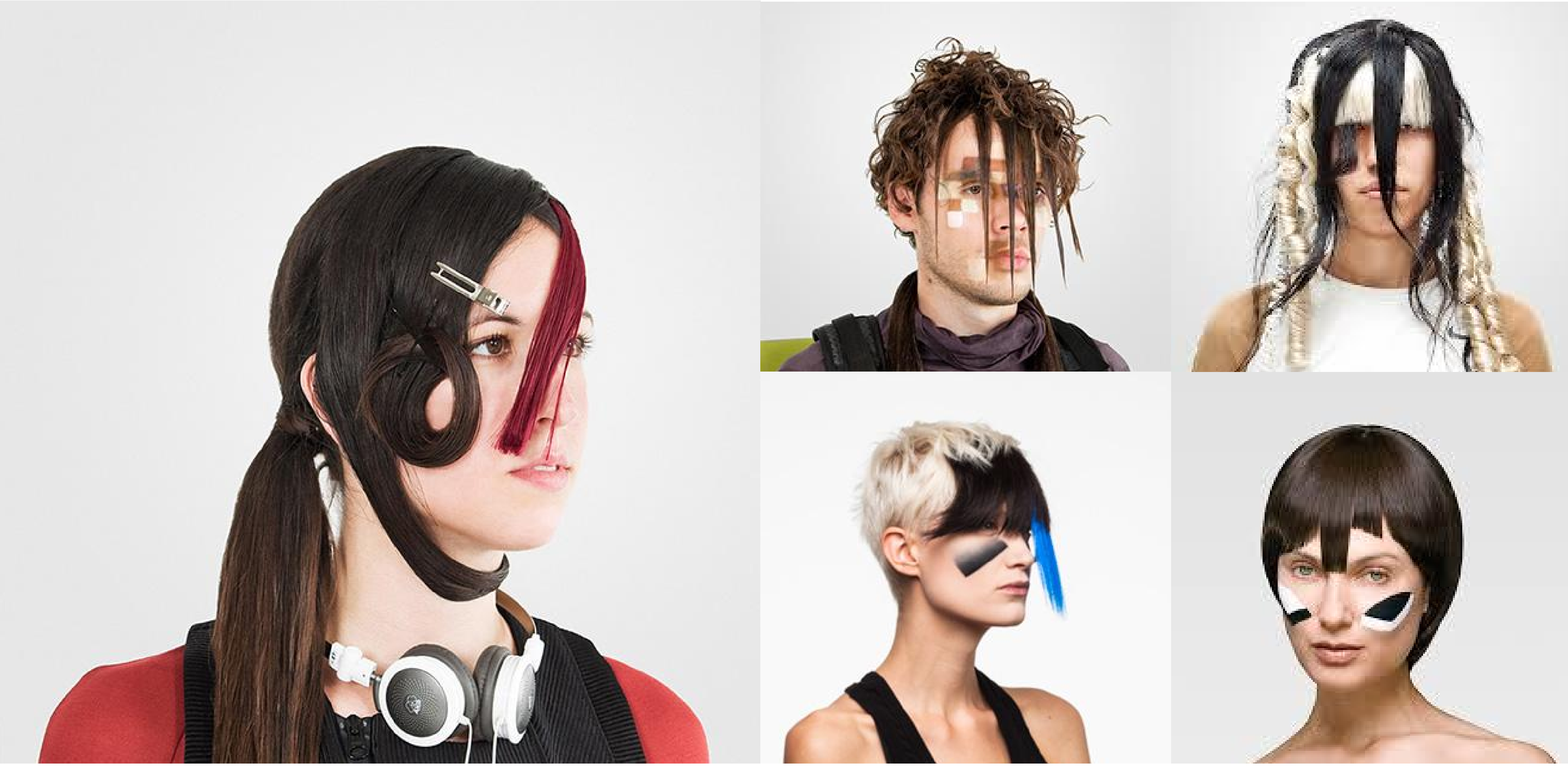


Photo © 2010-2016 Adam Harvey, CV Dazzle

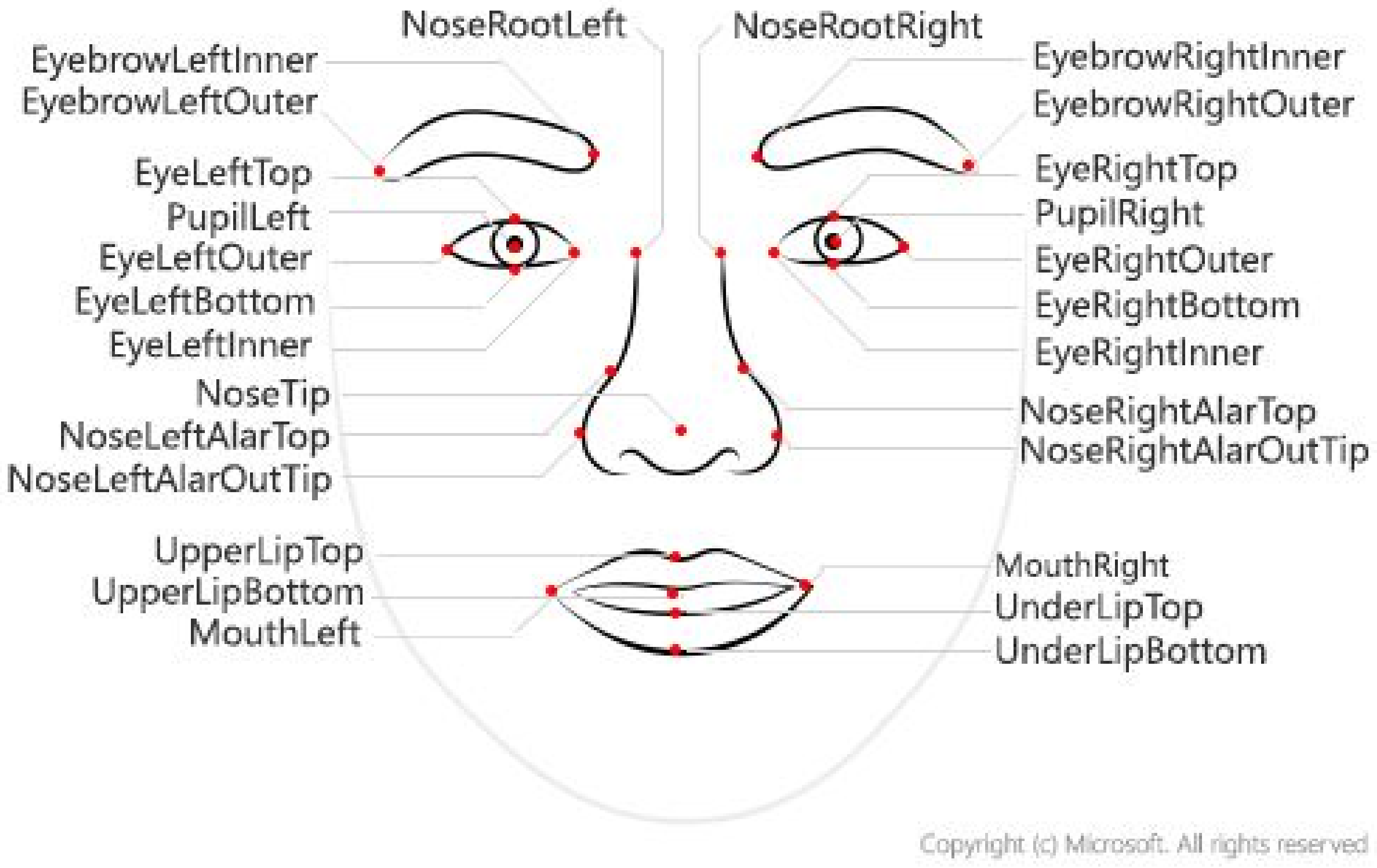
Step 2 – Normalization and Representation

- 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

- Procedure of extracting relevant information from a face image.
- Face color? Position of eyes, mouth, nose? Between eyes ratio? Width-lenght 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.

Face impersonation

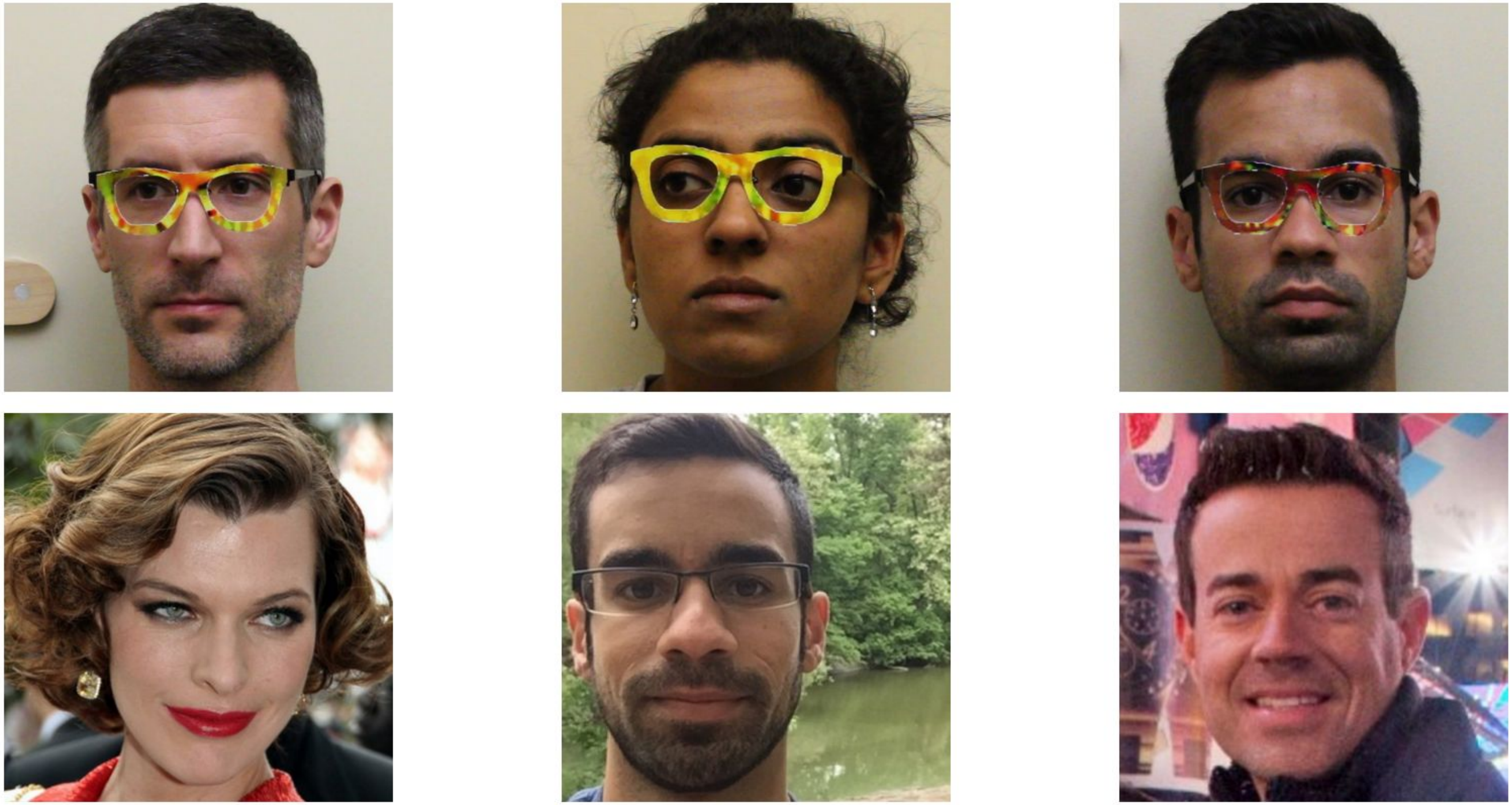


Photo © 2016 Carnegie Mellon University, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*

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"*

See more at: 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.

Output

- Confidence:
  - Euclidian distance to measure matching of pictures.
  - Interval (0,1), 0 = bad match, 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 (in the Euclidean sense) indicate higher similarity.

Testing sets (databases)

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

Duchenne de Boulogne (~1870)

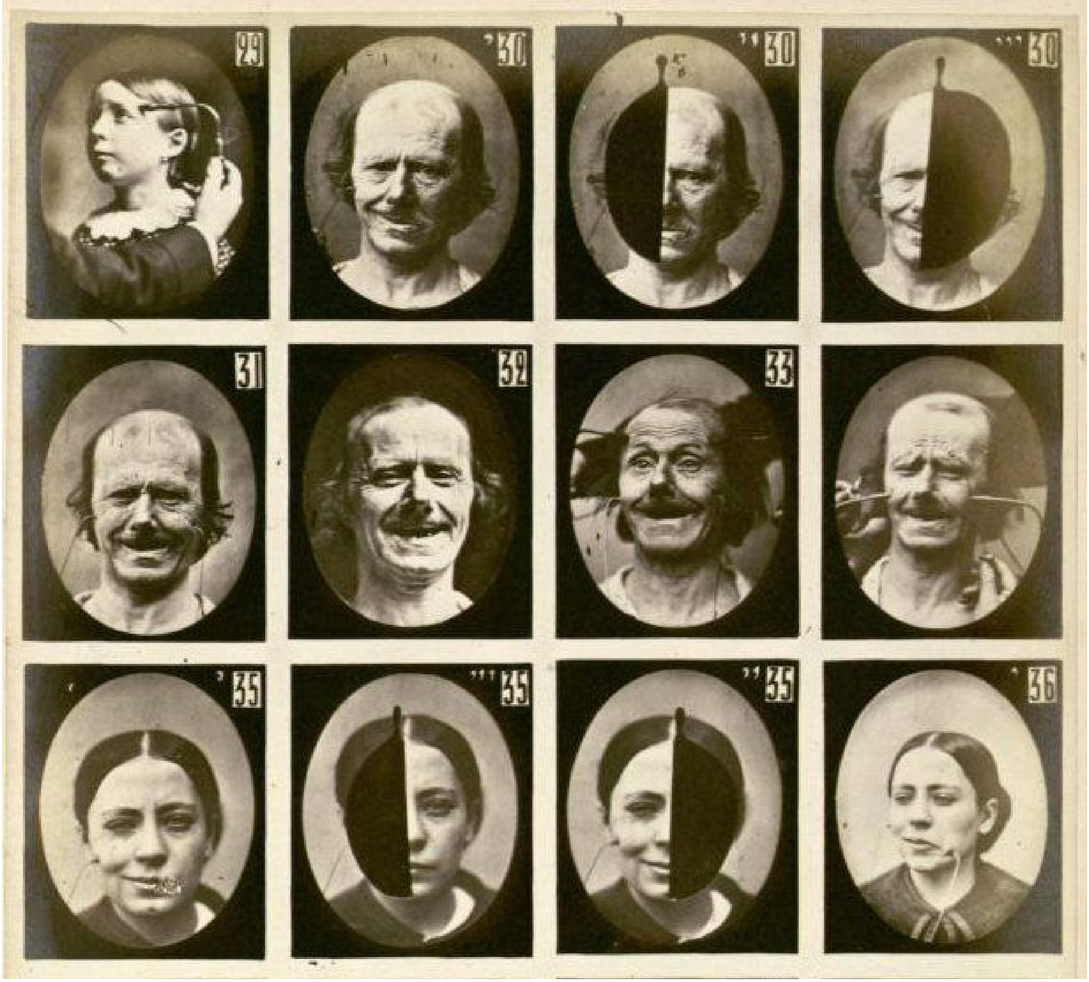


Photo in Public domain
Source: Wikipedia: Duchenne de Boulogne

Mugshots

BUDDSJD_10

CAUGHMANMD_3

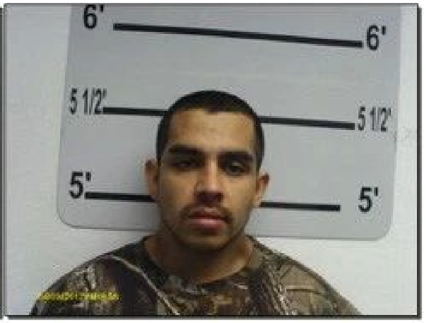
CLYMANNS_1

DELAROSAJ_2

CHEWEYSR_22

CLARKJ_6

DELOACHAM_1



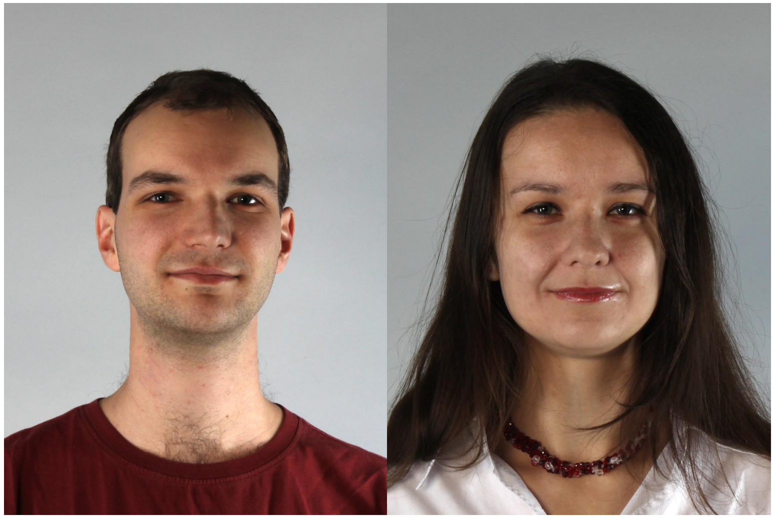
GILLEYNK_1

Fun with biometrics

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

Photo © 2016 Dominika Krejčí, InterSoB

Seminar task



- Inspect what influences face recognition In OpenBR
  - http://openbiometrics.org/
- Use faces of the teachers to experiment
  - Compare images to photoshopped versions to determine what changes matter most
  - Be creative and playful!
- Similar task with age recognition for homework

Seminar task (tips)

- What can influence identification/age estimation?
  - Distance between eyes/mouth/nose/…
  - Light/colour differences (think CV Dazzle)
  - Wrinkles, hair style, general “smoothness”
  - “Transplanting” eyes/parts of other faces
- What is necessary to avoid face detection completely?
  - Deleting/covering an eye/mouth/…
  - Multiple eyes/mouths/...
  - Colour changes, wrong distance ratios

Seminar task (examples)

OpenBR invocation (prepared VM)

- Face recognition/comparison

```
br -algorithm FaceRecognition -compare me.jpg you.jpg
```

Approximately: similarity < 2 is different people, similarity > 3 is the same person

- Age estimation

```
br -algorithm AgeEstimation -enroll me.jpg meta.csv
cat meta.csv
```

- Gender estimation

```
br -algorithm GenderEstimation -enroll me.jpg meta.csv
cat meta.csv
```

- Documentation

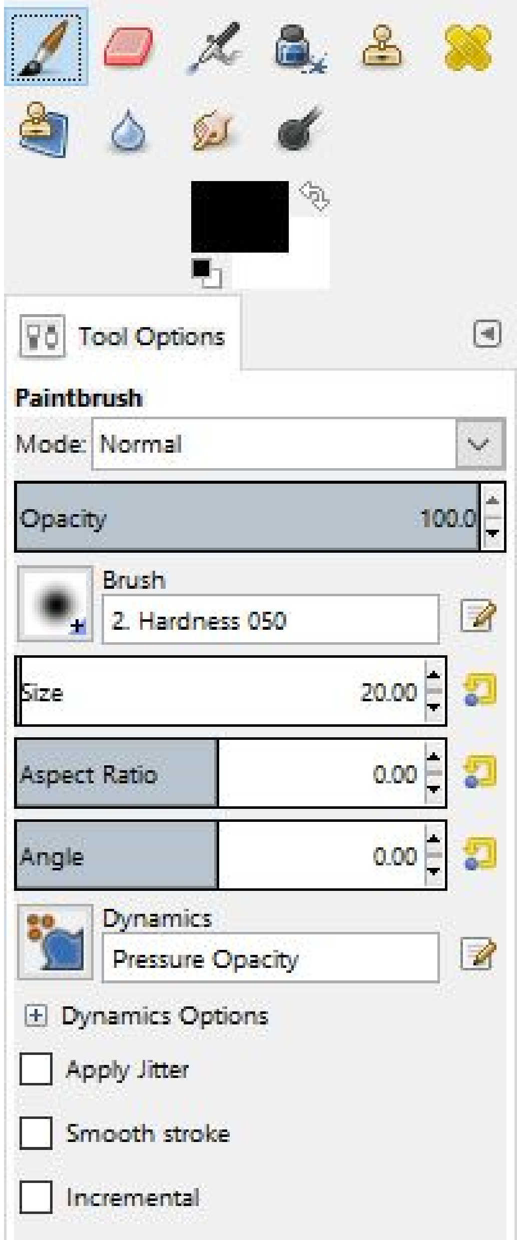
http://openbiometrics.org/docs/tutorials/#face-recognition

Prepared VM (details)

- .ova file at O:\pv181\pv181-biometrics1
- Import PV181-biometrics1.ova to VirtualBox
  - Import appliance (don’t create a new machine)
- Boot the system
  - Ubuntu 16.04
  - Login: ‘vagrant’, Password: ‘vagrant’
  - Everything necessary is already installed
  - You are sudo, in case you want to add something
- It’s build with Vagrant
  - Vagrantfile available in study materials, if interested

GIMP basics

- Paintbrush tool
  - Shape, opacity, size
  - Mode (normal, darken, saturation, ...)
- Clone tool
  - Select source with Ctrl
- Smudge tool
- Others as you see fit...
- You may want single-window mode
  - Windows > Single-Window Mode



Tool Options

Paintbrush

Mode: Normal

Opacity 100.0

Brush: 2. Hardness 050

Size 20.00

Aspect Ratio 0.00

Angle 0.00

Dynamics: Pressure Opacity

⊞ Dynamics Options

□ Apply Jitter

□ Smooth stroke

□ Incremental

Homework

- Investigate what influences age estimation
  - In https://how-old.net/ (neural-networks based)
  - Photoshop our pictures
- Write a summarizing report
  - What works, what does not, is it general behaviour?
  - At least 5 distinct features
  - Any other interesting findings?
- Submit to homework vault
  - Report (PDF/TXT)
  - Archive of photoshopped images illustrating findings
- Due date: 12. 12. 23:59