Biometrics 2
Face recognition

PV181 Laboratory of security and applied cryptography
Seminar 8. 12. 2021

Agáta Kružíková, kruzikova@mail.muni.cz
Katarína Galanská, xgalansk@fi.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. Fake fingerprints
   - Completion
2. Face recognition
3. Seminar activity
   - Hypotheses
4. Homework
   - Face detection

Fingerprint experiment

Completion

Fingerprints Completion

- Scan your genuine and fake fingerprints
  - In case of the bonus task do not forget to scan the fake without Gabor filtering it too!
- You will receive the scans in your Depository in IS
- Process the scans with NBIS software
- Try to “hack” your own smartphone

Preparation for post processing

- You will receive scans of your fingers
- Prepare the image for post processing
  - 8-bit grayscale raster
  - width at least 512 pixels
  - height at least 480 pixels
  - .png format

Fingerprints post processing

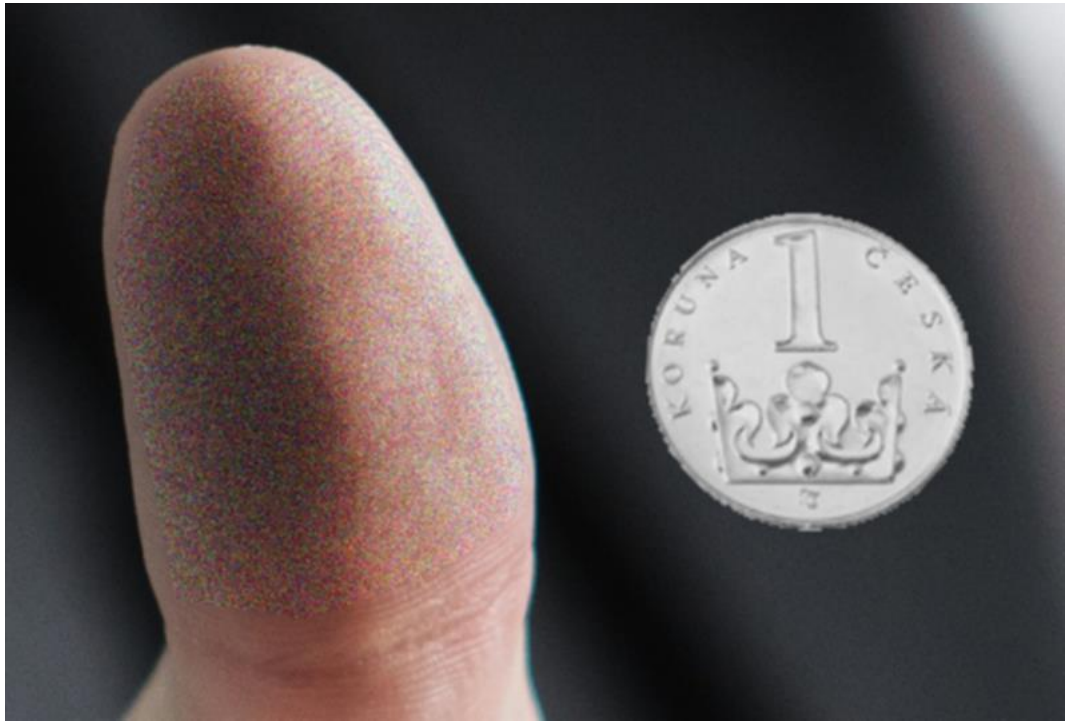
- Use NIST Biometric Image Software (NBIS)
  - It is preinstalled on lab PC in the within Ubuntu VM
- Create a minutia map in .xyt format (Mindtct)
  - /opt/nbis/bin>./mindtct -m1 <fingerprint_scan_from_reader.png> <new_name_of_fingerprint_in_xyt_format>
- Check quality of the fingerprint (Nfig)
  - /opt/nbis/bin>./nfiq -d <fingerprint_scan_from_reader.png>
  - Output: 1-5 where 1-best, 5-worst
- Check the number of identified minituas in .min file

Fingerprints post processing

- Repeat it for all fingerprint inputs which you scanned via reader
- Compare fake and real fingerprints (Bozoroth3)
  - Score above 40 means true match (“rule of thumb”)
  - /opt/nbis/bin>./bozorth3 <fake.xyt> <original.xyt>
- Bonus task: compare the real fingerprint to fake without Gabor filters
- Open the questionnaire and fill in the data from your observations
  - Mandatory for all, only the research questions are not

Help with future fingerprint image processing

1. Open your image in ImageJ.
2. Select your fingerprint with polygon selection.
3. Process → Noice → Add Noice
4. Save as → .png
5. Upload to: https://is.muni.cz/auth/el/fi/podzim2021/PV181/ode/121202412/



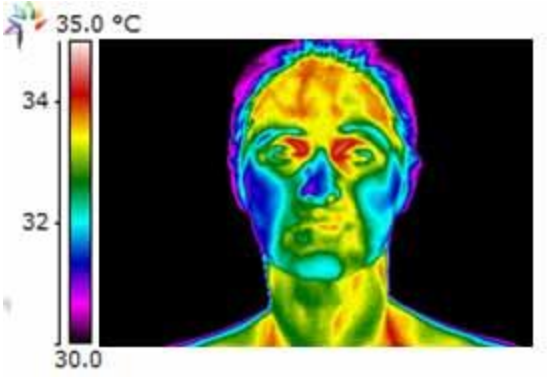
Face recognition

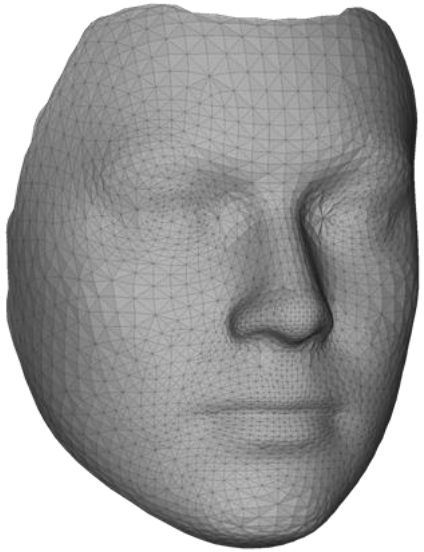
Theory and examples

Real-life example

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, ...

New 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

Face recognition overview (OpenFace)

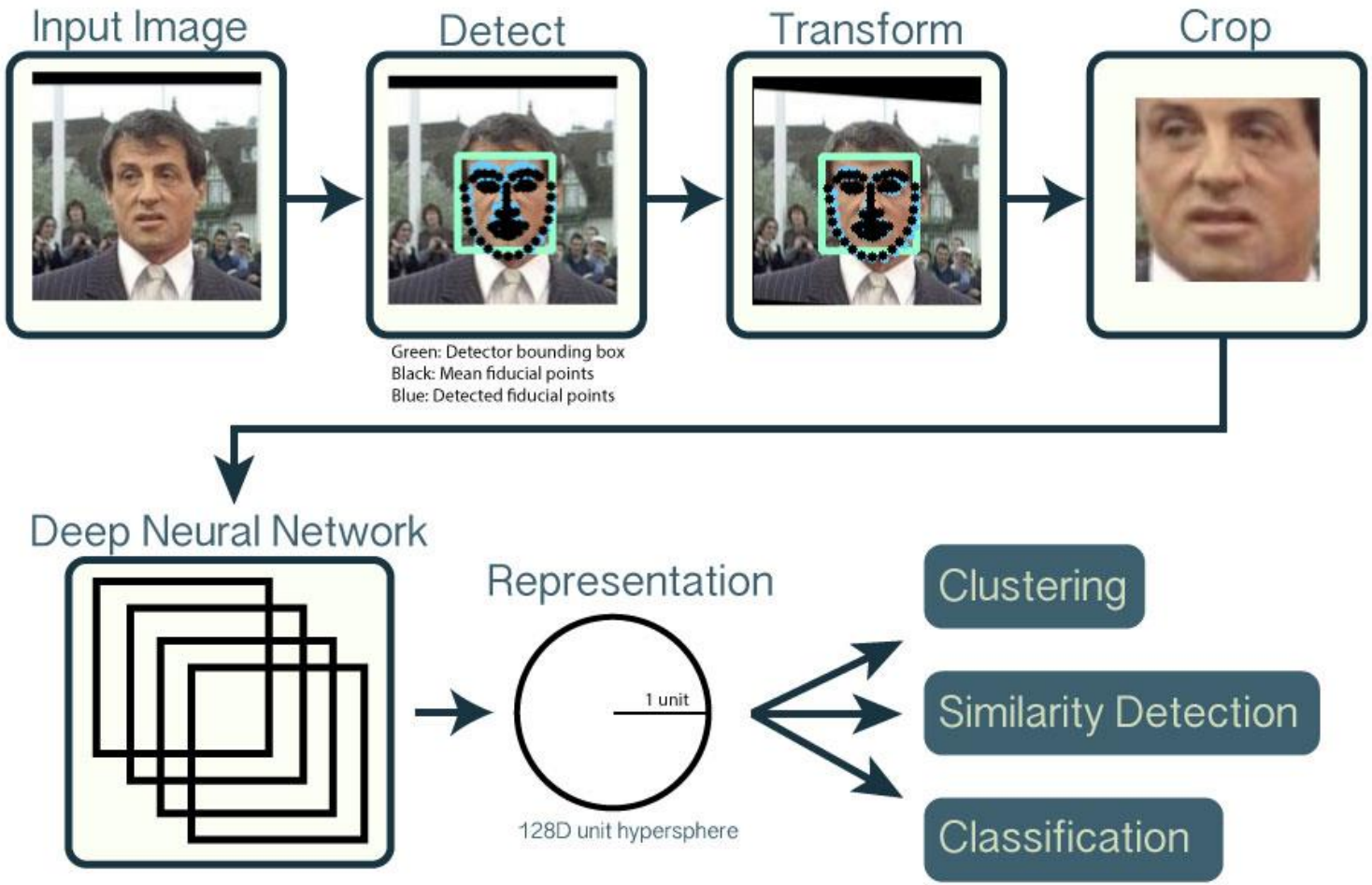
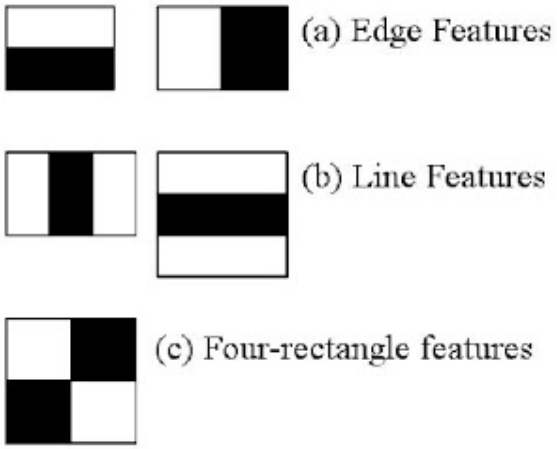
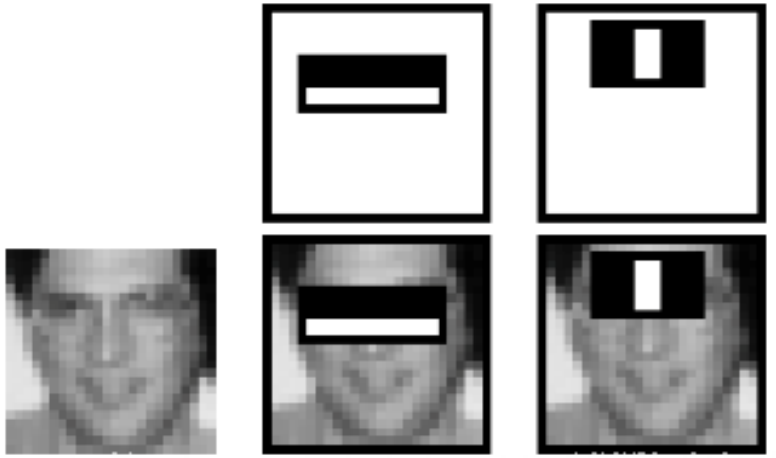


Photo © The OpenFace project, cmusatyalab.github.io/openface

Face detection: Haar cascades

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



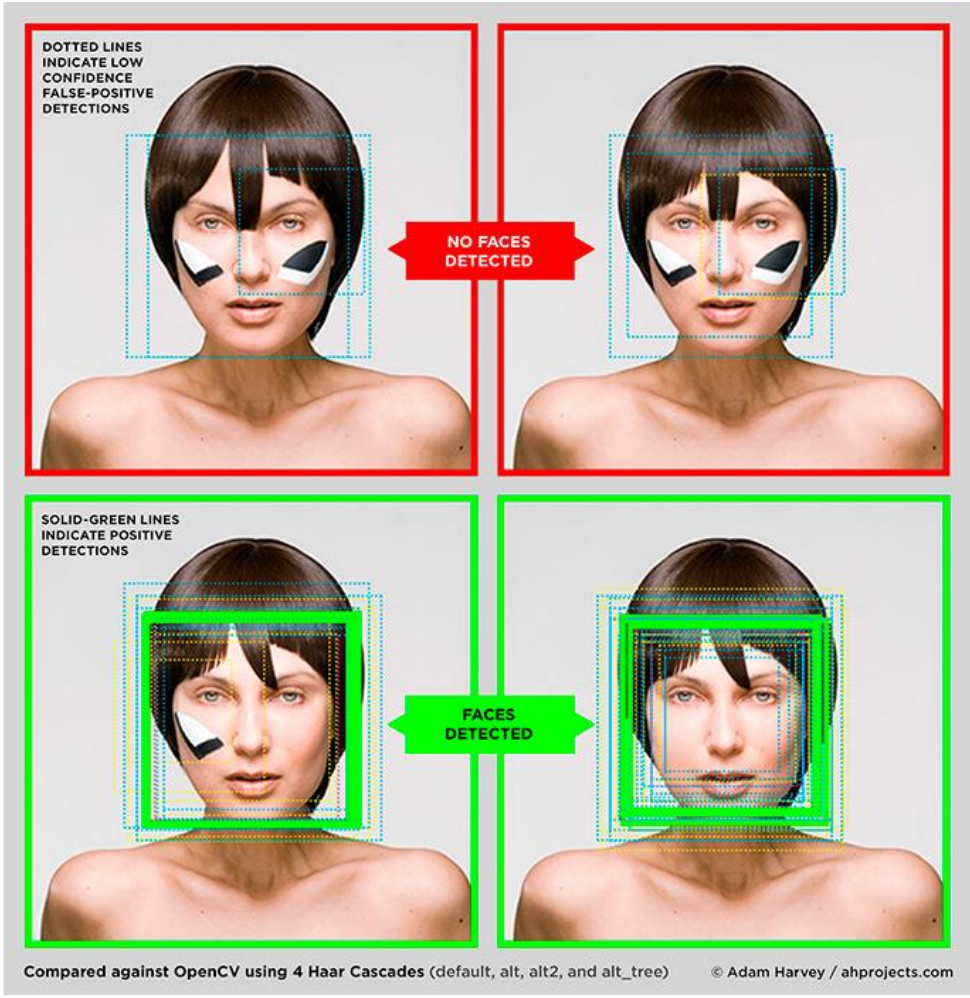


Face detection: Haar cascades

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

CV Dazzle: Anti face-detection

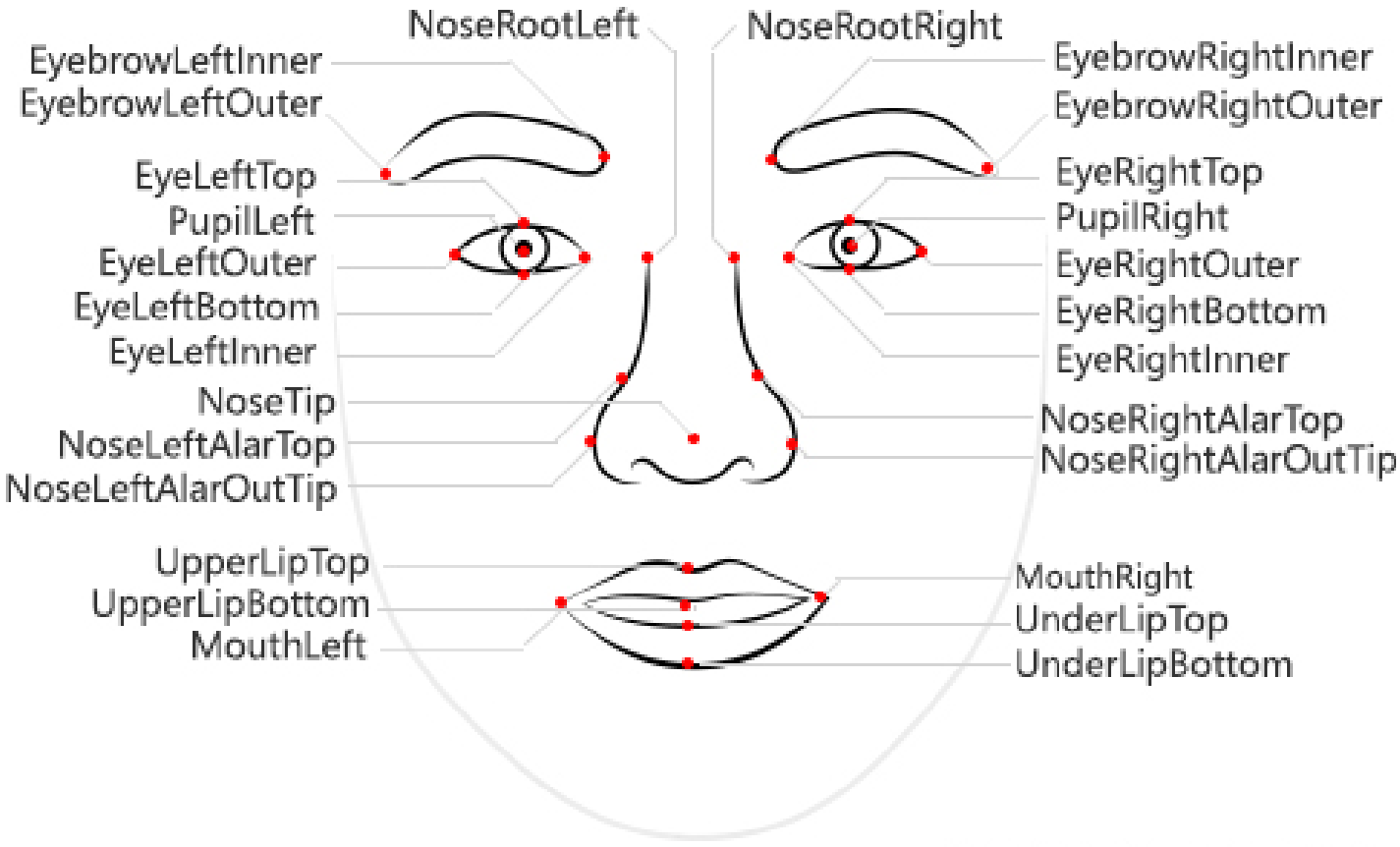
Photo © 2010-2016 Adam Harvey, CV Dazzle



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

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

KFC AliPay

Face impersonation

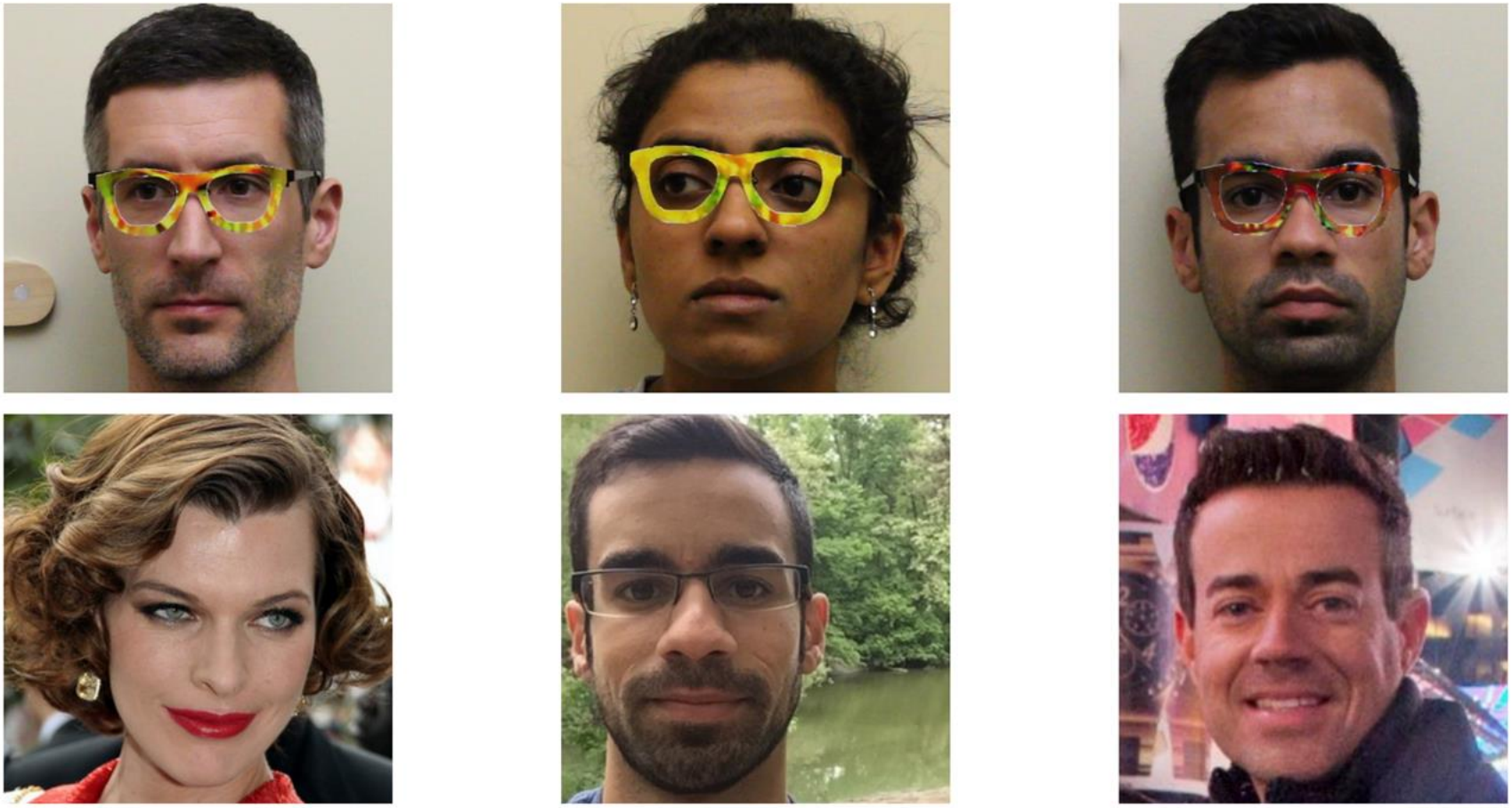


Photo © 2016 Carnegie Mellon University, *Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition*

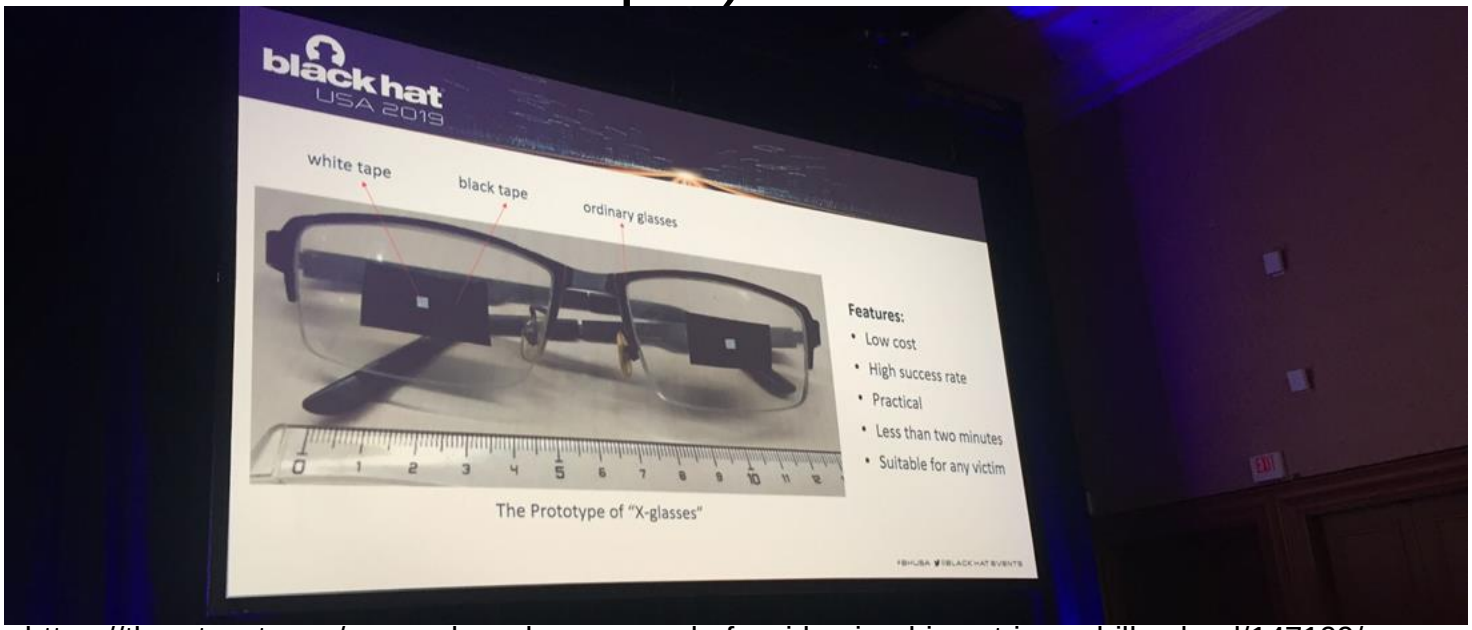
Face impersonation

- 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.

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/

Detecting sexual orientation from faces

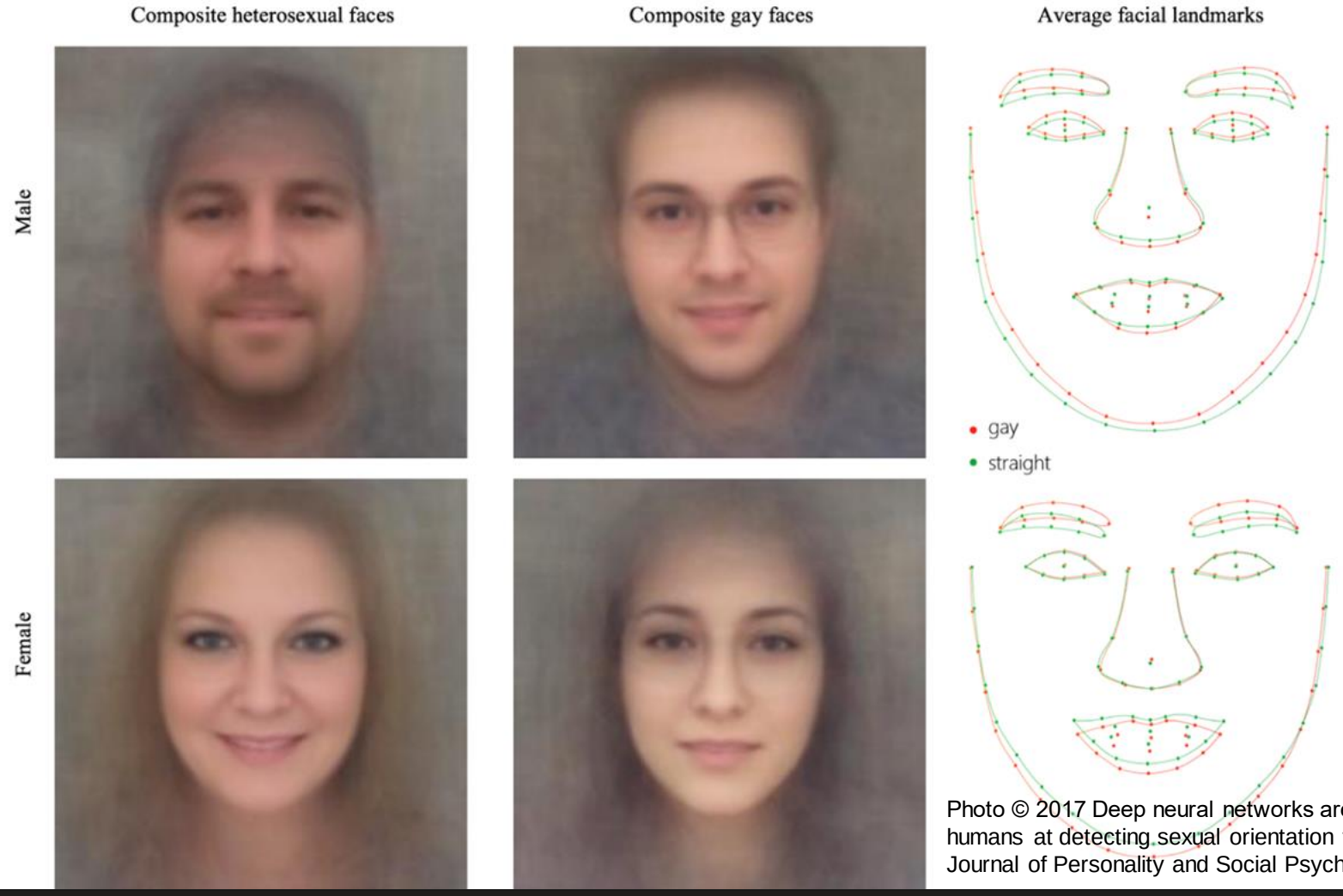


Photo © 2017 Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology

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

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: 15. 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. PV080 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 PV080 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!
- Have a look at old homework submission with good methodology in the Study Materials.
  - Special thanks to Vladimír Bouček for providing it.