The challenge of Morphing for border control

[redacted]

Biometric System Laboratory - University of Bologna (Italy)

International Conference on Biometrics for Borders

Warsaw – 09-10 October 2019

Outline

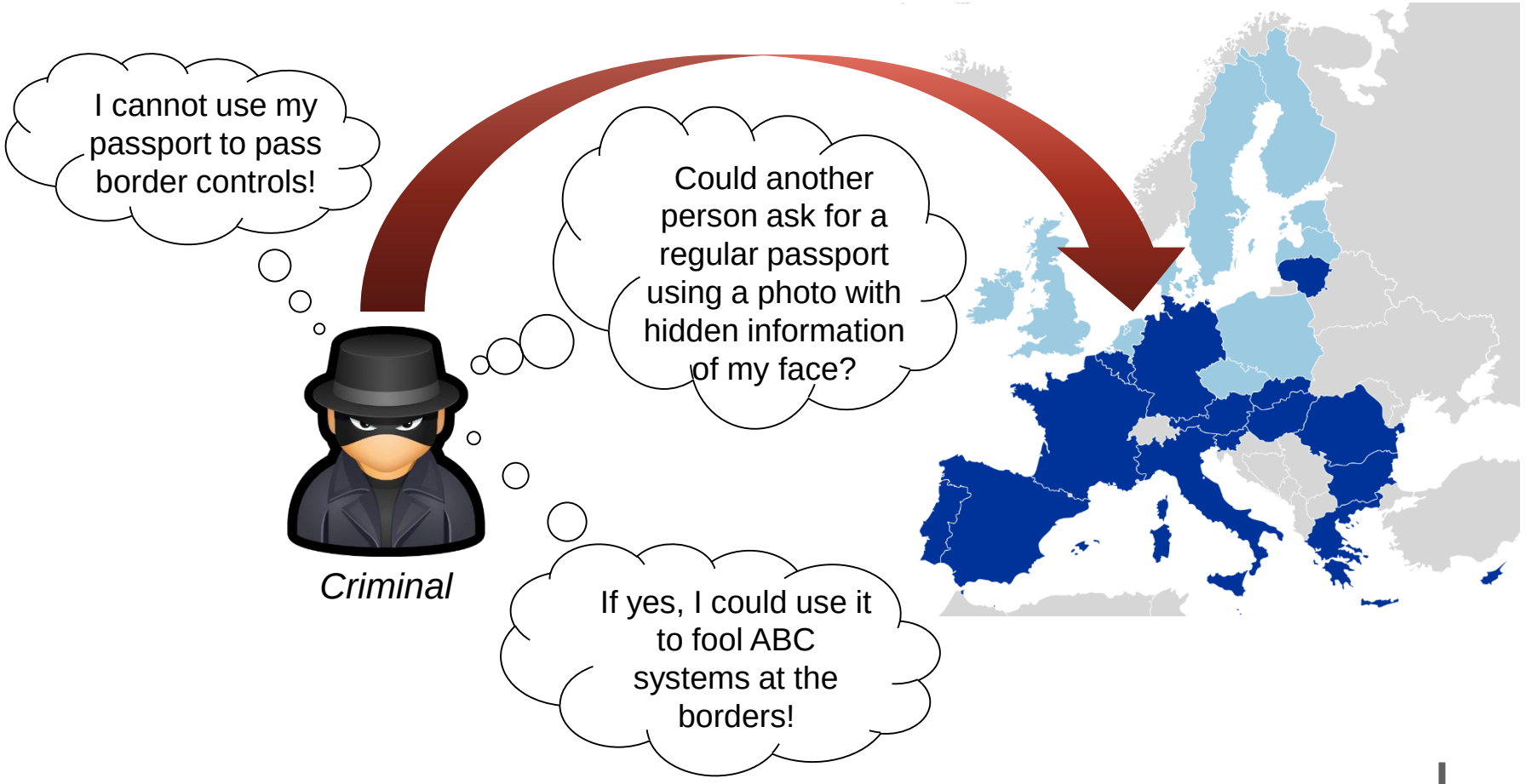
- What is morphing?
- The morphing attack
  - The idea
  - The morphing factor α
  - A real case
- Automatic morphing detection
  - Application scenarios
  - Different solutions
  - Open issues
- Conclusions

What is morphing?

“In computer graphics and animations, morphing is a special effect that transforms an image into another through a seamless transition”

https://noahmjacobs.com/computer-vision/face-morphing/

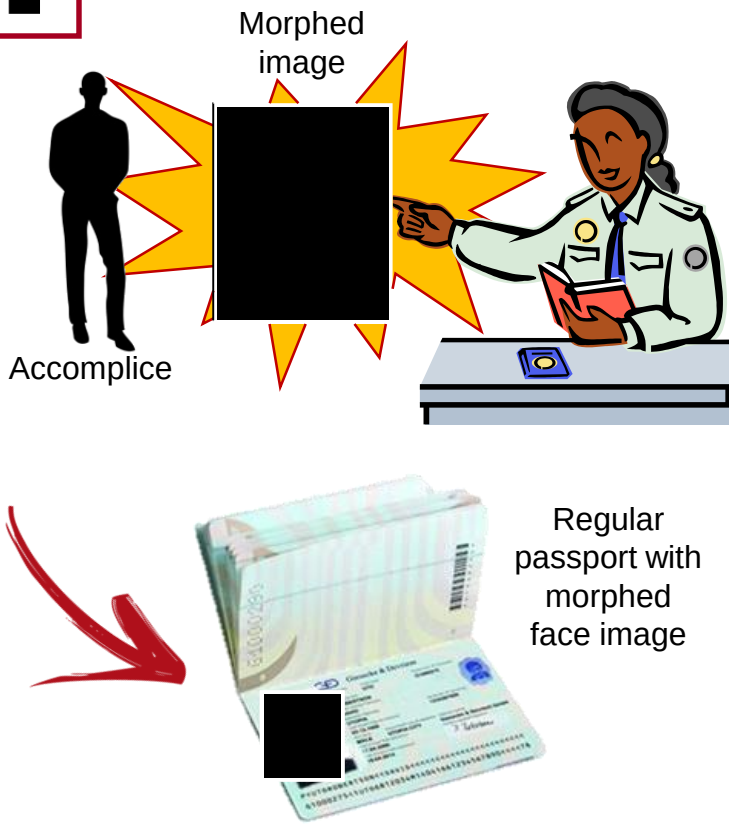
The morphing attack



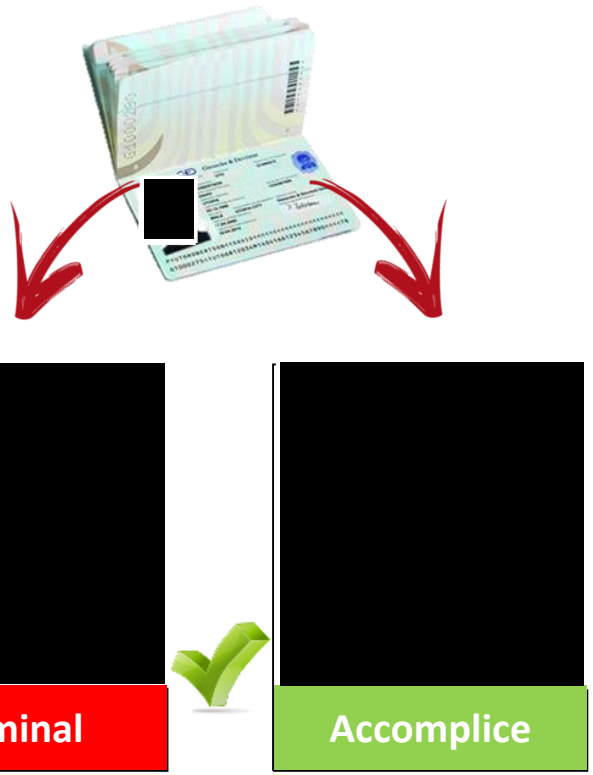
The morphing attack (2)

If a double-identity face image can be enrolled in the chip, two subjects can share the document

Passport Issuance



ABC Verification

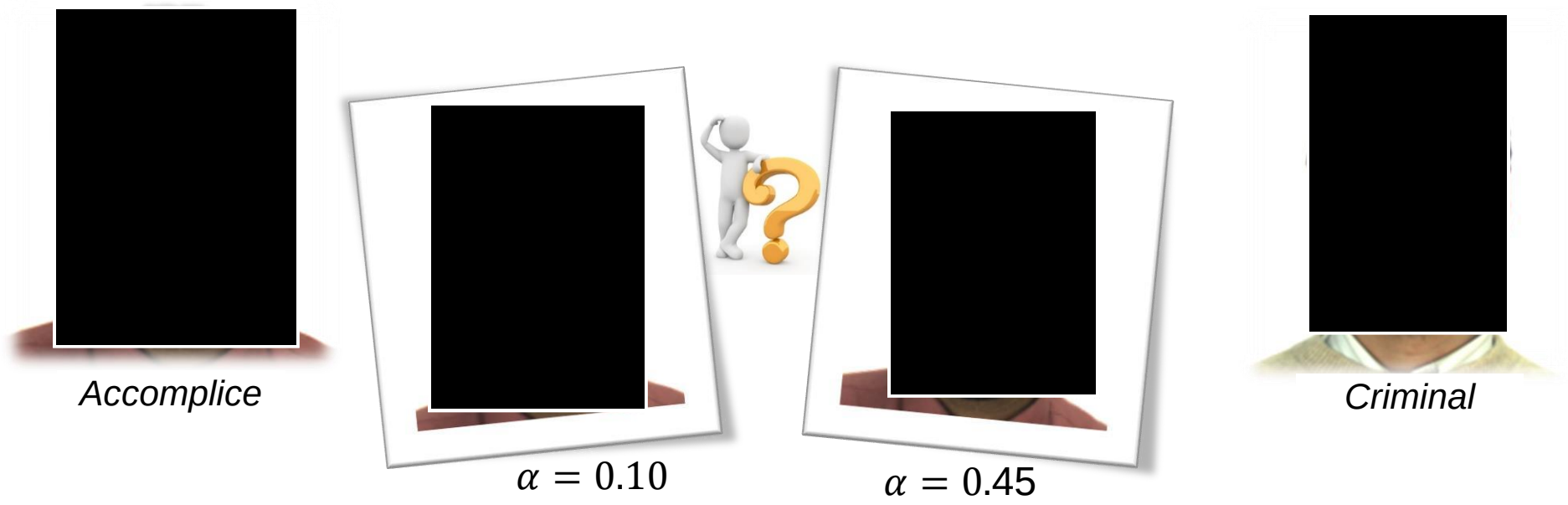


The morphing attack (3)

- The issued document is perfectly regular.
- The attack does not consist of altering the document content but in deceiving the officer during document issuing. For this reason the morphed photo ID must be **very similar to the applicant**.
- The document released will thus pass all the integrity checks performed at the gates.
- It has been proved that:

1. It is possible to create a realistic morphed image;
2. The morphed image is able to deceive the officer;
3. State-of-the-art face recognition algorithms can be easily fooled.

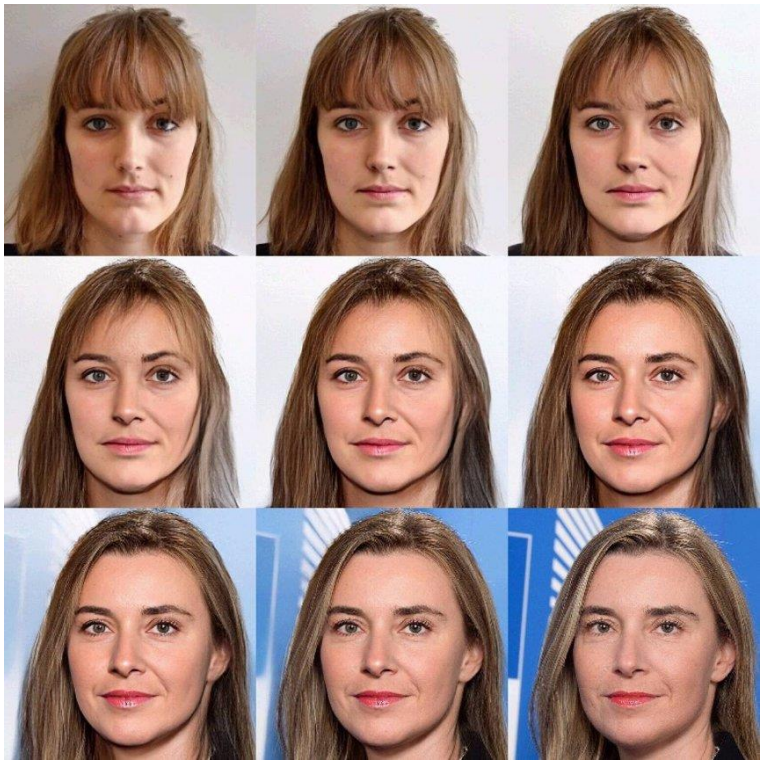
The morphing factor α



- The morphing factor α represents the percentage of criminal characteristics hidden in the morphed image.
- The value of α should be chosen to maximizes the probability of fooling both the *officer* during enrollment and the *automatic face recognition system* at the gate.
- Based on literature results and tests with human experts, α values in the range 20%→30% are considered a good trade-off.

A real case

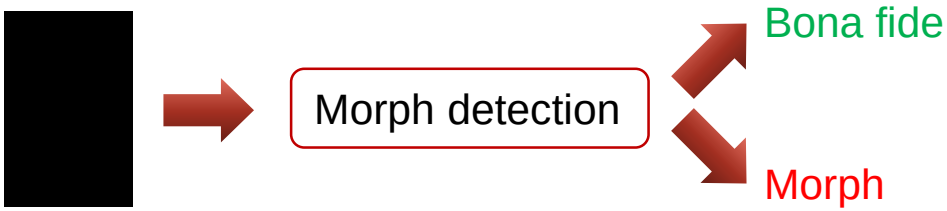
On October 2018, German activists used a morphed image of Federica Mogherini (High Representative of the European Union for Foreign Affairs and Security Policy) and a member of their group to get a genuine German passport.



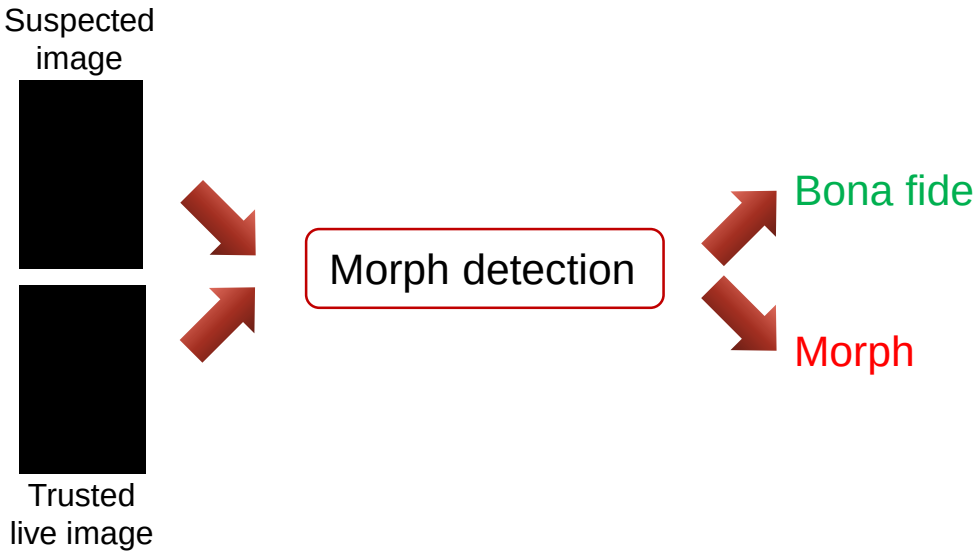
Automatic morphing detection

Two scenarios:

- Single image – an algorithm should be able to classify a face image as morphed or not.



- Differential image – a second image (e.g., captured live at the gate) is available to help deciding if the suspected image is morphed or not.



Automatic morphing detection (2)

Different solutions have been proposed based on:

- Micro-Texture analysis using different features (e.g., LBP, SURF, etc.);
- Topological analysis of facial landmarks;
- Deep learning techniques;
- Reverse the morphing process (also called Demorphing).

The results are encouraging but still far to be acceptable. This is mainly due to the following issues:

- Intra-subject variations are stronger than those introduced by morphing;
- Printed & scanned images;
- Lack of public databases.

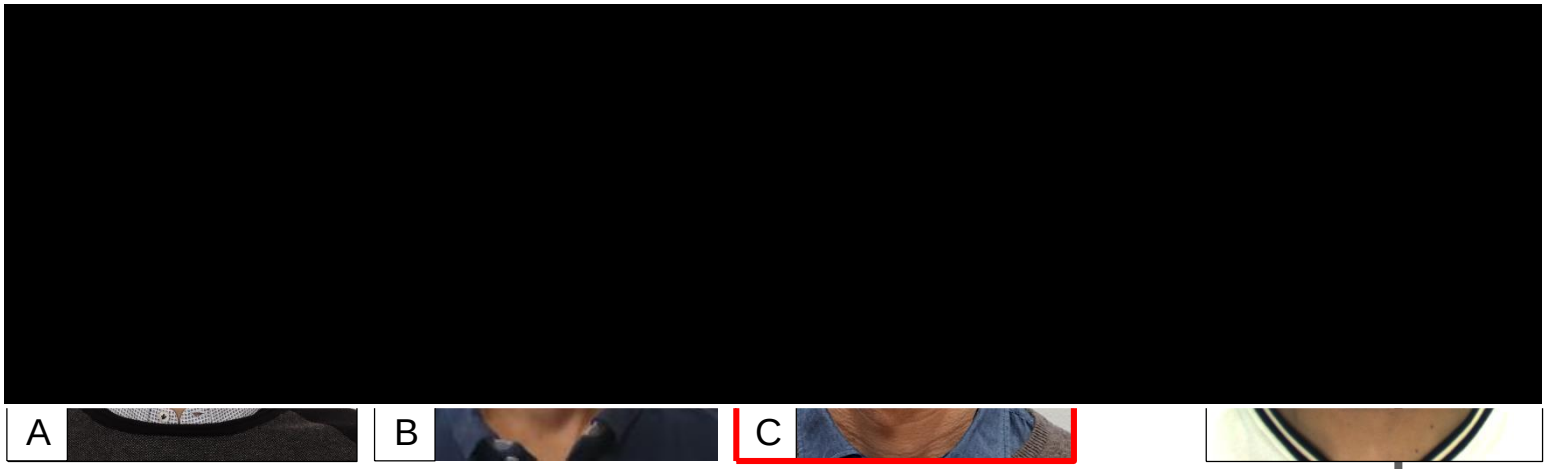
Intra-subject vs morphing variations

Beard and Hair style

Makeup

Aging

Which is the morphed image?



Printed & scanned images

Lack of public databases

To develop effective morphing detection systems, thousand high quality morphed images generated using different morphing techniques are needed.

About 20 minutes are needed to create a single high quality morphed image. Even more for printed & scanned images.

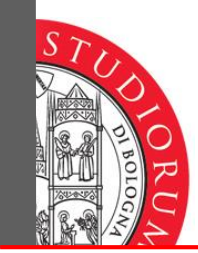
Morphed images cannot be shared between different research groups because of privacy issues.

Each research group creates its own private database containing only few hundreds high quality morphed images generated using a single morphing technique.

The morphing detection methods are not able to detect morphed images created using a different morphing process: small changes in the morphed images produce high degradation in the detection performance.

Conclusions

- Morphing attack is today a real security threat.
- The best solution is live enrolment, but to be effective, should be adopted by all countries.
- Detection techniques are being studied (with interesting but not satisfactory results).
- There are several open issues to be solved (e.g., different morphing techniques, different conditions, P&S images).
- Common benchmarks and evaluations needed:
  - NIST Face recognition Vendor Test (FRVT) MORPH
  - SOTAMD (State Of The Art Morph Detection) EU project



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

[redacted]

Department of Computer Science and Engineering
University of Bologna

[redacted]

Biometric System Laboratory
biolab.csr.unibo.it

[redacted]