The challenge of Morphing for border control

Matteo Ferrara and Annalisa Franco

Biometric System Laboratory - University of Bologna (Italy)

Workshop

Human-centered Vision: from Body Analysis to Learning and Language

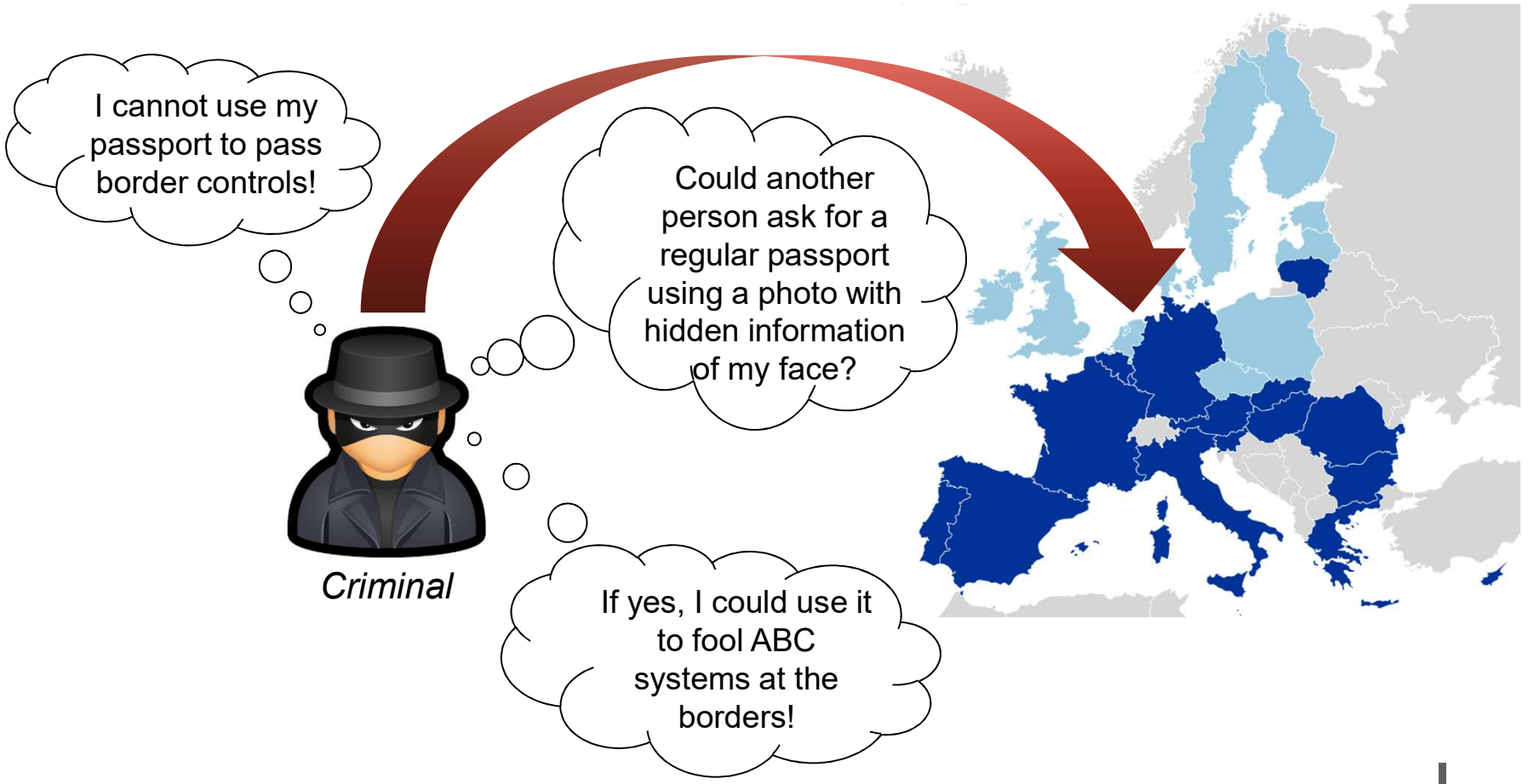
09 July 2020

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/

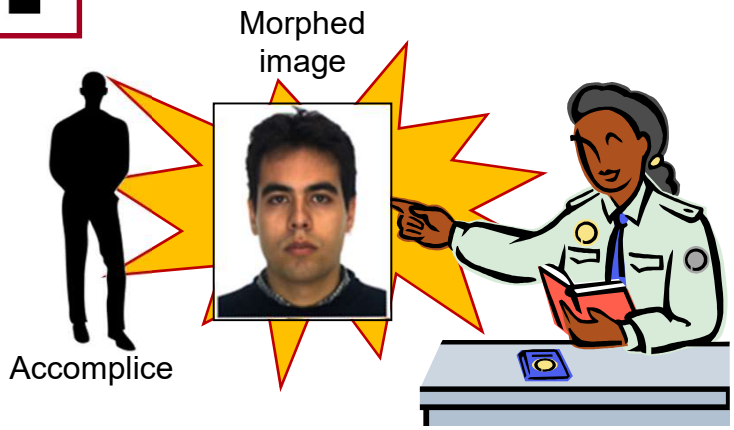
The morphing attack



The morphing attack (2)

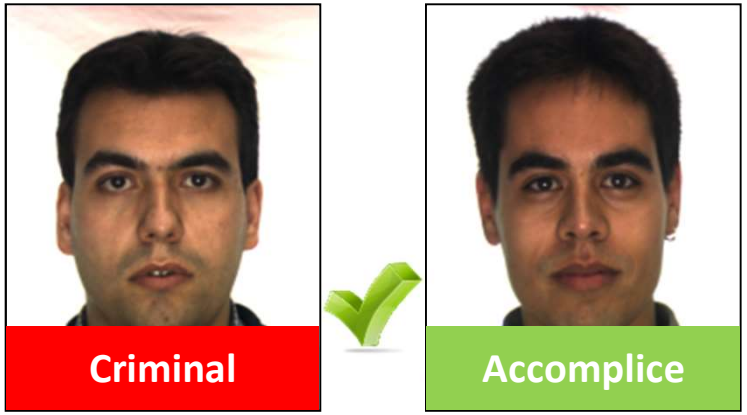
If a double-identity face image can be enrolled in the chip, two subjects can share the document

Passport Issuance



Regular passport with morphed face image

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.

Face recognition failures

Morphing (document image)

Criminal (at the gate)

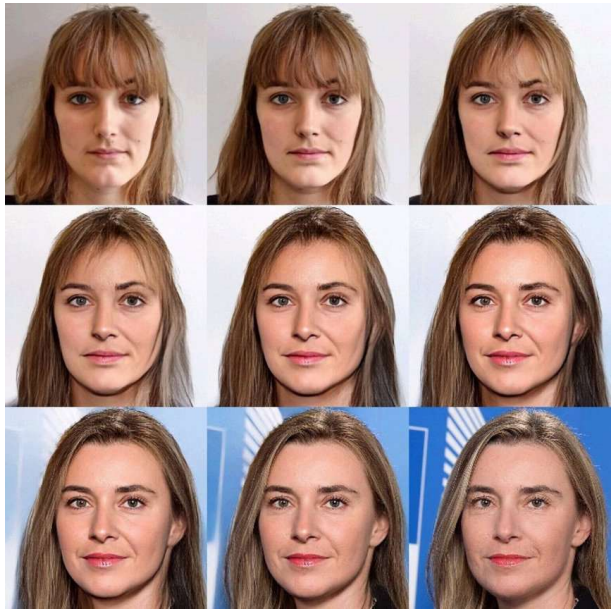
Face recognition failures (2)

Morphing (document image)

Criminal (at the gate)

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.



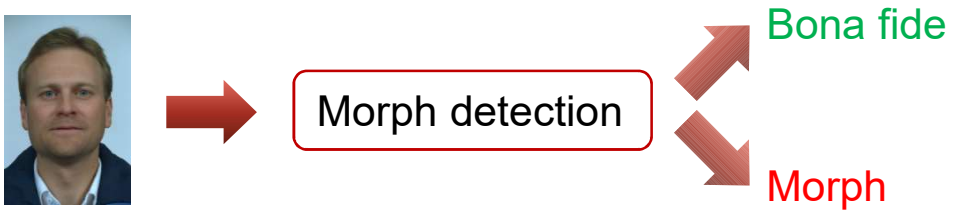
The same group declared they are sending "magic" passports to Libya, to help immigrants entering Europe borders.

http://www.spiegel.de/netzwelt/netzpolitik/bild-1229418-1342122.html
https://pen.gg/campaign/mask-id-2/
https://mask.id/en/

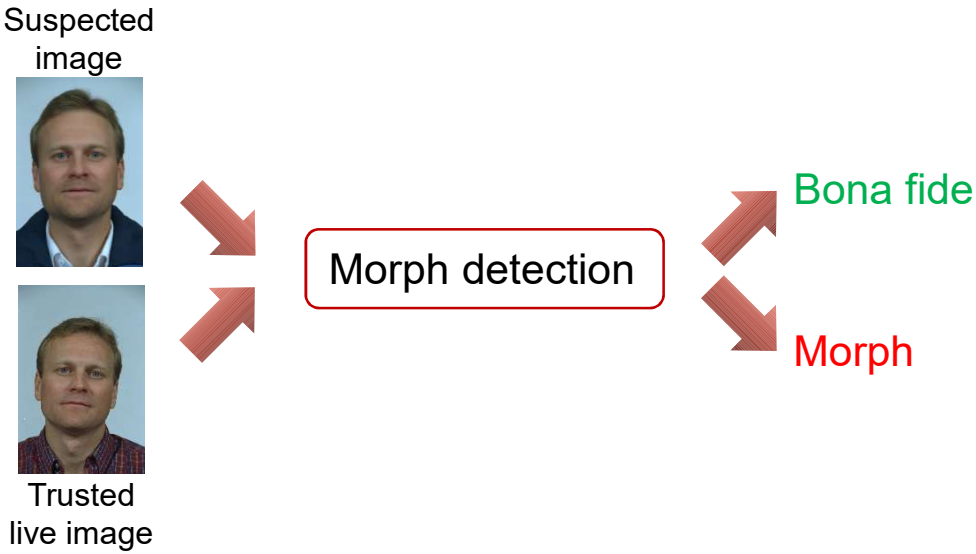
Automatic morphing detection

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).

Automatic morphing detection (3)

Results on SOTAMD benchmarks:

Single image Scenario (S-MAD)

Image format	Algorithm	EER	$BPCER_{10}$	$BPCER_{20}$	$BPCER_{100}$
Digital	PRNU	44.8%	100.0%	100.0%	100.0%
	SSE	**31.8%**	**65.0%**	**79.3%**	**91.7%**
	Deep-S-MAD	39.0%	100.0%	100.0%	100.0%
	S-MBLBP	41.4%	100.0%	100.0%	100.0%
P&S	PRNU	48.0%	**85.9%**	**97.4%**	100.0%
	SSE	54.4%	94.9%	98.3%	**99.9%**
	Deep-S-MAD	**37.1%**	100.0%	100.0%	100.0%
	S-MBLBP	43.3%	100.0%	100.0%	100.0%

Automatic morphing detection (4)

Differential image Scenario (D-MAD)

Image format	Algorithm	EER	$BPCER_{10}$	$BPCER_{20}$	$BPCER_{100}$
Digital	BSIF	45.9%	78.3%	84.1%	93.8%
	DFR	**4.5%**	**2.0%**	**3.9%**	**18.8%**
	MBLBP	33.5%	52.8%	59.9%	74.8%
	WL	37.1%	71.7%	83.3%	95.7%
	DR	52.0%	89.7%	94.7%	98.6%
	FaDe	14.2%	17.2%	22.8%	64.6%
P&S	BSIF	51.4%	95.7%	98.4%	99.6%
	DFR	**4.6%**	**1.8%**	**4.1%**	**19.7%**
	MBLBP	29.3%	51.5%	62.4%	81.2%
	WL	36.2%	70.4%	82.8%	95.6%
	DR	50.1%	90.3%	95.4%	99.2%
	FaDe	17.2%	24.8%	32.4%	74.6%

Automatic morphing detection (5)

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;
- Different morphing processes introduce different perturbations;
- Printed & scanned images;
- Lack of public databases.

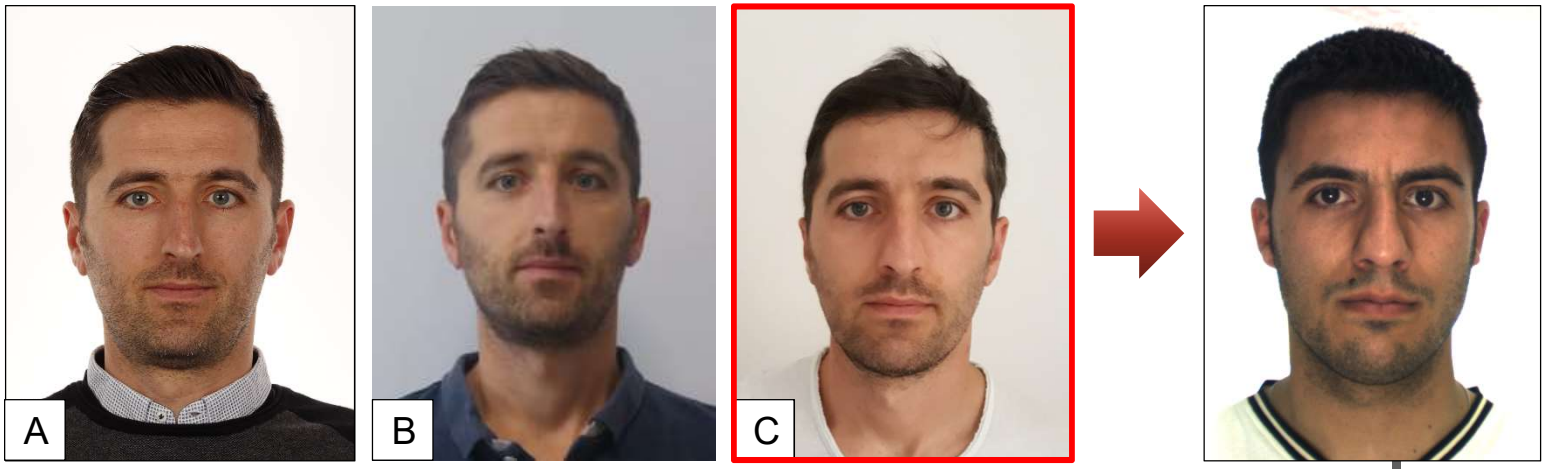
Intra-subject vs morphing variations

Beard and Hair style

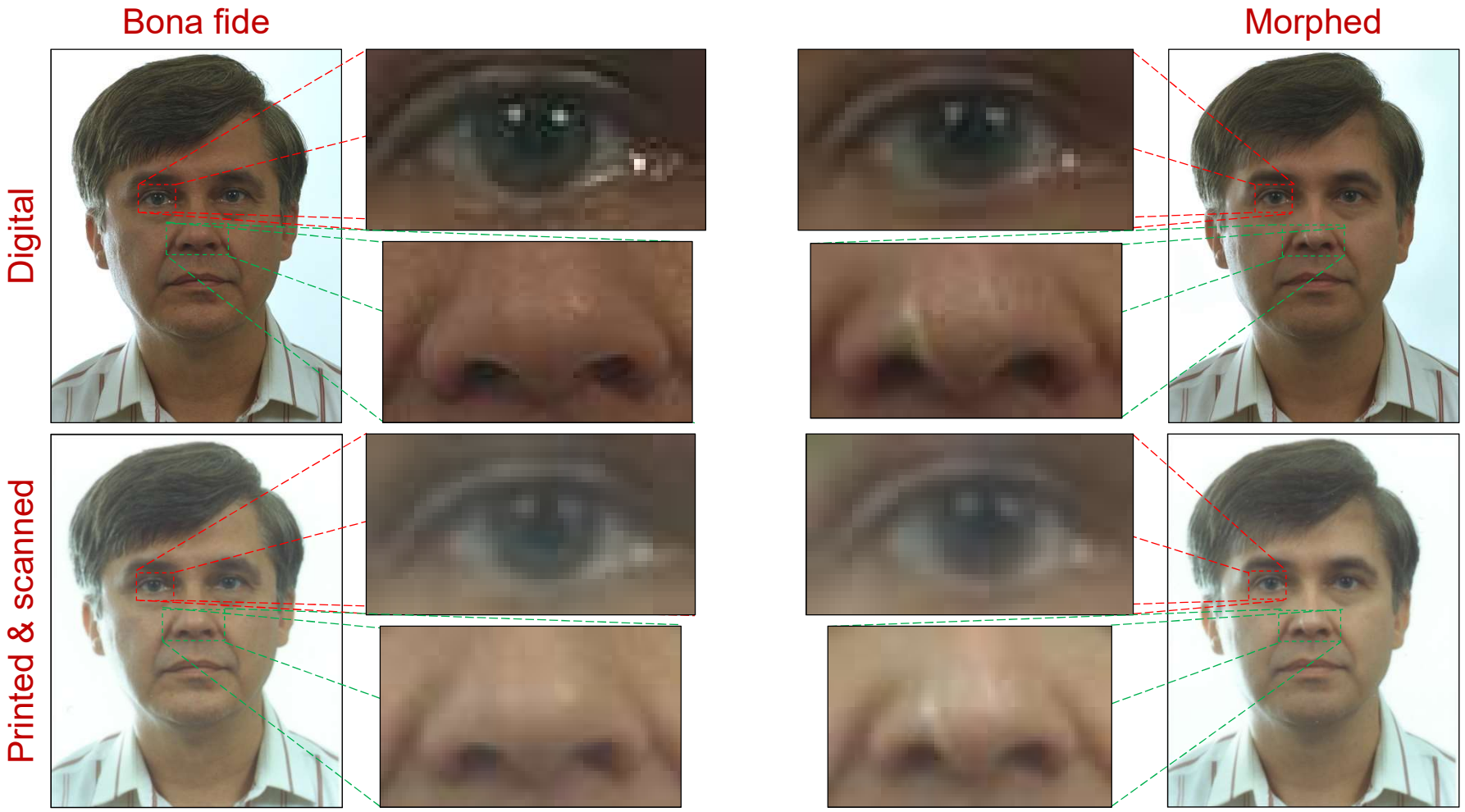
Makeup

Aging

Which is the morphed image?



Printed & scanned images



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

Matteo Ferrara and Annalisa Franco

Department of Computer Science and Engineering
University of Bologna
matteo.ferrara@unibo.it
annalisa.franco@unibo.it

Biometric System Laboratory
biolab.csr.unibo.it