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

I cannot use my passport to pass border controls!

Could another person ask for a regular passport using a photo with hidden information of my face?

If yes, I could use it to fool ABC systems at the borders!
The morphing attack (2)

Passport Issuance

Accomplice

Morphed image

Regular passport with morphed face image

ABC Verification

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

<table>
<thead>
<tr>
<th>Image format</th>
<th>Algorithm</th>
<th>EER</th>
<th>BPCR$_{10}$</th>
<th>BPCR$_{20}$</th>
<th>BPCR$_{100}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital</td>
<td>PRNU</td>
<td>44.8%</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>SSE</td>
<td>31.8%</td>
<td>65.0%</td>
<td>79.3%</td>
<td>91.7%</td>
</tr>
<tr>
<td></td>
<td>Deep-S-MAD</td>
<td>39.0%</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>S-MBLBP</td>
<td>41.4%</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td>P&amp;S</td>
<td>PRNU</td>
<td>48.0%</td>
<td>85.9%</td>
<td>97.4%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>SSE</td>
<td>54.4%</td>
<td>94.9%</td>
<td>98.3%</td>
<td>99.9%</td>
</tr>
<tr>
<td></td>
<td>Deep-S-MAD</td>
<td>37.1%</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>S-MBLBP</td>
<td>43.3%</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
### Differential image Scenario (D-MAD)

<table>
<thead>
<tr>
<th>Image format</th>
<th>Algorithm</th>
<th>EER</th>
<th>BPCER&lt;sub&gt;10&lt;/sub&gt;</th>
<th>BPCER&lt;sub&gt;20&lt;/sub&gt;</th>
<th>BPCER&lt;sub&gt;100&lt;/sub&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital</strong></td>
<td>BSIF</td>
<td>45.9%</td>
<td>78.3%</td>
<td>84.1%</td>
<td>93.8%</td>
</tr>
<tr>
<td></td>
<td>DFR</td>
<td>4.5%</td>
<td>2.0%</td>
<td>3.9%</td>
<td>18.8%</td>
</tr>
<tr>
<td></td>
<td>MBLBP</td>
<td>33.5%</td>
<td>52.8%</td>
<td>59.9%</td>
<td>74.8%</td>
</tr>
<tr>
<td></td>
<td>WL</td>
<td>37.1%</td>
<td>71.7%</td>
<td>83.3%</td>
<td>95.7%</td>
</tr>
<tr>
<td></td>
<td>DR</td>
<td>52.0%</td>
<td>89.7%</td>
<td>94.7%</td>
<td>98.6%</td>
</tr>
<tr>
<td></td>
<td>FaDe</td>
<td>14.2%</td>
<td>17.2%</td>
<td>22.8%</td>
<td>64.6%</td>
</tr>
<tr>
<td><strong>P&amp;S</strong></td>
<td>BSIF</td>
<td>51.4%</td>
<td>95.7%</td>
<td>98.4%</td>
<td>99.6%</td>
</tr>
<tr>
<td></td>
<td>DFR</td>
<td>4.6%</td>
<td>1.8%</td>
<td>4.1%</td>
<td>19.7%</td>
</tr>
<tr>
<td></td>
<td>MBLBP</td>
<td>29.3%</td>
<td>51.5%</td>
<td>62.4%</td>
<td>81.2%</td>
</tr>
<tr>
<td></td>
<td>WL</td>
<td>36.2%</td>
<td>70.4%</td>
<td>82.8%</td>
<td>95.6%</td>
</tr>
<tr>
<td></td>
<td>DR</td>
<td>50.1%</td>
<td>90.3%</td>
<td>95.4%</td>
<td>99.2%</td>
</tr>
<tr>
<td></td>
<td>FaDe</td>
<td>17.2%</td>
<td>24.8%</td>
<td>32.4%</td>
<td>74.6%</td>
</tr>
</tbody>
</table>
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

Jan '06

Jun '13

Which is the morphed image?

A

B

C

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
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