Face Morphing

\[
\begin{align*}
\text{Face 1} & \quad + \quad \text{Face 2} & \quad = & \quad \text{Morphed Face} \\
\text{Face 3} & \quad + \quad \text{Face 4} & \quad = & \quad \text{Morphed Face}
\end{align*}
\]
Face Morphing Software

**Desktop Apps**

- Morpheus Photo Morpher
  - Source: http://www.morpheussoftware.net

- FantaMorph 5 Professional
  - Source: http://www.fantamorph.com

- Adobe Photoshop
  - Source: https://www.adobe.com/products/photoshop.html

**Mobile Apps**

- FaceFusion
  - Source: https://en.softonic.com/solutions/apps/facefusion-lite

- Mixbooth
  - Source: http://www.piviandco.com/apps/mixbooth

**Websites**

- Morph Thing
  - Source: http://www.morphthing.com

- Learn OpenCV
  - Source: https://www.learnopencv.com/face-morph-using-opencv-cpp-python
Morph Examples


Existence Proof (c. 2014)

University of Bologna

• One morphing algorithm
• Two FR algorithms vulnerable
  – Luxand
  – Neurotechnology
  – Threshold set for FMR = 0.001
• All frauds successful:
  – Male-Male (5 pairs)
  – Female-Female (5 pairs)
  – Male-Female (1 pair)
  – Male-Male-Male (1 triple)
  – Close age pairings

NIST

• Two morphing algorithms
• Twelve FR algorithms vulnerable
• Most frauds successful:
  – Male-Male (5 subjects)
  – No algorithm immune

Conclusion: Existence proof - morphed images can match two people strongly

<table>
<thead>
<tr>
<th>Subjects</th>
<th>NTechLab</th>
<th>Gemalto</th>
<th>Megvii/Face++</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scores</td>
<td>1.983</td>
<td>1.842</td>
<td>1.428</td>
</tr>
<tr>
<td></td>
<td>3958</td>
<td>3497</td>
<td>2634</td>
</tr>
<tr>
<td></td>
<td>86.75</td>
<td>84.44</td>
<td>61.65</td>
</tr>
<tr>
<td></td>
<td>1.883</td>
<td>2.000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3727</td>
<td>3846</td>
<td></td>
</tr>
<tr>
<td></td>
<td>86.41</td>
<td>88.46</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.997</td>
<td>1.839</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3814</td>
<td>3609</td>
<td></td>
</tr>
<tr>
<td></td>
<td>86.42</td>
<td>84.56</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.965</td>
<td>1.836</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3761</td>
<td>3542</td>
<td></td>
</tr>
<tr>
<td></td>
<td>85.65</td>
<td>82.58</td>
<td></td>
</tr>
</tbody>
</table>

**Scores above matching thresholds:** Both subjects authenticate against all morphs at FMR = 0.001 AND FMR = 0.00001!

**Thresholds:**

<table>
<thead>
<tr>
<th>Face matching algorithm (2018)</th>
<th>Threshold for FMR=0.001</th>
<th>Threshold for FMR=0.00001</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTechLab</td>
<td>1.451</td>
<td>1.542</td>
</tr>
<tr>
<td>Gemalto</td>
<td>2847</td>
<td>3039</td>
</tr>
<tr>
<td>Megvii/Face++</td>
<td>68.65</td>
<td>79.09</td>
</tr>
</tbody>
</table>

Subjects do NOT authenticate at weak FMR = 0.001, because they’re naturally different people.
Face recognition algorithms (October 2018) are still vulnerable

- 2-person morphs
  - subject alpha ranged from 0.1 -> 0.9 per pair
  - morphed within race and gender label groups
  - 24,228 comparisons of morphs with constituents
  - > 30 million non-morph comparisons to generate FMR threshold
NIST FRVT MORPH

Automated Face Morph Detection Evaluation
• Single-image morph detection
• Single-image scanned morph detection
• Two-image differential morph detection
• 1:1 morph acceptance (FR resistance against morphing)

Currently Seeking...
• Developers of morph detection technology
• Collaboration partners with suitable morph data or software that can be shared with NIST

BREAKING NEWS
Face Recognition Vendor Test (FRVT) MORPH Evaluation
Now Accepting algorithm submissions! Google: FRVT MORPH
Single Image Morph Detection: Morphed image or not?

Use Case: Attack on enrollment

- Untrusted capture
- Upload to server

Protocol: Given single image X in isolation, produce

1) Morph decision
2) “morphiness” score

Morphiness = F(X)

Evaluation: ISO/IEC 30107-3 metrics

- Attack Presentation Classification Error Rate (APCER): proportion of morph attack samples incorrectly classified as bona fide presentation (missed detection rate over morphed images)
- Bona Fide Presentation Classification Error Rate (BPCER): proportion of bona fide samples incorrectly classified as morphed samples (false detection rate over un-morphed images)
- Others TBD
Two-Image Differential Morph Detection:
*Morph detection given live image?*

**Use Case:** Attack during verification (e.g., at eGate)
- Prior morph enrolled e.g. on identity document

**Goal:** Determine that image C is morphed by finding features in it that are not present in image B2. For example, the scar should be present but is not.

**PASSPORT**

A. Images of this image not available during authentication
B2: This image represents a live capture during an eGate border crossing, say.

**Protocol:** Given image X and suspected morph Y produce
1) Morph decision
2) “morphiness” score

**Evaluation:** ISO/IEC 30107-3 metrics
- BPCER
- APCER
- Others TBD
Single Image Scanned Morph Detection: *Morphed image or not?*

**Use Case:** Attack on enrollment
- Untrusted capture
- Upload to server

**Protocol:** Given *single printed + scanned image* $X$ in isolation, produce
1) Morph decision
2) “morphiness” score

Morphiness = $F(X)$

**Evaluation:** ISO/IEC 30107-3 metrics
- BPCER
- APCER
- Others TBD
1:1 Morph Acceptance: Do subjects verify successfully against morphed image?

Use Case: Test FR algorithm resistance against morphing

Protocol: Given image X and image Y, produce verification similarity score

Evaluation: ISO/IEC 30107-3 metrics
- Mated Morph Presentation Match Rate (MMPMR)
- True Accept Rate
- False Accept Rate
- Others TBD
Initial Test Data

• Tiered Approach
  – Morphs created with easily accessible morphing software (e.g. websites, mobile apps, etc.)
  – Morphs created with automated morphing algorithms
  – High quality morphs created manually with commercial tools (e.g. Photoshop, etc.)

• Factors
  – Alpha (subject % in morph)
  – Printing and Scanning
  – Compression Ratio/Resolution
  – Others

• New morph techniques/data TBD... open-ended
## How to participate

[https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-morph]

### Draft Evaluation Plan and API

*Developers send comments to NIST*

[frvt@nist.gov]

### Final Evaluation Plan and API

*Developers start implementing to final API*


### Participation Agreement

*Developers send signed participation agreement to NIST*


### Validation Package/API Software

*NIST publishes validation package (with null or reference implementation)*

*Developers must run their software against validation package*

[https://github.com/usnistgov/frvt/tree/master/morph]

### Algorithm submission

*Developers submit their validation results + algorithm to NIST*

*NIST executes algorithm against datasets*

### Ongoing Reporting

*NIST reports results back to participants and community*

[https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-morph]
Thank you!

Mei Ngan
[mei@nist.gov]