Impact of facial beautification on face recognition:
From plastic surgery to makeup presentation attacks

Christian Rathgeb

Hochschule Darmstadt, ATHENE, da/sec Security Research Group

International Face Performance Conference (IFPC), 28.10.2020
1. Introduction

2. Plastic Surgery

3. Retouching

4. Makeup

5. Makeup Presentation Attack Detection
Facial Beautification and Detection

► Scenario: either the reference or the probe image has been altered
► Further types of beautification: tattoos, piercings, etc.

Selfie face distortion is driving people to get nose jobs

Selfies make our noses look 30 percent larger than they really are, plastic surgeons warn.

By Julia Belluz | @juliatheoronto | julia.belluz@voxmedia.com | Updated Jun 21, 2018, 9:25am EDT

(a) head and face plastic surgeries

(b) types of plastic surgeries on head and face

Source: International Society of Aesthetic Plastic Surgery
Plastic Surgery

Verification with ArcFace and Cognitec

Plastic Surgery

► Low impact on biometric performance
► Only in case of severe alterations, e.g. feminisation surgeries
► Users may apply retouching with easy-to-use apps
► Common alterations: smoothing skin, slimming nose, enlarging eyes
Retouching

► Evaluation with Cognitec shows negligible impact on biometric performance
► Detection of retouching of interest

Cost-efficient way for beautification (mostly applied by women)

Areas: lips, skin, eyes

Alteration of perceived anatomy

Antitza Dantcheva, Cunjian Chen, Arun Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?", in IEEE Fifth international conference on biometrics: theory, applications and systems (BTAS), 2012.
Makeup Presentation Attacks

- Impact on face recognition in case of severe alterations

Public databases containing makeup presentation attacks:

(a) MIFS
(b) DFW
(c) AIM
(d) DMFaces

Table 1 — Examples of artificial and human presentation attack instruments

<table>
<thead>
<tr>
<th>Artificial</th>
<th>Complete</th>
<th>Partial</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>gummy finger, video of face</td>
<td>glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up</td>
</tr>
</tbody>
</table>

Source: ISO/IEC 30107-1:2016(E)
Makeup Presentation Attacks

- Attacker may apply makeup for impersonation or concealment
- Detection is difficult since bona fide users may also apply makeup

Makeup Presentation Attacks

- Vulnerability analysis using Cognitec and ArcFace
- Use of MIFS/DFW databases for attacks and FRGCv2 for bona fide
- High Impostor Attack Presentation Match Rates (IAPMR) and Relative Impostor Attack Presentation Accept Rates (RIAPAR)

<table>
<thead>
<tr>
<th>System</th>
<th>FMR</th>
<th>FNMR</th>
<th>IAPMR MIFS</th>
<th>IAPMR DFW</th>
<th>RIAPAR MIFS</th>
<th>RIAPAR DFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>COTS</td>
<td>0.001</td>
<td>2.085</td>
<td>0.000</td>
<td>1.121</td>
<td>2.085</td>
<td>3.206</td>
</tr>
<tr>
<td></td>
<td>0.010</td>
<td>0.751</td>
<td>1.878</td>
<td>4.746</td>
<td>2.629</td>
<td>5.497</td>
</tr>
<tr>
<td></td>
<td>0.100</td>
<td>0.500</td>
<td>6.573</td>
<td>14.898</td>
<td>7.073</td>
<td>15.398</td>
</tr>
<tr>
<td></td>
<td>1.000</td>
<td>0.334</td>
<td>29.577</td>
<td>44.034</td>
<td>29.911</td>
<td>44.368</td>
</tr>
<tr>
<td>ArcFace</td>
<td>0.001</td>
<td>1.090</td>
<td>1.168</td>
<td>2.742</td>
<td>2.258</td>
<td>3.832</td>
</tr>
<tr>
<td></td>
<td>0.010</td>
<td>0.922</td>
<td>2.804</td>
<td>7.759</td>
<td>3.726</td>
<td>8.681</td>
</tr>
<tr>
<td></td>
<td>0.100</td>
<td>0.838</td>
<td>7.243</td>
<td>21.940</td>
<td>8.081</td>
<td>22.778</td>
</tr>
<tr>
<td></td>
<td>1.000</td>
<td>0.587</td>
<td>32.477</td>
<td>51.104</td>
<td>33.063</td>
<td>51.691</td>
</tr>
</tbody>
</table>
Makeup Presentation Attacks

- Detection of attack in a differential detection scenario employ deep face representations
- Classification with SVM

- Problem: missing training data
- Idea: create a semi-synthetic database of makeup presentation attacks

Makeup Presentation Attacks

- Combination of image warping and makeup style transfer
- Target subjects from CelebA database
Makeup Presentation Attacks

► Good performance using ArcFace for feature extraction (in a differential scenario)
► D-EER: APCER=BPCER
► BPCER10: APCER=10%
► BPCER20: APCER=5%

<table>
<thead>
<tr>
<th>Feature Type</th>
<th>Mode</th>
<th>Feature Extractor</th>
<th>D-EER MIFS</th>
<th>D-EER DFW</th>
<th>BPCER10 MIFS</th>
<th>BPCER10 DFW</th>
<th>BPCER20 MIFS</th>
<th>BPCER20 DFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFR</td>
<td>single-image</td>
<td>ArcFace</td>
<td>38.785</td>
<td>44.860</td>
<td>84.652</td>
<td>89.953</td>
<td>90.068</td>
<td>92.991</td>
</tr>
<tr>
<td>FL</td>
<td>differential</td>
<td>dlib</td>
<td>19.484</td>
<td>20.768</td>
<td>28.125</td>
<td>73.132</td>
<td>45.313</td>
<td>87.813</td>
</tr>
<tr>
<td>FL</td>
<td>differential</td>
<td>OpenCV</td>
<td>25.837</td>
<td>41.116</td>
<td>43.770</td>
<td>76.205</td>
<td>52.716</td>
<td>86.433</td>
</tr>
<tr>
<td>TD</td>
<td>differential</td>
<td>LBP</td>
<td>33.803</td>
<td>45.168</td>
<td>93.569</td>
<td>86.023</td>
<td>97.917</td>
<td>91.250</td>
</tr>
<tr>
<td>TD</td>
<td>differential</td>
<td>BSIF</td>
<td>30.986</td>
<td>42.341</td>
<td>49.063</td>
<td>85.795</td>
<td>59.375</td>
<td>91.705</td>
</tr>
<tr>
<td>DFR</td>
<td>differential</td>
<td>VGG-Face</td>
<td>4.984</td>
<td>11.824</td>
<td>4.361</td>
<td>15.040</td>
<td>4.984</td>
<td>26.177</td>
</tr>
<tr>
<td>DFR</td>
<td>differential</td>
<td>ArcFace</td>
<td>0.704</td>
<td>1.791</td>
<td>0.313</td>
<td>0.799</td>
<td>0.313</td>
<td>0.799</td>
</tr>
</tbody>
</table>

Graph showing APCER in different scenarios for various feature extractors and modes.
Thank you for your attention!

Questions?