Vulnerability Evaluation for Presentation + Morphing Attacks

Marta Gomez-Barrero, Ulrich Scherhag, Andreas Nautsch, Christian Rathgeb, Raymond Veldhuis, Luuk Spreeuwers, Maikel Schils, Davide Maltoni, Patrick Grother, Sébastien Marcel, Ralph Breithaupt, R. Raghavendra, Christoph Busch

Hochschule Darmstadt, CRISP, da/sec Research Group
IFPC ‘18, Gaithersburg (US), 28/11/18
Outline

- Context
- Quality Evaluation
- Attack Success Evaluation
- Detection Performance Evaluation
- Conclusions
Context
Context

Morphing / Presentation Attack Detection Steps

- To establish a fair and realistic benchmark, we first need to model a realistic scenario...

- Taking into account all the intermediate steps

Quality Evaluation
Quality Evaluation Goals

- Key question: is the attack realistic?

- Different aspects might influence presentation attack instruments (PAIs):
  - Unattended scenario: the PAI must “only” fool the system
  - Attended scenario: PAI appearance gains importance

- Major factors for achieving realistic morphed samples:
  - Morphing quality
  - Similarity of the constituent subjects (e.g., age, gender, etc.)
  - Consistent quality of the database (bona fides vs morphs)
Morphing Quality (I)

- Attackers can take a long time (even weeks) for each morphed sample creation ⇒ high quality morph
- For research, this task is automated ⇒ low quality morph
- Don’t forget, that images must be accepted at the passport application office!
Equal quality for bona fide and morphed samples is important
Otherwise, the classifier is biased towards different quality levels
Impact of Compression

Bona fide sample

Uncompressed morphed sample

Compressed morphed sample

BRISQUE = 21.0

BRISQUE = 29.1

BRISQUE = 50.0

Blind / Referenceless Image QUality Evaluator (BRISQUE)
Attack Success Evaluation
Attack Success Evaluation Goals

- **Key question:** is the system **vulnerable** to the attacks?
  - We need to evaluate the percentage of successful attacks
  - This depends on the operating point of the system!
    \[ \Rightarrow \text{decision threshold } \delta \]

- **Key question 2:** is the system still **convenient**?
  - We can choose a high security operating point, and then reject all bona fide samples as well!

- **Note:** all comparisons should be uncorrelated (Mansfield, Wayman)
Presentation Attack Success: IAPMR

- ISO/IEC 30107-3 on Presentation Attack Detection evaluation defines:
  - **Impostor Attack Presentation Match Rate (IAPMR):** in a full system evaluation of a verification system, the proportion of impostor attack presentations [...] in which the target reference is matched

\[
IAPMR = \frac{1}{M} \cdot \sum_{m=1}^{M} \{[S_m] > \delta\}
\]

- But a morph is only successful if **all** contributing subjects are matched.
Morphing Attack Success: MMPMR

- **Mated Morph Presentation Match Rate (MMPMR)**: proportion of mated morph presentations (i.e., the morph image is compared to a bona fide samples stemming from one of the constituent subjects) in which the target reference is matched

- We compare all $N_m$ samples of each of the $M$ constituent subjects to the morphed sample

- If all samples are matched (i.e., scores above $\delta$) $\Rightarrow$ success!

\[
\text{MMPMR} = \frac{1}{M} \cdot \sum_{m=1}^{M} \left\{ \min_{n=1,\ldots,N_m} S_{mn}^{n} \right\} > \delta
\]
Morphing Attack Success: MMPMR

Min = 0.947
Morphing Attack Success: MinMax-MMPMR

But in a border control scenario, the attacker is able to conduct several authentication attempts (and is successful if one is positive).

\[
\text{MinMax-MMPMR} = \frac{1}{M} \cdot \sum_{m=1}^{M} \left\{ \left( \min_{n=1,\ldots,N_m} \left[ \max_{i=1,\ldots,I_m^m} S_{m,i}^{n,m} \right] \right) > \delta \right\}
\]
Morphing Attack Success: MinMax-MMPMR

Max = 0.987
Min = 0.987
Max = 0.993
Reaching a Balance

Decision threshold

IAPMR / MMPMR: 0% 😊
FNMR: 65% 😞

IAPMR / MMPMR: 41% 😞
FNMR: 1% 😊
Relative Morph Match Rate (RMMR)

- The IAPMR and the MMPMR only measure the vulnerabilities of the system.

- We need to take into account as well the system convenience:
  - In terms of the FNMR or the TMR.

- Both values depend on the decision threshold and can be combined in a single measure, the Relative Morph Match Rate (RMMR):

\[
\text{RMMR}(\delta) = 1 + \text{MMPMR}(\delta) - (1 - \text{FNMR}(\delta)) \\
= 1 + (\text{MMPMR}(\delta) - \text{TMR}(\delta))
\]
Attack Success Eval.

Reaching a Balance v2 (I)

Decision threshold

<table>
<thead>
<tr>
<th>BF mated</th>
<th>BF non-mated</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>!IAPMR / MMPMR: 0% 😊</td>
<td>1 - FNMR: 45% 😞</td>
<td>RMMR: 55 😞</td>
</tr>
<tr>
<td>!IAPMR / MMPMR: 41% 😞</td>
<td>1- FNMR: 99% 😊</td>
<td>RMMR: 42 😊</td>
</tr>
</tbody>
</table>
Attack Success Eval.

Reaching a Balance v2 (II)

IAPMR / MMPMR: 3% 😊
1 - FNMR: 96% 😊
RMMR: 7 😊

IAPMR / MMPMR: 0% 😊
1 - FNMR: 55% 😞
RMMR: 45 😞
Reaching a Balance in PAD: Relative IAPMR

A similar approach can be followed for PAD

Relative Impostor Attack Presentation Match Rate (RIAPMR): proportion of impostor attack presentations using the same PAI species in which the target reference is matched in relation to the proportion of completed biometric comparison trails that do not result in a false non-match:

\[ RIAPMR(\delta) = 1 + IAPMR(\delta) - (1 - FNMR(\delta)) \]
\[ = 1 + IAPMR(\delta) - TMR(\delta) \]
Detection Performance Evaluation
Detection Performance Evaluation Goals & How To

- Key question: can we detect the attacks?
- Key question 2: is the system still convenient?

- Follow ISO/IEC 19795-1 on biometric performance testing and reporting:
  - Disjoint subdivision of training and test-set
  - Remember: one morphed sample is related to at least two subjects

- Follow ISO/IEC 30107-3 on biometric presentation attack detection:
  - Attack Presentation Classification Error Rate (APCER) ⇒ Security
  - Bona Fide Presentation Classification Error Rate (BPCER) ⇒ Convenience
Detection Perf. Eval.

Example

![Detection Performance Evaluation Graph]

- BPCER (in %)
- APCER (in %)

Legend:
- Digital
- HP-Scan
- RICOH-Scan
- BPCER 20
- BPCER 10
Conclusions
A complete evaluation should include:
- Quality evaluation
- Attack success evaluation: IAPMR / MMPMR\(^1\) and RIAPMR / RMMR\(^1\)
- Detection performance evaluation: BPCER vs APCER (DET plot)

And should follow the ISO/IEC 19795-1 and 30107-3 standards

We should model a realistic scenario with
- High quality attacks
- Equal quality over the database (especially between morph and bona fide samples)

We need to analyse both the security (APCER, MMPMR) and the convenience (BPCER, FNMR) ⇒ we need the RMMR and RIAPMR!

\(^1\) Python implementations available at [https://github.com/dasec/mvr](https://github.com/dasec/mvr)
Marta Gomez-Barrero
(marta.gomez-barrero@h-da.de)