Methods to Prevent Registration Using Fake Face Images

Luis Cárabe - luiscarabe@gmail.com
Eduardo Cermeño - eduardo.cm@vaelsys.com
Presenter: E. Cermeño - Research Department Vaelsys

2021
Eduardo Cermeño obtained the degrees of Superior Engineer in computer science, Master in computer science and artificial intelligence and PhD in computer science and telecommunications from the Autonomous University of Madrid (UAM).

He currently serves as General and Research Director of the company Vaelsys in Madrid and Associate Professor at the Autonomous University of Madrid in the department of Computer Engineering. He has directed several projects and research activities related to video surveillance that have obtained public funding and received recognition of excellence by the European Commission.
1 Introduction

2 Methods

3 Basic Scenario

4 Advanced Scenario

5 Conclusion
Facial recognition and impersonation

- New spoofing attack methods emerge.
What is morphing

- Generating intermediate frames between two images.

![Images of morphing process]

- One photo to verify two different subjects successfully\(^1\).

---

Two scenarios

- Basic: performance of the recognizers in correct subject identification.
- Advanced: ability to detect fraudulent registrations.
1 Introduction

2 Methods

3 Basic Scenario

4 Advanced Scenario

5 Conclusion
Methods

- Morphing: based on Delaunay triangulation.
- Face recognition:

<table>
<thead>
<tr>
<th>Category</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holistic</td>
<td>Eigenfaces</td>
</tr>
<tr>
<td></td>
<td>Fisherfaces</td>
</tr>
<tr>
<td>Local</td>
<td>LBPH</td>
</tr>
<tr>
<td></td>
<td>SIFT</td>
</tr>
<tr>
<td>Deep Learning</td>
<td>FaceNet</td>
</tr>
</tbody>
</table>

- Database: Labeled Faces in the Wild (LFW).
1 Introduction

2 Methods

3 Basic Scenario

4 Advanced Scenario

5 Conclusion
Robustness

- Testing dataset: 25 similar-looking pairs.
  - 99 in-between morphings.

The most robust algorithm should be the one requiring the highest amount of morphing to force its failure.
Top 1 results
Top 3-5 results

(a) Top 3.

(b) Top 5.
Performance of the morphing detector

- Using the morphed images of the basic scenario.

![Graph showing morphing detection confidence vs. morphing amount](image-url)
Testing dataset:

- Impostors: based on the 25 SL pairs and using random morphings, 490 images.
- Genuine: 490 images of different subjects not included in training.

A recognizer will accept a person as a new record when it has 0 identified subjects with confidence above a threshold.

- False Acceptance Rate (FAR): impostors being able to register again.
- False Rejection Rate (FRR): genuine subjects not being able to be registered for the first time.
FaceNet results

![Graph showing FaceNet results with curves for FRR, FAR, and FRR with morphological detection, and FAR with morphological detection. The x-axis represents the threshold, and the y-axis represents error percentage.]
LBPH results

![Chart showing error rates vs. threshold for FRR, FAR, FRR with morphological detection, and FAR with morphological detection. The chart plots the percentage of error against the threshold, with FRR decreasing and FAR increasing as the threshold increases. The FRR with morphological detection line is slightly above the FRR line, and the FAR with morphological detection line is slightly below the FAR line.]
Eigenfaces results

![Graph showing performance metrics for different thresholds. The graph compares False Reject Rate (FRR) and False Accept Rate (FAR) for different conditions: without and with morphological detection.]
Fisherfaces results

![Graph showing Fisherfaces results](image-url)
SIFT results

The graph illustrates the performance of the SIFT algorithm with respect to error rates (FRR, FAR) and threshold values. The y-axis represents the error percentages, ranging from 0% to 100%, while the x-axis represents the threshold values, ranging from 0% to 100%.

- **FRR (False Rejection Rate)**: The percentage of genuine images that are incorrectly rejected. This line shows a decrease as the threshold increases, indicating a reduction in FRR.
- **FAR (False Acceptance Rate)**: The percentage of impostor images that are incorrectly accepted. This line shows an increase as the threshold increases, indicating an increase in FAR.
- **FRR with mor. det.**: This line represents the FRR with additional modifications or detection methods. It shows a slight decrease compared to the standard FRR, indicating improved performance.
- **FAR with mor. det.**: This line represents the FAR with additional modifications or detection methods. It shows a slight decrease compared to the standard FAR, indicating improved performance.

As the threshold increases, the FRR decreases and the FAR increases. The additional detection methods (mor. det.) help in balancing the error rates more effectively.
1 Introduction

2 Methods

3 Basic Scenario

4 Advanced Scenario

5 Conclusion
Basic Scenario

- FaceNet obtains the best performance identifying the in-between morphed images correctly.
- The morphing detector has an excellent performance.
Advanced Scenario

- FaceNet is the recognizer with the best FRR.
- Eigenfaces is the recognizer with the best FAR.
- The inclusion of the morphing detector has a significant impact on all recognizers.
  - As the morphing detector fixes the FAR problem, FaceNet is the best algorithm.
Final conclusion

A reasonable solution for preventing registration and login using fake face images can be built using face recognition and morphing detection state-of-the-art techniques.

Future work:

- Test newer and promising deep learning facial recognition algorithms.
- Better-designed algorithms for fooling its detection systems.
Thank you for your attention.
Appendix
Morphing based on Delaunay triangulation

- Correspondence between the two images created by determining the face key landmarks.
- Delaunay triangulation.
- Warping.
- Blending.