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

Presenter

- 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.

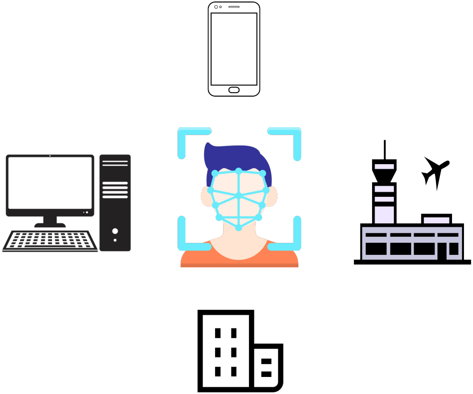
Index

1. Introduction
2. Methods
3. Basic Scenario
4. Advanced Scenario
5. Conclusion

1. Introduction
2. Methods
3. Basic Scenario
4. Advanced Scenario
5. Conclusion

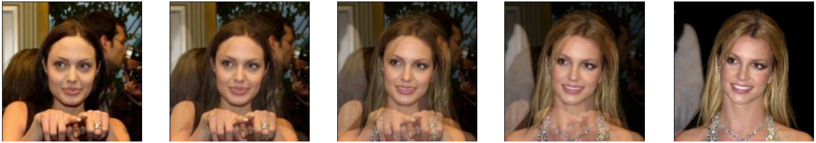
Facial recognition and impersonation

- New spoofing attack methods emerge.



What is morphing

- Generating intermediate frames between two images.



- One photo to verify two different subjects successfully[1].

[1] M. Ferrara, A. Franco, and D. Maltoni “The magic passport,” in *IEEE International Joint Conference on Biometrics,* Clearwater, FL, 2014, pp. 1–7.

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:

Category	**Algorithm**
Holistic	Eigenfaces Fisherfaces
Local	LBPH SIFT
Deep Learning	FaceNet

- Database: Labeled Faces in the Wild (LFW).
- Morphing detector: Single Image Morphing Attack Detection (S-MAD).

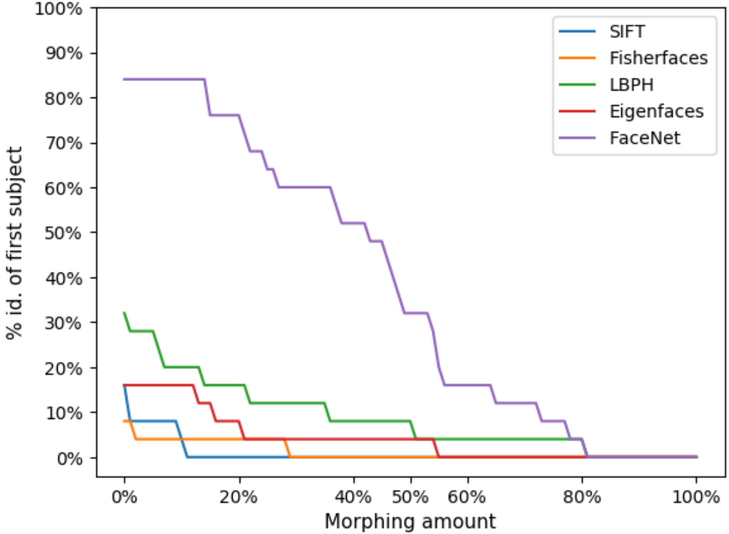
1. Introduction
2. Methods
3. Basic Scenario
4. Advanced Scenario
5. Conclusion

Robustness

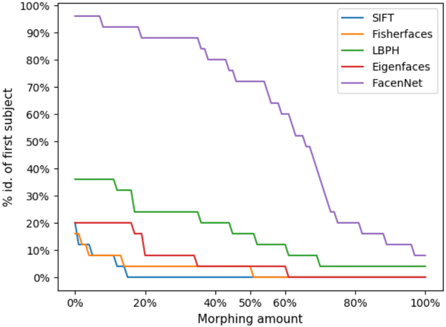
- Testing dataset: 25 similar-looking pairs.
  - 99 in-between morphings.

The most robust algorithm should be the one requiring the highest amount of morphing to force its failure.

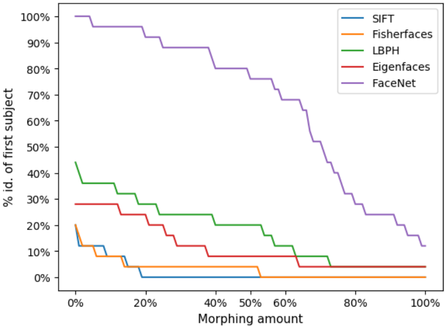
Top 1 results



Top 3-5 results



(a) Top 3.

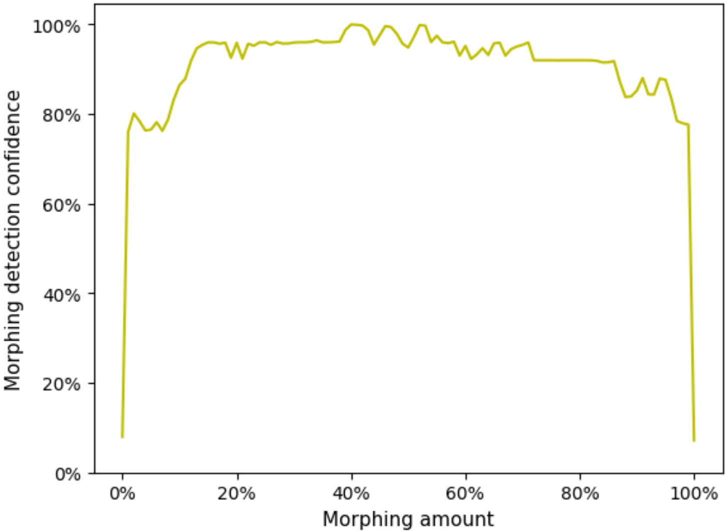


(b) Top 5.

1. Introduction
2. Methods
3. Basic Scenario
4. Advanced Scenario
5. Conclusion

Performance of the morphing detector

- Using the morphed images of the basic scenario.



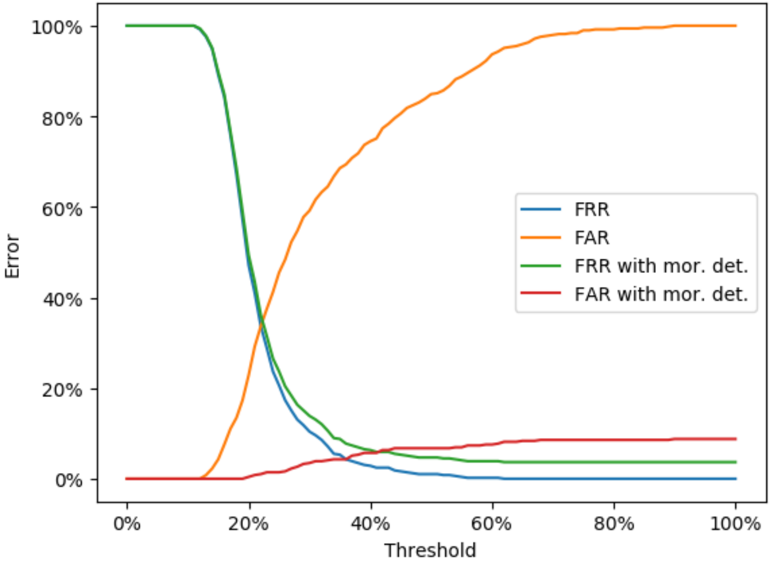
FAR and FRR

- 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.

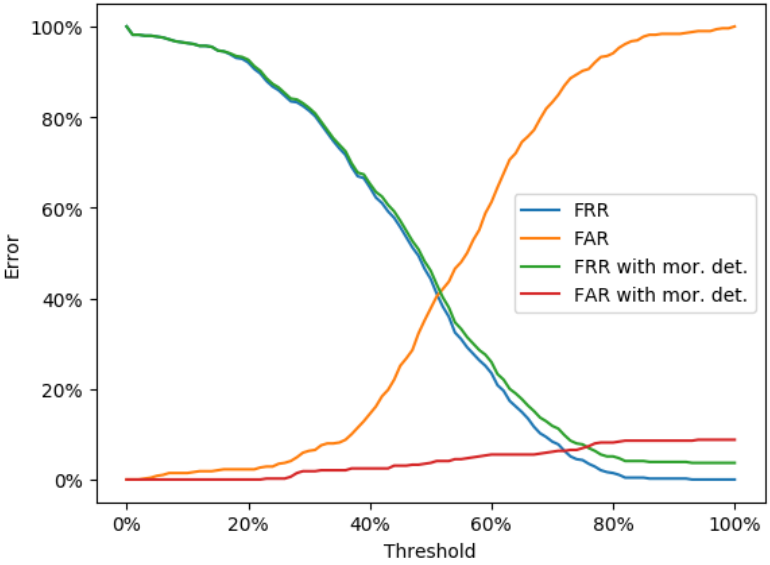
A recognizer will accept a person as a new record when it has 0 identified subjects with confidence above a threshold.

- 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.

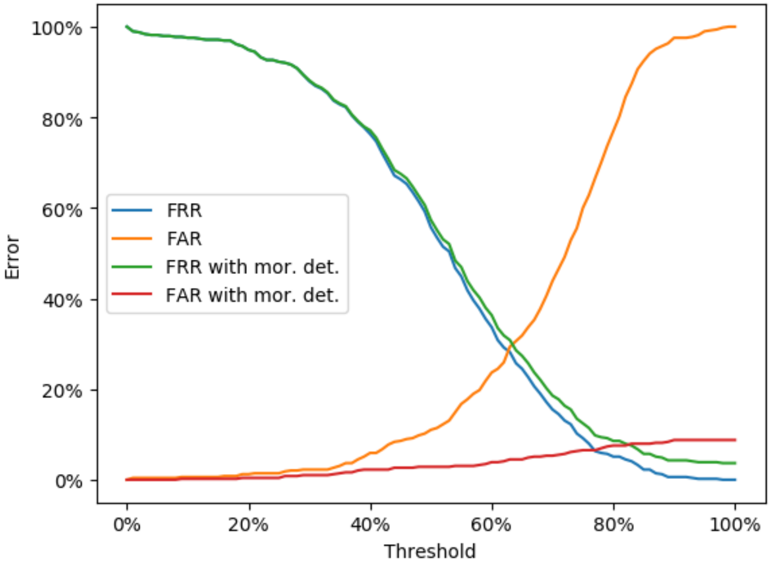
FaceNet results



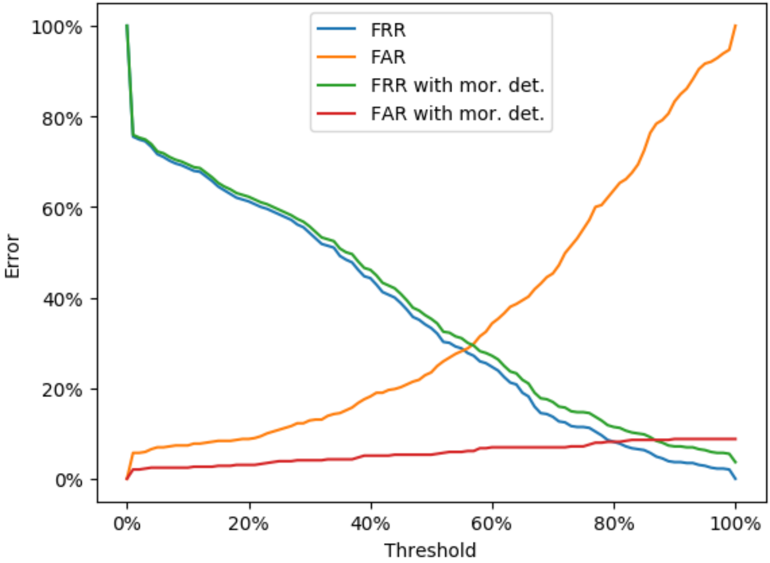
LBPH results



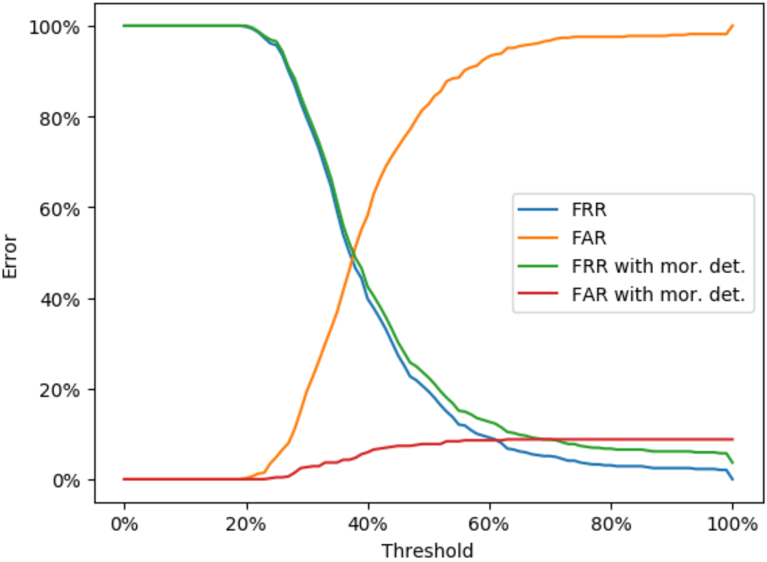
Eigenfaces results



Fisherfaces results



SIFT results



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.

6 Appendix

Morphing based on Delaunay triangulation

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

Return