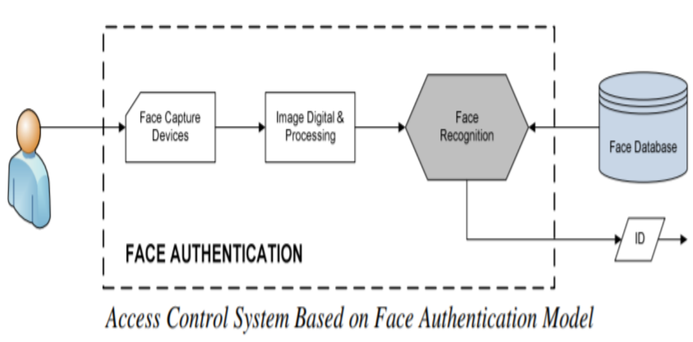
CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Biometric Security: The Vulnerability of Facial Recognition to Face Morphing

Cynthia Jules, Dr. Masooda Bashir

Introduction



Access Control System Based on Face Authentication Model

There are two main uses for facial recognition systems: identification and verification. Identification is 1 to many, where you have to check the biometric data against all the other biometric data in the set to find out who the person is. Verification is 1 to 1, where you compare biometric data of one person against another biometric data to authenticate that this is the proper person.

An image is acquired of the potential target, the system locates the face, and when it detects the face, it records the spatial geometry of unique features. The system needs to focus on key features of the face which are the areas surrounding the cheekbones, sides of the mouth, and location of the nose and eyes in some systems. Facial metrics are taken, and based on the algorithm, they will calculate and determine if the person is authentic.

Overview

Morphed face images are artificially generated images, which blend the facial images of two or more different subjects into one [1]. This allows two people to use one ID to gain access to passport and banking systems or allows an attacker to present the morphed image, in conjunction with other spoofing methods, to gain access to facial recognition systems.

Goals

The goal of this research was to determine a security vulnerability in facial recognition that could be exploited with minimal amount of work by the attacker.

Morphing facial images has not been heavily researched other than using these images to create false passport pictures.

There is little research done on spoofing systems with a 2D morphed images, and none on the use of 3D mask with a morphed images.

Fundamental Questions

What is the threshold that a facial recognition system allows access to a presentation attack using minimal face morphing?

How similar do the faces of the people need to be? What is the rate of acceptance?

What points on the morphed facial image, when edited, have higher rates of acceptance by the system?

Method

The face database used is the AR Face Database. [6] These photos are all in raw format and it can be assumed that the authors of the experiment did not change the format because they did not indicate otherwise.

The experiment used 2 commercial facial recognition software tools: Neurotechnology VeriLookSDK 5.4 and Luxand FaceSDK 4.0. The thresholds of the software were fixed according to the Frontex guidelines.

Two images of different people who had some physical similarity but did not falsely match were chosen. Then they were morphed into a new image.

The GIMP and GAP software were used to morph the images.

Follow the morphing process outline in “The Magic Passport” [1].

Phase 1 and Phase 2 are done separately.

Conclusion

It would be extremely difficult for an average person to attempt to morph facial images to spoof a facial recognition system with the method laid out in “The Magic Passport”[1]. However, it is still feasible because of the new photo editing and morphing technology widely available.

Future Work

- Complete this experiment outlined by the authors of “The Magic Passport” [1] with all the necessary software that wasn’t available or difficult to use.
- Create a simpler method for morphing facial images with accessible software and face databases that an average person can use.
- Use the methodology to experiment with smartphones and computers and measure their vulnerability to images that have been morphed.
- Create a 3D mask experiment using a morphed facial image and experiment on smartphones and computers.

Acknowledgments

This material is based upon work supported by **The Department of Homeland Security** under Grant Award Number, 2015-ST-061-CIRC01

References

[1] M. Ferrara, A. Franco, and D. Maltoni, “On the vulnerability of face recognition systems towards morphed face attacks - IEEE Conference Publication,” *Design and implementation of autonomous vehicle valet parking system - IEEE Conference Publication*, 02-Oct-2014. [Online]. Available: https://ieeexplore.ieee.org/document/7935088/. [Accessed: 02-Aug-2018].

[2] M. Ferrara, A. Franco, and D. Maltoni, “The magic passport,” *IEEE International Joint Conference on Biometrics*, Oct. 2014.

[3] N. Minh Duc and B. Quang Minh, “Your Face is NOT Your Password: Face Authentication ByPassing Lenovo - Asus- Toshiba,” *Black Hat*, 2010. [Online]. Available: http://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf. [Accessed: Jul-2018].

[4] S. Karahan, M. Kilinc Yildirum, K. Kirtac, F. Sukru Rende, G. Butun, and H. Kemal Ekenel, “How Image Degradations Affect Deep CNN-Based Face Recognition? - IEEE Conference Publication,” *Design and implementation of autonomous vehicle valet parking system - IEEE Conference Publication*, 21-Oct-2016. [Online]. Available: https://ieeexplore.ieee.org/document/7736924/. [Accessed: 06-Aug-2018].

[5] "Features versus Context: An approach for precise and detailed detection and delineation of faces and facial features," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 32, No. 11, pp. 2022-2038, 2010.

[6] A.M. Martinez and R. Benavente. *The AR Face Database*. CVC Technical Report #24, June 1998.

[7] FRONTEX-Research and Development Unit, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, v2.0, 2012.