Evaluating the Resilience of Face Recognition Systems against Malicious Attacks

Luma Omar[1]
luma.omar@durham.ac.uk
Ioannis Ivrissimtzis[1]
ioannis.ivrissimtzis@durham.ac.uk

[1] School of Engineering and Computing Sciences
Durham University
Durham, UK

Abstract

This paper presents an experiment designed to test the resilience of several user verification systems based on face recognition technology against simple identity spoofing methods, such as trying to gain access to the system by using mobile camera shots of the users, their ID cards, or social media photos of them that are available online. We also aim at identifying the compression threshold above which a photo can be used to gain access to the system. Four major user verification tools were tested: Keyemon and Luxand Blink on Windows and Android Face Unlock and FaceLock on Android. The results show all tested systems to be vulnerable to even very crude attacks, indicating that the technology is not ready yet for adoption in applications where security rather than user convenience is the main concern.

1 Introduction

Biometrics based user verification systems rely on the extraction of some human biological characteristics and their statistical analysis to verify the identity of a person. It is a relatively new technology, competing against more traditional methods such as pins and passwords. Apart from enhancing security, biometric methods aim at improving user experience, as there is no need for the user to memorise passwords, which could easily be forgotten or guessed. [2] [6].

Biometric methods are classified into categories. Physiological biometric methods are based on human body part measurements and prominent examples include fingerprint, face and iris recognition. Behavioural biometric methods are based on human's action measurements and prominent examples include gesture, key stroking, gaits and signature recognition. [2] [1].

Among the various physiological biometric methods, face recognition has recently received attention from both industry and academia [17]. The developed techniques vary in sophistication, as well as in hardware and software requirements, ranging from systems based on 3D face scans, to systems based on video and systems that can work with a single still image [9]. Enhancing the security of face recognition systems is a major challenge since a secure system should be able to withstand a variety of attacks, ranging from systematic algorithmic attacks to attacks based on theft of data.

Pages 5.1-5.9
https://dx.doi.org/10.5244/C.29.BMVW.5

In this paper, we present an experiment designed to test the resilience of face recognition systems against theft of data attacks. The first part of the experiment uses still face images collected in different ways and from various sources, i.e., instant still images taken during the experiment by a smartphone camera; ID card photos; images found through Google Image searches and images on social media platforms such as Facebook and WhatsApp. In the second part of the experiment we resize some of the still images that were successfully used to gain access to the system and we find the minimum resolution required for such an attack.

2 Background

2.1 Face Recognition

Holistic methods for face recognition from still images use the whole face region the input of the face recognition algorithm. Eigenfaces, based on Principal Component Analysis is the best known example of such methods. The basic algorithm was proposed by Sirovich and Kirby [12] and used for face classification by Turk and Pentland [15] [16]. The eigenfaces are the eigenvectors with the lowest eigenvalues of the covariance matrix of a high dimensional vector space of face image. They are used as the basis of a lower dimension vector space of face images. The reduction in the dimension allows for an efficient solution to the face classification problem.

In feature based methods for face recognition from still images, local features such as the eyes, the curve of the eyebrows, nose, mouth, shape of the lips and chin, are first extracted and their locations and local statistics (geometric and/or appearance) are fed into a structural classifier [17]. Hybrid methods use a mix of the two previous methods, local features and the whole face region, to recognize a face [17].

Techniques for face recognition from video may be based on still image face recognition methods, or on multimodal methods, combining for example video and audio, or spatiotemporal methods, analysing for example the trajectory of face features [17].

2.2 Attacks on Face Recognition Systems

In [5], attacks on biometric security systems are classified in to two categories. Direct attacks are based on theft of biometric data and are carried out against the sensor using synthetic traits, such as printed iris images or gummy fingers. Indirect attacks are carried out against some of the algorithmic modules of the system.

An indirect attack based on the hill-climbing algorithm and Bayesian statistics is proposed in [3][4]. This attacking technique adapts a global distribution computed from a set of all users to the local specificities of the client being attacked and Gelby *et al* [4] reports success rates of over 85% in by-passing the system. Such indirect attack are more interesting than direct attacks from a theoretical point of view, however their applicability is currently limited by their unrealistic assumption that the system is leaking information to the attacker in the form of, for example, face matching scores.

2.3 Liveness Tests

Liveness tests use common video or some other form of input such as infrared camera and aim at distinguishing between those objects that are alive and those that are not. In [11]

three different liveness detection solutions where proposed: (a) liveness detection by using a challenge and response method such as eye-blinking (b) by analysing face texture on high quality images, and (c) by combining two or more biometrics for example speech and face recognition together.

A liveness detection test against photo spoofing was proposed in [8] based on the analysis of spontaneous eye blinking behaviour. Another liveness detection test against photo spoofing was proposed in [13], using the differences in the reflective properties between a real human face and a photograph of it to discriminate between them.

2.3.1 KeyLemon

KeyLemon is a biometric authentication solution based on face and speaker recognition. It offers a non-password login to Windows using face recognition on a standard webcam and it can also be used for login to web based systems such as Facebook and Twitter. KeyLemon claims that its latest face recognition algorithms enhance security by using 3D depth sense cameras to combine depth, near-infrared and colour information [18]. Here, we run the freely available version of the system on a common laptop hardware configuration which did not support such features.

2.3.2 Luxand Blink

Luxand Blink is one of the most popular user verification systems used as a convenient alternative to passwords. It supports quick non-password login on different operating systems, e.g. Windows, Mac OS, linux, iOS and Android. Luxand Blink's algorithm processes the coordinates of 40 facial feature points such as mouth corners, nose tip, eyes, eye corners and eyebrows [19].

2.3.3 Android Face UnLock

It was first released for the Android 4.0 "Ice Cream Sandwich" for unlocking Android mobile phones. Afterwards, an enhanced version was offered on Android 4.1 "Jelly Bean" with a new liveness test option embedded, which checks if the person in front of the camera is blinking making sure they are alive [20]. Being a non-standard feature, here we did not enable this liveness test.

2.3.4 FaceLock for Apps

FaceLock for Apps is an alternative face recognition tool for locking either an android phone or some of its applications. It is a very popular system, having with a 4/5 star rating based on the feedback from more than 10,000 users on google play store [21].

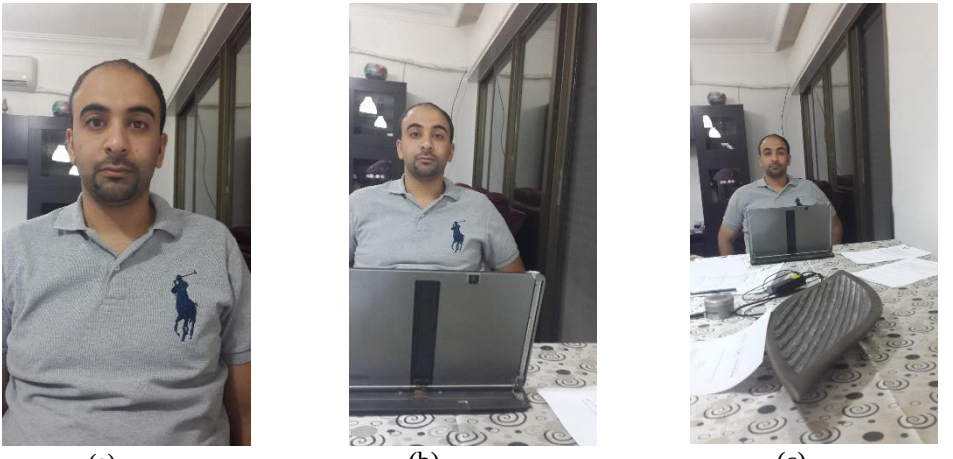
3 Experimental set-up

3.1 General Setup

Two main operating systems were tested in the experiment: Windows 8.1 and Google Android 4.4.2. A laptop with Windows 8.1, Intel Core i3 CPU @ 1.90 GHz, GB RAM, 64-bit Operating System and a Front HD webcam was used to test the KeyLemon and Luxand

Blink systems. A Samsung Galaxy S4 mobile running Android 4.4.2 with a 2MP front camera was used to test the Android built-in Face Unlock and the FaceLock for Apps.

A Samsung Galaxy S4 13 MP rear camera was used to take images of the participant at size 2322 x 4128 pixels (9:16). Images were taken from different distances: one at short distance (50 cm) where the face is 15% of the full image, one at intermediate distance (100 cm) where the face is 3% of the full image, and one at far distance (150 cm) where the face is 0.8% if the full image.



(a) (b) (c)

Figure 1: Instant photos of a participant taken by a Samsung Galaxy S4 Rear 13 MP camera from different distances: (a) Camera Distance: 50 cm, (b) Camera Distance: 100 cm, (c) Camera Distance: 150 cm.

The experiment took place in Amman, Jordan in an indoor environment under stable, good illumination conditions. It was a preliminary experiment, aiming at establishing the general level of resilience of the most commonly used face recognition systems, rather than understanding the specific vulnerabilities of each one of them. As it was a simple, black box experiment with binary outcomes, and as we did not aim at that stage to identify and explain any sources variance in the collected data, we opted for a small number of participants. However, that means that we were not able to run meaningful statistical tests on the results and in particular, we were not able to do any comparisons between the four systems we tested.

3.2 Systems Setup

The recommended default levels of security were chosen for all tested systems. In particular, the KeyLemon security level, which ultimately is a trade-off between convenience of use and security, was set at medium recognition accuracy. In Luxand Blink, the high convenience mode was set, while the medium security level was chosen for the Facelock for Apps system. The Android Face Unlock does not have any parameters to be set up.

3.3 The experiment

Prior to the experiment each participant was asked to sign a consent form. The form contained a brief about the experiment and a reassurance that there were no direct risks to them by participating to the study. The duration of the experiment was about one hour per participant and it was separated in to four sessions. A sample video of an experiment is provided as a supplementary material.

In the first session, the participants were asked to register with the four systems and test their registration. In the second session, the participants were involved in a photoshoot session in which three frontal face images of them from distances of 50cm, 100cm and 150cm and then the participants tried to gain access to the system using these images displayed on the smartphone's camera. In the third session, the participants were asked to try to gain access to the systems using the photo of their ID card. Finally, the participants were asked to find three face-front photos of them published on the internet/social media and these photos, displayed on the smartphone's camera were again used to try to gain access to the systems. After the end of the four sessions, we compressed the participant's photo that was taken in the second session from distance 50cm and tried to gain access to the system until the maximum compression ration still allowing access to the system was found.

4 Results

4.1 Gaining access to the system during the experimental sessions

The following table shows the results of each experimental session with each participant.

Instant Photos by the mobile at various distances

Instant Photo by the mobile from a close distance (approx. 50 cm) was successful in gaining access to the following tools: (Yes/No)							
Tool	**E1**	**E2**	**E3**	**E4**	**E5**	**Average**	
KeyLemon	Yes	Yes	Yes	Yes	Yes	**100%**	**Yes**
Luxand Blink	Yes	Yes	Yes	Yes	Yes	**100%**	**Yes**
Face Unlock	Yes	Yes	Yes	Yes	Yes	**100%**	**Yes**
FaceLock for Apps	Yes	Yes	Yes	Yes	Yes	**100%**	**Yes**
Instant Photo by the mobile from a close distance (approx. 100 cm) was successful in gaining access to the following tools: (Yes/No)							
Tool	**E1**	**E2**	**E3**	**E4**	**E5**	**Average**	
KeyLemon	No	No	No	No	No	**0%**	**Yes**
Luxand Blink	No	No	No	No	No	**0%**	**Yes**
Face Unlock	No	No	No	No	No	**0%**	**Yes**
FaceLock for Apps	No	No	No	No	No	**0%**	**Yes**

Instant Photo by the mobile from a close distance (approx. 150 cm) was successful in gaining access to the following tools: (Yes/No)

Tool	E1	E2	E3	E4	E5	Average	
KeyLemon	No	No	No	No	No	**0%**	**Yes**
Luxand Blink	No	No	No	No	No	**0%**	**Yes**
Face Unlock	No	No	No	No	No	**0%**	**Yes**
FaceLock for Apps	No	No	No	No	No	**0%**	**Yes**

ID Photo

ID photo was successful in gaining access to the following tools: (Yes/No)

Tool	E1	E2	E3	E4	E5	Average	
KeyLemon	No	No	Yes	Yes	No	**40%**	**Yes**
Luxand Blink	No	No	No	Yes	No	**20%**	**Yes**
Face Unlock	No	Yes	Yes	Yes	No	**60%**	**Yes**
FaceLock for Apps	No	No	No	Yes	No	**20%**	**Yes**

Photos on Internet/Social Media

Photos on Internet/Social Media were successful in gaining access to the following tools: (Number of successful images out of 3)

Tool	E1	E2	E3	E4	E5	Average	
KeyLemon	1	1	2	2	1	**46.67%**	**Yes**
Luxand Blink	0	1	1	2	1	**33.33%**	**Yes**
Face Unlock	1	0	1	2	1	**33.33%**	**Yes**
FaceLock for Apps	0	0	0	2	1	**20.00%**	**Yes**

The participants were able to gain access to all systems using a smartphone shot taken from a distance of 50cm, while frontal images taken from distances of 100cm and 150cm were not able to gain access to any of our tested systems. However, as the compression results in section 4.2 indicate the participant can easily gain access using longer distance photos, after zooming into the face and cropping the image.

Getting access to the systems using ID photos was partially successful. Android Face Unlock had the highest by-pass rate with 3/5, followed by keyLemon with 2/5 and then Luxand Blink and FaceLock for Apps with 1/5. Photos on the Internet and/or social media were also partially successful in gaining access to the tested systems. KeyLemon had a successful by-pass rate of 7/15, followed by Luxand Blink and Android Face Unlock with 5/15 and FaceLock for Apps with 3/15.

4.2 Compression results

The following table shows the highest compression rate of the photos that were taken at a distance of 50cm so that access to the system was still possible. The original photo size is 2322 x 4128 (9:16) and the face is 15% of the whole image. All photos are encoded in JPEG and the percentages in the table correspond to the ratio of the filesize of the compressed image to the filesize of the original.

Face Recognition System	E1	E2	E3	E4	E5	Average
KeyLemon	2%	3%	2%	2%	3%	**2%**
Luxand Blink	4%	4%	4%	5%	4%	**4%**
Face Unlock	1%	1%	2%	1%	1%	**1%**
FaceLock for Apps	2%	2%	3%	2%	2%	**2%**

We notice that even highly compressed images can be used to gain access to the tested systems. That suggests that the failure in gaining access with the long range images (100cm and 150cm) was most probably due to particular system settings requiring the recognised face to be closer to the camera, rather than the lack of information in the long range images. To test this hypothesis, the images taken from the 150cm distance were cropped around the face, compressed as 50 kb JPEG files, and finally resized by an x2 zoom. In all five cases, these cropped, compressed and zoomed-in images were successfully used in gaining access to all five systems.

5 Conclusion and future work

We tested four user verification systems based on face recognition against basic, direct malicious attacks. We found all of them to be vulnerable even against the crudest of attacks, such as using highly compressed still images taken with smartphone cameras, or using still images that can be found in social media. We believe that part of the high success rate of the attacks is due to the developers of the systems prioritising user convenience over security, at least on the default configuration of their product. However, the question on whether face recognition, at least by its own, is suitable for user verification can also be raised. Indeed, face recognition seems to rely on data which are personal in nature but, nevertheless, are often already in the public domain or can be easily stolen.

In the future we plan to work on developing stronger liveness tests and in particular, liveness tests that will not require non-standard hardware configuration such as the illuminated IR sensor required by Windows Hello.

References

[1] Ballard, L., Lopresti, D., Monrose, F., "Forgery Quality and Its Implications for Behavioral Biometric Security," *Systems, Man, and Cybernetics, Part B:*

Cybernetics, IEEE Transactions on , vol.37, no.5, pp.1107-1118, Oct. 2007

[2] Faundez-Zanuy, M., "Biometric security technology," *Aerospace and Electronic Systems Magazine, IEEE* , vol.21, no.6, pp.15-26, June 2006

[3] Galbally, J., Fierrez, J., Ortega-Garcia, J., Bayesian hill-climbing attack and its application to signature verification. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 386–395. Springer, Heidelberg (2007)

[4] Galbally, J., Fierrez, J., Ortega-Garcia, J., McCool, C., Marcel, S., "Hill-climbing attack to an Eigenface-based face verification system," *Biometrics, Identity and Security (BIdS), 2009 International Conference on* , vol., no., pp.1-6, Sept. 2009

[5] Galbally, J., Fierrez, J., Ortega-Garcia, J., Hill-climbing Attack Based on the Uphill Simplex Algorithm and Its Application to Signature Verification," *the COST 2101 European Conference on Biometrics and ID Management*, pp. 83–94. Springer, Heidelberg (2011)

[6] Jain, A.K., Ross, A., Pankanti, S., "Biometrics: a tool for information security," *Information Forensics and Security, IEEE Transactions on* , vol.1, no.2, pp.125-143, June 2006

[7] Jain, A.K., Ross, A., Prabhakar, S., "An introduction to biometric recognition," *Circuits and Systems for Video Technology, IEEE Transactions on* , vol.14, no.1, pp.4-20, Jan. 2004

[8] Pan G., Sun L., Wu Z., Lao S., "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on* , vol., no., pp.1-8, Oct. 2007

[9] Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Jin Chang, Hoffman, K., Marques, J., Jaesik Min, Worek, W., "Overview of the face recognition grand challenge," *Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on* , vol.1, no., pp.947-954 vol. 1, June 2005

[10] Ratha, N.K., Connell, J.H., Bolle, R.M., "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal* , vol.40, no.3, pp.614-634, 2001

[11] Singh, A.K., Joshi, P., Nandi, G.C., "Face recognition with liveness detection using eye and mouth movement," *Signal Propagation and Computer*

Technology (ICSPCT), 2014 International Conference on , vol., no., pp.592-597, July 2014

[12] Sirovich, L. and Kirby, M., "Low-dimensional procedure for the characterization of human face." J. Opt. Soc. Am. 4, 519–524, 1987.

[13] Tan, X., Li, Y., Liu, J., & Jiang, L. "Face liveness detection from a single image with sparse low rank bilinear discriminative model".Springer Berlin Heidelberg, 2010.

[14] Tolba, A. S., A. H. El-Baz, and A. A. El-Harby. "Face recognition: A literature review." International Journal of Signal Processing 2.2 (2006): 88-103.

[15] Turk M., Pentland A., "Eigenfaces for recognition", *Journal of cognitiveNeuroscience*, vol. 3, no. 1, pp.71-86, 1991.

[16] Turk M. and Pentland A., "Face recognition using Eigenfaces," *In Proc. IEEE Conference on Computer Vision and Pattern Recognition*, pp. 586–591, 1991.

[17] Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, P. J., 2003. Face recognition: A literature survey.*ACM Comput. Surv.* 35, 4 (December 2003), pp.399-458.

[18] About KeyLemon, Retrieved July 5th, 2015 from http://www.keylemon.com

[19] Luxand FaceSDK, Retrieved on July 06th, 2015 from http://www.luxand.com

[20] Android FaceUnlock, Retrieved on July 04th 2015 from http://www.androidcentral.com

[21] FaceLock for Apps, Retrieved on July 07th, 2015 from http://www.facelock.mobi/