Smile in the face of adversity much? A print based spoofing attack

Vinay Uday Prabhu
UnifyID
San Francisco, CA 94107

John Whaley
UnifyID
San Francisco, CA 94107

Abstract

In this paper, we demonstrate a simple face spoof attack targeting the face recognition system of a widely available commercial smart-phone. The goal of this paper is not proclaim a new spoof attack but to rather draw the attention of the anti-spoofing researchers towards a very specific shortcoming shared by one-shot face recognition systems that involves enhanced vulnerability when a smiling reference image is used.

1. Introduction

One-shot face recognition (OSFR) or single sample per person (SSPP) face recognition is a well-studied research topic in computer vision (CV) [8]. Solutions such as Local Binary Pattern (LBP) based detectors [1], Deep Lambertian Networks (DLN) [9] and Deep Supervised Autoencoders (DSA) [4] have been proposed in recent times to make the OSFR system more robust to changes in illumination, pose, facial expression and occlusion that they encounter when deployed *in the wild*. One very interesting application of face recognition that has gathered traction lately is for mobile device unlocking [6]. One of the highlights of Android 4.0 (Ice Cream Sandwich) was the **Face Unlock**[1] screen-lock option that allowed users to unlock their devices with their faces. It is rather imperative that we mention here that this option is always presented to the user with a cautioning clause that typically reads like **Face recognition is less secure than pattern, PIN, or password.*

The reasoning behind this is that there exists a plethora of face spoof attacks such as print attacks, malicious identical twin attack, sleeping user attack, replay attacks and 3D mask attacks. These attacks are all fairly successful against most of the commercial off-the-shelf face recognizers [7]. This ease of spoof attacks has also attracted attention of the CV researchers that has led to a lot of efforts in developing liveness detection anti-spoofing frameworks such as `Secure-face` [6]. (See [3] for a survey.)

[1] https://developer.android.com/about/versions/android-4.0-highlights.html

Recently, a large scale smart-phone manufacturer introduced a face recognition based phone unlocking feature. This announcement was promptly followed by media reports about users demonstrating several types of spoof attacks.[2]

In this paper, we would like to explore a simple print attack on this smart-phone. The goal of this paper is not proclaim a new spoof attack but to rather draw the attention of the anti-spoofing community towards a very specific shortcoming shared by face recognition systems that we uncovered in this investigation.

2. Methodology and Results

The methodology we used entailed taking a low quality printout of the target user's face on a plain white US letter paper size (of dimension 8.5 by 11.0 inches) and then unlocking the device by simply exposing this printed paper in front of the camera.[3] Given the poor quality of the printed images, we observed that this simple print attack was duly repulsed by the detector system as long as the attacker sported neutral facial expressions during the registration phase. However, when we repeated the attack in such a way that the attacker had an overtly smiling face when (s)he registered, we were able to break in successfully with high regularity.

In Figure 1, we see two examples of neutral expression faces that failed to spoof the smart-phone's face recognition system when the registering image had a neutral facial expression. A video containing the failed spoofing attempt with a neutral facial expression can be viewed at: https://goo.gl/QhBnhP.

In Figure 2, we see the same two subjects' images that successfully spoofed the phone's face recognition system when the registering (enrollment) image was overtly smiling. The face training demo videos are available at: https://goo.gl/hXAFD2. The video of the successful spoof can be viewed at: https://goo.gl/X1GS7H.

[2] https://goo.gl/TBlTE8, https://goo.gl/6OR0oP

[3] The print status and print quality diagnostic report of the printer is available here: https://goo.gl/wSto24

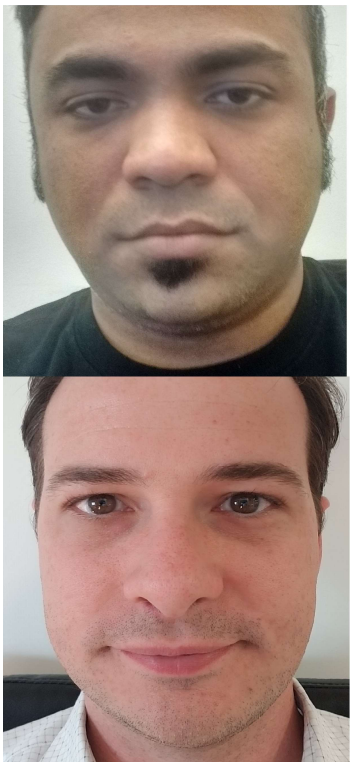

Figure 1. Example of two neutral expression faces that failed to spoof the smart-phone's face recognition system.

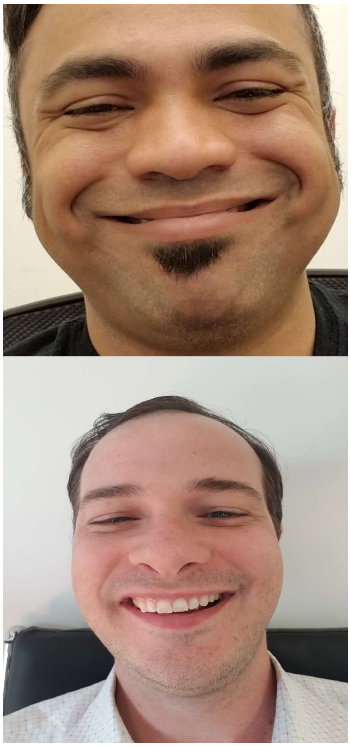

Figure 2. Example of 2 smiling registering faces that successfully spoofed the smart-phone's face recognition system

2.1. Motivation for the attack and discussion

It has been well known for a long time in the computer vision community that faces displaying expressions, especially smiles, resulted in stronger recall and discrimination power [10]. In fact, the authors in [2] termed this the *happy-face advantage*, and showcased the variation in detection performance for varying facial expressions. Through experimentation, we wanted to investigate the specific one-shot classification scenario when the registering enrollment face had a strong smile that resulted in the discovery of this attack. As for defense from this attack, there are two straightforward recommendations. The first recommendation would be to simply display a message goading the user to maintain a passport-type neutral facial expression.[4] The second would entail having a smile detector such as [5] as a pre-filter that would only allow *smile-free* images as a reference image.

References

[1] T. Ahonen, A. Hadid, and M. Pietikainen. Face description with local binary patterns: Application to face recognition. *IEEE transactions on pattern analysis and machine intelligence*, 28(12):2037–2041, 2006. 1

[2] W. Chen, K. Lander, and C. H. Liu. Matching faces with emotional expressions. *Frontiers in psychology*, 2:206, 2011. 2

[3] J. Galbally, S. Marcel, and J. Fierrez. Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2:1530–1552, 2014. 1

[4] S. Gao, Y. Zhang, K. Jia, J. Lu, and Y. Zhang. Single sample face recognition via learning deep supervised autoencoders. *IEEE Transactions on Information Forensics and Security*, 10(10):2108–2118, 2015. 1

[5] P. O. Glauner. Deep convolutional neural networks for smile recognition. *arXiv preprint arXiv:1508.06535*, 2015. 2

[6] K. Patel, H. Han, and A. K. Jain. Secure face unlock: Spoof detection on smartphones. *IEEE Transactions on Information Forensics and Security*, 11(10):2268–2283, 2016. 1

[7] D. F. Smith, A. Wiliem, and B. C. Lovell. Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security*, 10(4):736–745, 2015. 1

[8] X. Tan, S. Chen, Z.-H. Zhou, and F. Zhang. Face recognition from a single image per person: A survey. *Pattern recognition*, 39(9):1725–1745, 2006. 1

[9] Y. Tang, R. Salakhutdinov, and G. Hinton. Deep lambertian networks. *arXiv preprint arXiv:1206.6445*, 2012. 1

[10] Y. Yacoob and L. Davis. Smiling faces are better for face recognition. In *Automatic Face and Gesture Recognition, 2002. Proceedings. Fifth IEEE International Conference on*, pages 59–64. IEEE, 2002. 2

[4] http://www.cic.gc.ca/english/passport/apply/photos.asp