Resilience of Luminance based Liveness Tests under Attacks with Processed Imposter Images

Luma Omar
Durham University
School of Eng. & Comp. Sciences
South Road, Durham, DH1 3LE, UK
luma.omar@durham.ac.uk

Ioannis Ivrissimtzis
Durham University
School of Eng. & Comp. Sciences
South Road, Durham, DH1 3LE, UK
ioannis.ivrissimtzis@durham.ac.uk

ABSTRACT

Liveness tests are techniques employed by face recognition authentication systems, aiming at verifying that a live face rather than a photo is standing in front of the system camera. In this paper, we study the resilience of a standard liveness test under imposter photo attacks, under the additional assumption that the photos used in the attack may have been processed by common image processing operations such as sharpening, smoothing and corruption with salt and pepper noise. The results verify and quantify the claim that this type of liveness tests rely on the imposter photo images being less sharp than live face images.

Keywords

Liveness tests; face recognition; luminance models; difference of Gaussians; logistic regression

1 INTRODUCTION

Compared to the other main biometric authentication methods which are based on fingerprints or high resolution iris images, face recognition has the unique characteristic that it is based on data that can easily be found in the public domain. For example, in many cases can be very easy to obtain a photo of someone's face, either doing a quick online search or by logging into a social network. As a result, face recognition based authentication is particularly vulnerable to imposter attacks, when, for example, an attacker holds someone's photo in front of the camera trying to gain access through the face recognition system.

To counter such concerns, *liveness tests* are binary classification algorithms aiming at determining whether the recognized face is a live face, or a photo or video played in front of the system's camera. Developing accurate liveness tests is a challenging task and they often require use of specialized hardware, such as infrared cameras. In [10] several commercial user authentication systems that do not use additional hardware to support liveness tests were evaluated and they were found vulnerable to even very crude imposter image attacks.

The research on liveness tests that do not rely on specialized hardware is motivated by the desire to have secure face recognition based authentication on machines of everyday use, such low end laptops and smartphones. The current state of the art, such as the Tan et al. paper [16], is based on machine learning algorithms trained to distinguish between images of live faces taken by the face recognition system and images of photos fed to the system by the imposters. In particular, it has been established that the different reflectance properties of these two categories of can lead to the development of an effective liveness test.

In this paper we study the effect of image processing operations applied on the imposter images on the performance of a variant of the Tan et al. test based on differences of Gaussians and sparse logistic regression. As a possible explanation of why their algorithm is effective, Tan et al. observe that images of face photos fed into the system by imposters tend to be smoother, as they lack detail. The main contribution of our paper is a verification and quantification of this claim by processing the imposter images and measuring the effect on the performance of their algorithm. As expected, the sharpening of the imposter images reduced the accuracy of the liveness test, while the smoothing of the imposter images increased it.

The main limitation of our paper is that we process the imposter images of an existing database (NUAA), which are images of a photo of the subject, rather than processing the photos of the subject and then taking photos of them. While this approach allows for a better quantitative understanding of the basic principle underlying the Tan et al. algorithm, we note that we have not yet measured the effect of a direct attack consisting of processing the photo of the subject and feeding it into the system.

2 RELATED WORK

As biometrics based security applications become increasingly popular, the study of their vulnerabilities and the development of countermeasures is becoming a research topic of current interest. Attacks on face recognition systems fall into two main categories; direct and

indirect attacks. Direct attacks rely on the use of stolen biometric data of some form; digital images displayed on a screen, printed photos, or gummy fingerprints. Pan et al. [11] classified direct attacks into three categories: a photograph of the real user is used; a video; or a 3D model. One particular strength of direct attacks is that they do not require knowledge of the face recognition system they attack.

Indirect attacks use algorithms to construct an input face that will gain entry to the biometric security system. They presuppose some knowledge of the attacked system and a certain level of information leakage from it. Martinez et al. [9] uses similarities scores assumed to be outputted by the face recognition system and the hill climbing technique to construct an image giving access to the system. Galbally et al. [3] tested the vulnerability of a Principal Component Analysis (PCA) based face recognition system against a Bayesian hill climbing attack algorithm and reported a 85% success rate for such attacks. In [5], two face recognition systems using a Gaussian Mixture Model (GMM) and PCA, respectively, were tested against a Hill Climbing indirect attack and were both found vulnerable, with the GMM system being nevertheless the more robust.

Liveness tests are binary classification algorithms developed as countermeasures to the imposter attacks to distinguish between live faces and imposter images, video or 3D models. Robust liveness tests that do not require the use of any specialized hardware have been developed based on the observation that the high frequency components of the imposter images are weaker than those of the live faces.

The algorithm in Tan et al. [16] we study in this paper is based on this observation and will be discussed in more detail in Section 3. Peixoto et al. [13] further improved the Tan et al. algorithm by addressing limitations related to bad illumination conditions. Another anti-spoofing approach proposed by Komulainen et al. [7] uses support vector machine classification of histograms of gradient descriptors. Maatta et al. [8] uses Local Binary Patterns to analyze the local texture of the face and the resulting single feature histograms are classified with Support Vector Machines. Galbally et al. [4] use image quality metrics and classify the lower quality images as imposter.

Other approaches to rely on biometric motion analysis, focusing on different types of motion such as: head tilting [2], mouth movement [6] and eye-blinking [12]. Foreground and background motion correlation is used in [1]. Finally, the accuracy rates of liveness tests can be boosted with the use of specialized hardware. Socolinsky et al. [14] analyzed face thermograms acquired by a thermal imaging camera, while Steiner et al. [15] recently proposed a liveness test based on the analysis of the spectral signatures in the infrared.

3 IMPLEMENTATION

In [16], Tan et al. proposed a series of liveness tests where information sensitive to the reflectance properties of the scene is extracted from the image and it is used to train a binary classifier so that it can distinguish between images of live faces and images of photos of faces. The variant we implemented extracts a *difference of Gaussians* from the image and uses it to train a sparse logistic regression classifier. The implementation was done in Matlab and the *SLEP* package was used for the sparse logistic regression.

Following the recommendation in [16], we smooth the image using Gaussian filters with $\sigma_1 = 0.5$ and $\sigma_2 = 1.0$ and compute the difference of the two smoothed images. Regarding the machine learning part of the algorithm, following the notation and parameter choices in [16], we use the class labels $\{-1, 1\}$, where -1 corresponds to client images and 1 to imposter images and the conditional probability of the the imposter class $y = 1$ is given by

$$\text{Prob}(y|x) = \frac{1}{1+\exp(-y(w^T x+b)} \tag{1}$$

where x is the sample image, and w and b are the weight vector and the intercept. To avoid overfitting, the values of w and b are computed through the minimization of the cost function

$$\min_{w,b} \text{loss}(w,b) + \lambda \|w\|_1 \tag{2}$$

where λ is a user defined constant favoring sparse weight vectors and loss given by

$$\text{loss}(w,b) = \frac{1}{m}\sum_{i=1}^{m} \log(1+\exp(-y_i(w^T x_i+b))) \tag{3}$$

where m is the size of the training set of images x_i with associated labels y_i.

The choice of λ has a significant effect in the performance of the algorithm and depends on the size of the training set. In our implementation, using a training set of 1000 images we found experimentally that $\lambda = 0.25$ gives good results. Figure 2 (top) shows the ROC curves of the liveness test for several values of λ.

3.1 Experimental design

We used the NUAA Photograph Imposter Database, which contains grayscale images of 15 different subjects in various poses under different illumination conditions. The images are organized into the two categories: the *client images* which are images of live faces, and the *imposter images* which are images of photos of the subjects. The size of all images is 64×64 pixels.

Our training dataset consisted of 1000 client and imposter images. The test set consisted of several subsets,

Figure 1: Test images. From left to right: (i) client, (ii) imposter, (iii) sharpened imposter, (iv) sharpened and blurred imposter, (v) imposter with salt and pepper noise added to it.

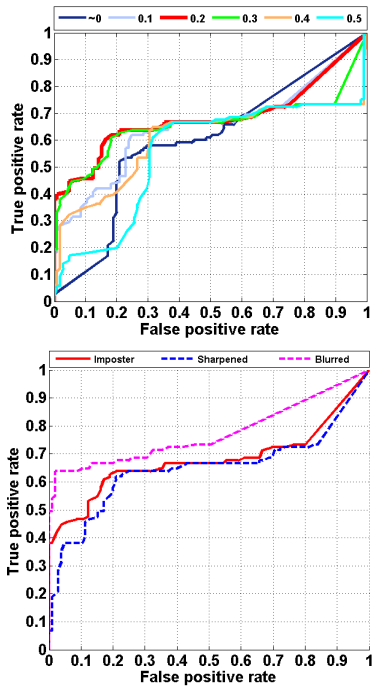

Figure 2: **Top:** ROC curves for several values of λ. **Bottom:** ROC curves for the unaltered imposter images in test set (ii); the sharpened images in (iii); and the sharpened blurred images in (vi) with $\sigma = 1.25$.

each one containing 105 images, i.e. seven from each subject. More specifically, we used test sets of:

(i) client images.

(ii) imposter images without any alteration.

(iii) imposter images sharpened by subtracting from them the response of the Laplacian filter.

(iv) imposter images sharpened with the *imsharpen* Matlab function with parameter values 0.5, 1.0, 1.5 and 2.0.

(v) the sharpened imposter images in (iii) are blurred with a Gaussian filter with $\sigma = 0.1$, 0.5, 1.25 and 2.0.

(vi) imposter images with 0.01, 0.1, 0.5 and 0.9 amount of added salt and pepper noise.

Figure 1 shows typical examples of test set images.

4 RESULTS

Figure 2 (bottom) shows the ROC curves of the liveness test when the imposter test images are either sharpened by subtracting from them the response of the Laplacian filter, or first sharpened and then blurred by a Gaussian filter. The performance decreased when the imposter images were sharpened even with the very basic sharpening algorithm we used. The performance increased when the imposter images were first sharpened and then smoothed, further demonstrating the the sharpness of the image is a key factor in distinguishing between client and imposter images.

Next we want to establish that the differences in the performance of the liveness test are commensurable with the amount of sharpening and blurring applied on the imposter images. Figure 3 (left) shows the ROC curves when the imposter images are sharpened using the *imsharpen* Matlab function which subtracts from the images a blurred version of it. The strength of the *imsharpen* command is controlled by a user defined parameter and we used values of 0.5, 1.0, 1.5 and 2.0. We notice that larger amounts of sharpening on the imposter images result into larger decreases in the performance of the liveness test. Similarly, in Figure 3 (middle) we show the ROC curves when the Laplacian filter sharpened imposter images are blurred with Gaussian filters with $\sigma = 0.1$, 0.5, 1.25 and 2.0, respectively. We notice that larger amounts of smoothing result to larger increases in the performance of the liveness test.

Finally, we experimented with the addition of various amounts of salt and pepper noise on the imposter images. This test is relevant in our context since in [10] it was shown that commercial face recognition systems can cope with large amounts of salt and pepper noise and as a consequence they are also vulnerable to imposter image attacks even when imposter images contain large amounts of salt and pepper noise. Figure 3 (right) shows the results when salt and pepper noise with probability 0.01, 0.1, 0.5 and 0.9 was added. We notice that the addition of noise increases the performance of the liveness test and the performance gain is commensurable with the amount of added noise.

5 CONCLUSIONS

In a real life situation, we should expect that an attacker will process an imposter photo before using it, increasing their chances of successfully evading a liveness test. Motivated by that observation, we evaluated the resilience of a standard luminance based liveness

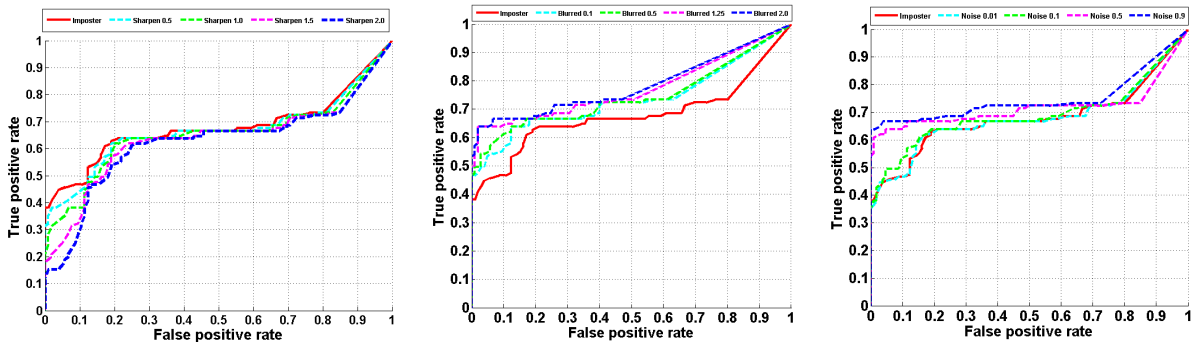

Figure 3: From left to right: ROC curves for the liveness test with different amounts of sharpening, blurring and salt and pepper noise applied on the imposter images.

test in conjunction with certain image processing operations of the imposter database. Our results verified and quantified the assumption that luminance based tests rely on the different amount of sharpness between images of live faces and imposter images. In particular, the sharpening of the imposter images decreased the accuracy of the liveness test while sharpening followed by smoothing increased accuracy rates.

While we expect that the sharpening of an imposter image before using it for an attack will result into a sharpening of the image acquired by the face recognition system, this is an assumption that still has to be verified. Thus, in the future we plan to simulate and evaluate imposter image attacks that use processed images.

6 REFERENCES

[1] A. Anjos, M.M. Chakka, and S. Marcel. Motion-based counter-measures to photo attacks in face recognition. *IET Biometrics*, 3(3):147–158, 2014.

[2] W. Bao, H. Li, N. Li, and W. Jiang. A liveness detection method for face recognition based on optical flow field. In *IEEE IASP*, pages 233–236, 2009.

[3] J. Galbally, J. Fierrez, J. Ortega-Garcia, C. McCool, and S. Marcel. Hill-climbing attack to an eigenface-based face verification system. In *BIdS*, pages 1–6, 2009.

[4] J. Galbally, S. Marcel, and J. Fierrez. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Trans. on Image Processing*, 23(2):710–724, 2014.

[5] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition*, 43(3):1027–1038, 2010.

[6] K. Kollreider, H. Fronthaler, M.I. Faraj, and J. Bigun. Real-time face detection and motion analysis with application in "liveness" assessment. *IEEE Trans. on Information Forensics and Security*, 2(3):548–558, 2007.

[7] J. Komulainen, A. Hadid, and M. Pietikainen. Context based face anti-spoofing. In *IEEE BTAS*, pages 1–8, 2013.

[8] J. Maatta, A. Hadid, and M. Pietikainen. Face spoofing detection from single images using micro-texture analysis. In *IEEE IJCB*, pages 1–7, 2011.

[9] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12):1643–1651, 2011.

[10] L. Omar and I. Ivrissimtzis. Evaluating the resilience of face recognition systems against malicious attacks. In *BMVW*, 2015.

[11] G. Pan, L. Sun, and Z. Wu. *Liveness detection for face recognition*. INTECH Open Access Publisher, 2008.

[12] G. Pan, L. Sun, Z. Wu, and S. Lao. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *IEEE ICCV*, pages 1–8, 2007.

[13] B. Peixoto, C. Michelassi, and A. Rocha. Face liveness detection under bad illumination conditions. In *IEEE ICIP*, pages 3557–3560, 2011.

[14] D.A. Socolinsky, A. Selinger, and J.D. Neuheisel. Face recognition with visible and thermal infrared imagery. *Computer Vision and Image Understanding*, 91(1):72–114, 2003.

[15] H. Steiner, S. Sporrer, A. Kolb, and N. Jung. Design of an active multispectral swir camera system for skin detection and face verification. *Journal of Sensors*, 2016, 2015.

[16] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In *ECCV*, pages 504–517, 2010.