Biometric Counter-Spoofing for Mobile Devices Using Gaze Information

Asad Ali, Nawal Alsufyani, Sanaul Hoque, and Farzin Deravi

School of Engineering and Digital Arts, University of Kent, Canterbury, Kent CT2 7NT, UK
F.Deravi@kent.ac.uk

Abstract. With the rise in the use of biometric authentication on mobile devices, it is important to address the security vulnerability of spoofing attacks where an attacker using an artefact representing the biometric features of a genuine user attempts to subvert the system. In this paper, techniques for presentation attack detection are presented using gaze information with a focus on their applicability for use on mobile devices. Novel features that rely on directing the gaze of the user and establishing its behaviour are explored for detecting spoofing attempts. The attack scenarios considered in this work include the use of projected photos, 2D and 3D masks. The proposed features and the systems based on them were extensively evaluated using data captured from volunteers performing genuine and spoofing attempts. The results of the evaluations indicate that gaze-based features have the potential for discriminating between genuine attempts and imposter attacks on mobile devices.

Keywords: Biometrics · Spoofing · Presentation attacks · Mobile security · Liveness detection

1 Introduction

Spoofing attacks on biometric systems are one of the major impediments to their use for secure unattended applications. With the growing use of biometric authentication on mobile devices, this problem may need special attention in the context of the limitations of such devices. This study will address the threat of spoofing attacks on mobile biometric systems using artefacts presented at the sensor (e.g. projected photograph, 2D mask or 3D mask of a genuine user). The focus will be on the development and evaluation of liveness detection and counter-spoofing technologies based on eye-gaze in operational mobile scenarios. Such technologies can enhance the trust and reliability of remote communications and transactions using the increasingly prevalent mobile devices.

Various approaches have been presented in the literature to establish "liveness" and to detect presentation attacks. Spoofing detection approaches can be grouped into two broad categories: active and passive. Passive approaches do not require user co-operation or even user awareness but exploit involuntary physical movements, such as spontaneous eye blinks, and 3D properties of the image source [1–13]. Active approaches require user engagement to enable the biometric system to establish the liveness of the

B.U. Shankar et al. (Eds.): PReMI 2017, LNCS 10597, pp. 11–18, 2017.
https://doi.org/10.1007/978-3-319-69900-4_2

source through an evaluation of the sample captured at the sensor [14–23]. In this work, we present a novel active approach using gaze information for liveness detection for application on mobile devices. Section 2 presents the proposed system. Experimental results and a comparison with the state-of-the-art is presented in Sect. 3 while conclusions are provided in Sect. 4.

2 Liveness Detection Through Gaze Tracking

A block diagram of the proposed system is shown in Fig. 1. A visual stimulus (as part of the challenge) appears on the display which the participant is asked to follow and the camera (sensor) captures facial images at each position of the stimulus on the screen. A control mechanism is used to ensure that the placement of the target and the image acquisition are synchronized. The system extracts facial landmarks in the captured frames and computes various features from these landmarks which are then used to classify whether the presentation attempt is by a genuine user. The spoofing attack may be by means of an impostor attempting authentication by holding a projected photo, 2D or 3D mask of a genuine subject to the camera.

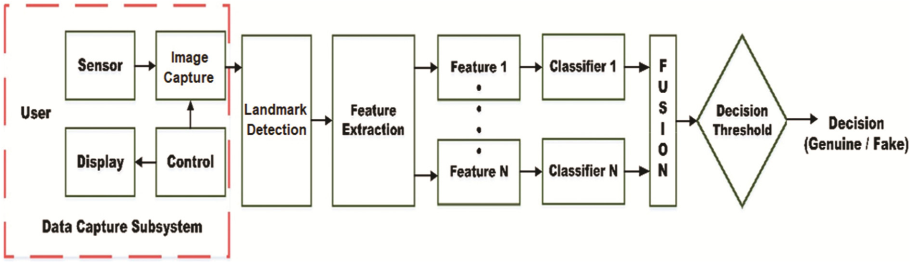
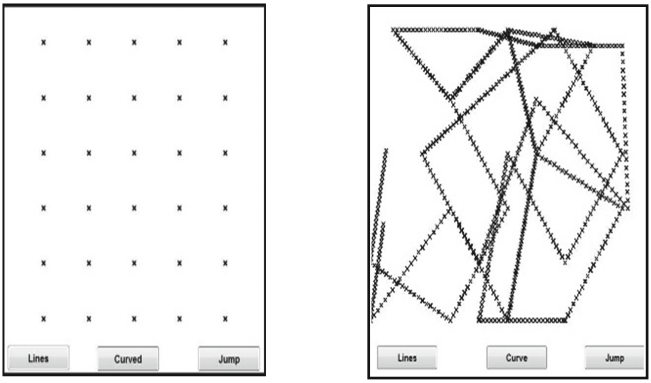


Fig. 1. Proposed system block diagram.

2.1 A Subsection Sample

The restricted geometry of a mobile phone display (6.45 × 11.30 cm) is simulated in the experiments that follow using a limited area of a desktop computer screen. A small shape (“x”) is presented, at distinct locations on the screen as shown in Fig. 2. In this figure, the cross indicates the chosen locations in which the cross sign appears in 30 distinct locations (Points Challenge) (Fig. 2(a)) and along straight-line trajectories (Lines Challenge) (Fig. 2(b)). The order of points and lines is randomised for each presentation. During each presentation attempt images were acquired at every location of the challenge. The presentation of the challenge sequence lasted approximately 90 s, however, a small section of each session was used for spoofing detection.



(a) (b)

Fig. 2. Samples of challenge trajectory: (a) Points challenge, (b) Lines challenge.

Data was collected from 80 participants. This number of participants is sufficient to illustrate the potential of the proposed approach and is in line with current state-of-the-art. Participants were of both male and female gender aged over 18 years old. The volunteers were from Africa, Asia, Middle-East, and Europe. Three spoofing attempts (photo projection, 2D mask, 3D mask) and one genuine attempt for each challenge type (Points and Lines) were recorded for each participant.

2.2 Facial Landmark Detection and Feature Extraction

The images thus captured during the challenge-response operation were processed using Chehra Version 3.0 [24] in order to extract facial landmark points. Chehra returns 59 different landmarks on the face region. The coordinates of some of these landmarks were used for feature extraction in the proposed scheme. Features proposed here are based on eye movements during the challenge presentation.

2.3 Gaze-Based Collinearity and Colocation Features

A set of points lying on a straight line is referred to here as a collinear set and this property of collinearity is used for detecting presentation attacks. Collinearity features are, therefore, extracted from sets of images captured when the stimulus is on a given line. The novel gaze-based collinearity feature explored in this paper is designed to capture significant angular differences between the stimulus trajectory and the trajectory of the participant's pupil movement for each line segment.

Let (x_i, y_i) be points on the trajectory of the challenge, where the stimulus moves on a straight line, and (u_i, v_i) are the corresponding facial landmarks (e.g., pupil centres). Let θ_c be the angle of the challenge calculated using any two points along the line of the trajectory.

$$\theta_c = tan^{-1}\left(\frac{y_j - y_i}{x_j - x_i}\right) \tag{1}$$

Let θ_r be the angle of the response trajectory. The response angle is calculated using the Least Squares regression method as shown:

$$\theta_r = tan^{-1}\left(\frac{\sum\left(u_i - \bar{u}\right)\left(v_i - \bar{v}\right)}{\sum\left(u_i - \bar{u}\right)^2}\right) \tag{2}$$

The feature vector is then defined as the absolute difference between these two angles $\Delta\theta(= |\theta_c - \theta_r|)$ for each of the line segments included in the challenge.

$$F_{collin} = \left[\Delta\theta_1, \Delta\theta_2, \ldots\right] \tag{3}$$

For the colocation feature, the Points stimulus is used, causing the user to fixate on a number of random locations on the screen. At each stimulus location, the facial image of the user is captured. The gaze colocation features are extracted from images where the stimulus is at the same locations at different times. It can, therefore, be assumed that the coordinates of the pupil centres in the corresponding frames should also be very similar. This should result in a very small variance, σ^2, in the observed coordinates of the pupil centres in genuine attempts. A feature vector is thus formed from the variances of pupil centre coordinates for all the frames where the stimulus is colocated. These variances are calculated for the horizontal and vertical directions independently,

$$\sigma_u^2 = \frac{1}{M}\sum\nolimits_i\left(u_i - \bar{u}\right)^2 \tag{4}$$

$$\sigma_v^2 = \frac{1}{M}\sum\nolimits_i\left(v_i - \bar{v}\right)^2 \tag{5}$$

where $\bar{u}$ and $\bar{v}$ are the mean of the observed landmark locations and M is cardinality of the corresponding subset of response points. These variances are concatenated together to form the feature vector as shown below:

$$F_{coloc} = \left[\sigma_u^2, \sigma_v^2, \ldots\right] \tag{6}$$

The features are passed to the classifier to detect attack attempts.

3 Experiments

The ROC curves using gaze-based colocation features are presented in Fig. 3 for photo attack (by displaying on an iPad Mini 2), 2D mask attack (using printed photos with holes at pupils) and 3D mask attack (using life-size 3D model made of hard resin with holes at pupils) detection. This experiment was conducted for the mobile Phone format using 10 sets of colocated points (amounting to a challenge duration of 30 s). At 10%

FPR, the TPR is 90% for photo attack. The performance is about 21 and 29% TPR for 2D mask and 3D mask respectively. Photo attack is easier to detect using this feature. 2D and 3D mask attacks are challenging and difficult to discriminate from genuine presentations using this feature.

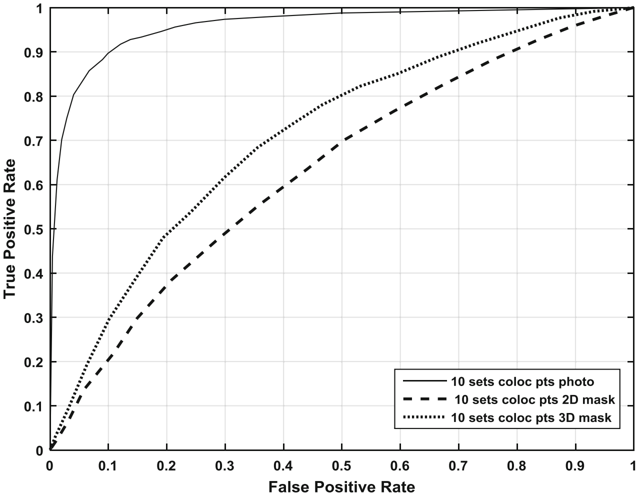


Fig. 3. ROC curves for photo, 2D mask and 3D mask for 10 sets of colocation points (approximately 30 s of challenge duration).

Table 1 summarizes the TPRs at FPR 0.10 for various sets of colocation points representing different challenge durations ranging from 9 s (3 colocated sets of points) to 45 s (15 colocated sets of points). The lowest performance is noticed for 2D and 3D mask attacks. Increasing the challenge duration did not significantly improve the results.

Table 1. TPR at FPR = 0.10 for various sets of colocation points

Attack type	Sets of collocated points		
	3	10	15
Photo	82%	90%	88%
2D mask	9%	21%	25%
3D mask	18%	29%	30%

In summary, it appears that the colocation feature does not work effectively when used with the smaller geometries of mobile devices in detecting 2D and 3D mask attacks. While it is effective in detecting photo attacks, the minimum challenge duration for the feature is around 9 s.

The ROC curves using collinearity features are presented in Fig. 4 for all attack scenarios for five line segments representing approximately 5 s of challenge duration. At 10% FPR, the TPR is 95%, 88% and 87% for photo, 2D and 3D mask attack detection respectively.

Although several lines are shown in the trajectory in Fig. 2b, only five consecutive line segments (picked at random) have been used for this analysis.

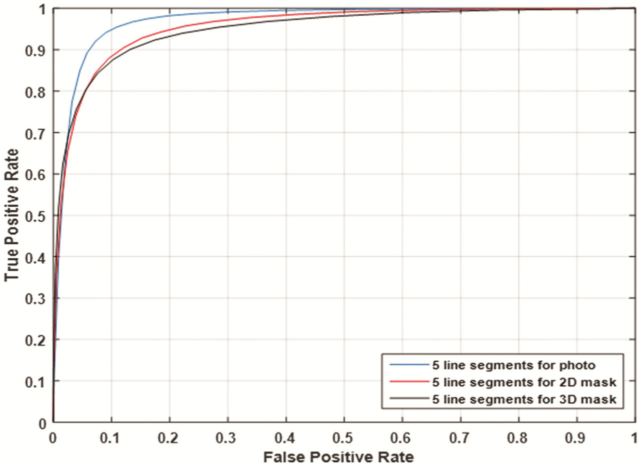


Fig. 4. ROC curves for photo, 2D mask, and 3D mask for 5 sets of line segments (approximately 5 s) for collinearity feature.

Changing the number of lines used has a significant effect not only on the execution time but also on accuracy.

Table 2 summarize the TPRs at FPR = 0.10 for various numbers of lines included in a challenge presentation. The proposed system was able to detect a majority of attacks when using a set of five line segments. When increased to 10 line segments, the performance is significantly improved, however, it drops to 83%, 62% and 62% for photo, 2D mask and 3D mask attack respectively when only three lines are used.

Table 2. TPR at FPR = 0.10 for various sets of lines of collinearity

Attack type	Number of line segments		
	3	5	10
Photo	83%	95%	99%
2D mask	62%	88%	97%
3D mask	62%	87%	99%

In summary, the collinearity feature appears to be more effective in detecting all the attack types compared with the colocation feature; even when the challenge duration is as low as 3 s.

Table 3 presents a comparison of the performance results obtained using the proposed novel collinearity feature with results reported in the literature. It is difficult to make a direct comparison between these results due to the different databases used for system evaluation and the novel and unique way that the challenge response mechanism is deployed in our proposed system. However, the results are very promising and indicate the potential of the proposed features and approach to substantially exceed current performance limits.

Table 3. FPR and FNR for various methods

	Method	FPR	FNR
Collinearity 10 s	Kollreider *et al.* [22]	1.5%	19.0%
	Tan *et al.* cf. [7]	9.3%	17.6%
	Peixoto *et al.* [7]	6.9%	7.0%
	Photo Detection	6.0%	2.2%
	2D Mask Detection	6.0%	7.8%
	3D Mask Detection	6.0%	2.4%

The choice of operating points on the ROC curve that determines the balance between FPR and FNR should be set according to the needs of particular applications. The proposed system allows for considerable flexibility in adjusting the system parameters to meet the needs of different applications.

4 Conclusion

This work reports on an investigation of novel gaze-based features for liveness detection on mobile devices. The research extends the authors' previous works on gaze-based presentation attack detection using enhanced features, mobile device geometry and additional attack artefacts. The work explored not only presentation of static photographs using another mobile device as the attack instrument but also the use of 2D and 3D masks representing different attack effort levels required by potential attackers. An important part of this work was evaluating the system with a large database (80 subjects) of genuine and attack presentations simulating mobile access scenarios.

The main conclusion of this investigation is to suggest that gaze information when captured in smaller device geometries such as those available on mobile phones has the potential to discriminate between genuine and subversive attempts.

References

1. Sun, L., Pan, G., Wu, Z., Lao, S.: Blinking-based live face detection using conditional random fields. In: Lee, S.-W., Li, S.Z. (eds.) ICB 2007. LNCS, vol. 4642, pp. 252–260. Springer, Heidelberg (2007). doi:10.1007/978-3-540-74549-5_27
2. Pan, G., Sun, L., Wu, Z., Lao, S.: Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In: IEEE 11th International Conference on Computer Vision (ICCV), pp. 1–8 (2007)
3. Schwartz, W.R., Rocha, A., Pedrini, H.: Face spoofing detection through partial least squares and low-level descriptors. In: International Joint Conference on Biometrics (IJCB), pp. 1–8 (2011)
4. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing. In: Proceedings of IEEE BIOSIG, pp. 1–7 (2012)
5. Pinto, A., Schwartz, W.R., Pedrini, H., Rocha, A.: Using visual rhythms for detecting video-based facial spoof attacks. IEEE Trans. Inf. Forensics Secur. **10**(5), 1025–1038 (2015)

6. Maatta, J., Hadid, A., Pietikainen, M.: Face spoofing detection from single images using texture and local shape analysis. IET Biometrics **1**(1), 3–10 (2012)
7. Peixoto, B., Michelassi, C., Rocha, A.: Face liveness detection under bad illumination conditions. In: 18th IEEE International Conference on Image Processing, pp. 3557–3560 (2011)
8. Wen, D., Han, H., Jain, A.K.: Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics Secur. **10**(4), 746–761 (2015)
9. Georghiades, A.S., Belhumeur, P.N., Kriegman, D.J.: From few to many: illumination cone models for face recognition under variable lighting and pose. IEEE Trans. Pattern Anal. Mach. Intell. **23**(6), 643–660 (2001)
10. Anjos A., Marcel, S.: Counter-measures to photo attacks in face recognition: a public database and a baseline. In: 2011 International Joint Conference on Biometrics (IJCB), pp. 1–7 (2011)
11. Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., Sridharan, S.: Liveness detection based on 3d face shape analysis. In: International Workshop on Biometrics and Forensics (IWBF), pp. 1–4 (2013)
12. Wang, T., Yang, J., Lei, Z., Liao, S., Li, S.Z.: Face liveness detection using 3d structure recovered from a single camera. In: 2013 International Conference on Biometrics (ICB), pp. 1–6 (2013)
13. De Marsico, M., Galdi, C., Nappi, M., Riccio, D.: Firme: face and iris recognition for mobile engagement. Image Vis. Comput. **32**(12), 1161–1172 (2014)
14. Frischholz R.W., Werner, A.: Avoiding replay-attacks in a face recognition system using head-pose estimation. In: IEEE International Workshop on Analysis and Modeling of Faces and Gestures (AMFG), pp. 234–235 (2003)
15. Ali, A., Deravi, F., Hoque, S.: Liveness detection using gaze collinearity. In: 2012 Third International Conference on Emerging Security Technologies (EST), pp. 62–65 (2012)
16. Ali, A., Deravi, F., Hoque, S.: Spoofing attempt detection using gaze colocation. In: 2013 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–12 (2013)
17. Ali, A., Deravi, F., Hoque, S.: Directional sensitivity of gaze-collinearity features in liveness detection. In: 4th International Conference on Emerging Security Technologies (EST), pp. 8–11 (2013)
18. Singh, A.K., Joshi, P., Nandi, G.C.: Face recognition with liveness detection using eye and mouth movement. In: 2014 International Conference on Signal Propagation and Computer Technology (IC- SPCT), pp. 592–597 (2014)
19. Smith, D.F., Wiliem, A., Lovell, C.: Face recognition on consumer devices: reflections on replay attacks. IEEE Trans. Inf. Forensics Secur. **10**(4), 736–745 (2015)
20. Boehm, A., Chen, D., Frank, M., Huang, L., Kuo, C., Lolic, T., Martinovic, I., Song, D.: Safe: secure authentication with face and eyes. In: 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8 (2013)
21. Cai, L., Huang, L., Liu, C.: Person-specific face spoofing detection for replay attack based on gaze estimation. In: Yang, J., Yang, J., Sun, Z., Shan, S., Zheng, W., Feng, J. (eds.) Biometric Recognition. LNCS, vol. 9428, pp. 201–211. Springer, Cham (2015). doi: 10.1007/978-3-319-25417-3_25
22. Kollreider, K., Fronthaler, H., Bigun, J.: Evaluating liveness by face images and the structure tensor. In: 4th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2005), pp. 75–80 (2005)
23. Ali, A., Hoque, S., Deravi, F.: Gaze stability for liveness detection. Pattern Anal. Applic. (2016). doi:10.1007/s10044-016-0587-2
24. Asthana, A., Zafeiriou, S., Cheng, S., Pantic, M.: Incremental face alignment in the wild. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1859–1866 (2014)