PRESENTATION ATTACK DETECTION ON FACE RECOGNITION SYSTEMS IN MOBILE DEVICES

Artur Costa-Pazo, Esteban Vazquez-Fernandez and José Luis Alba-Castro

Motivation of the work

Access to personal data using our smartphones has become a part of normal everyday life. It is common to use passwords, unlock patterns, as well as biometric recognition systems for accessing securely to our social networks, bank apps, etc. For face recognition to become widespread on mobile devices' authentication systems, robust countermeasures must be developed for face Presentation Attack Detection (PAD). Existing databases for evaluating face-PAD are not fairly comparable (differences on capture process, protocols under analysis, etc). Moreover, the existing mobile face-PAD methods have shown lack of generalization in real-world scenarios. Current systems obtain decent performance in the intra-dataset analysis, but this decreases considerably when tested on different datasets. Therefore, our work is focused on analysing the current challenges of face-PAD in real scenarios, create a framework for fairly comparison of face-PAD between main public available databases, and finally, propose novel face-PAD techniques that will be able to generalize between different conditions.

Thesis Objectives

Analysis of the challenges of face-PAD in Real Scenarios

Analyse and categorize the current challenges of face-PAD, reviewing the current anti-spoofing methods available in today's commercial face recognition systems for mobile authentication.

A Fair Evaluation Framework

Create a fair evaluation framework for testing face-PAD systems considering constraints of the actual world. Consider creating new metrics for face-PAD comparison.

Improve face-PAD with ensembles and data generation techniques

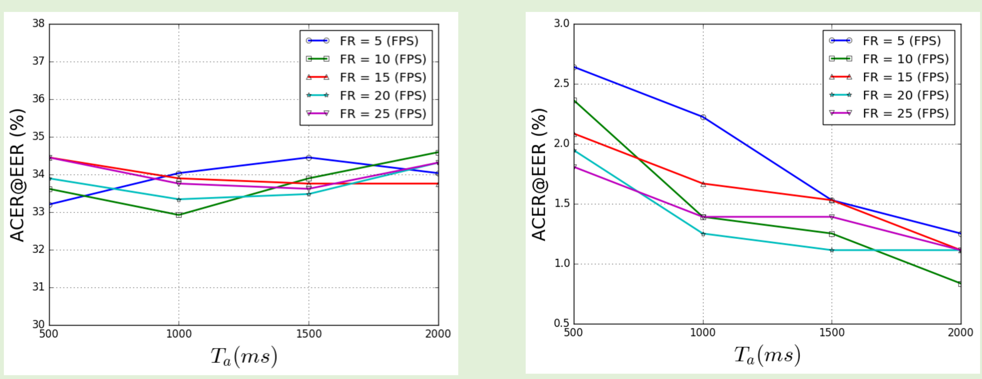
Mitigate the non-representability of current publicly available datasets categorising a wide range of attacks, and proposing new techniques for data augmentation. Study the combination of different experts face-PAD using ensembles.

Results

We have reviewed the **Challenges of Face Presentation Attack Detection in Real Scenarios** on our accepted chapter on the Handbook of Biometric Anti-Spoofing (2nd Edition). In that work, we have designed a novel evaluation framework to better model the performance of a face-PAD method on a real application. The following evaluation procedures will help us to research some unstudied parameters and their influence in the performance of a deployed system.

- **Algorithmic Unconstrained Evaluation**, or *AUE* is the given name for a classical algorithmic evaluation. On this stage, every method is evaluated following defined database protocols, without any constraint about on-device implementation (i.e. T_a or *FR*). This classical evaluation is still fundamental in order to provide a fair performance comparison in terms of error rates, so we propose it to be the starting point for the design, develop and parametrization process of a face-PAD method. The calculated error rates and working points on this evaluation are only reliable for an unconstrained comparison of the algorithm, since unrestricted video duration and frame rate are used. These results and parameters should not be considered on a real implementation, nevertheless they can help on the initial parameterization of the algorithm.
- **Algorithmic Constrained Evaluation**, or *ACE*, provides information about performance and error rates related to an actual deployment constraints. More specifically, *FR* (frame rate) and T_a (total time of acquisition). This stage consists of evaluating a method cloning each input video but simulating different acquisition settings, obtaining, this way, valuable information to forecast the face-PAD performance. From this evaluation we can determine the best configuration of a face-PAD accompanied by a *WorkingPoint* (normally represented by a *Threshold*) for a given *FR* and T_a.
- **End-to-end Evaluation**: Once a parameterization laboratory was finished (using both of previous evaluation stages), it is necessary to evaluate the whole system (determined by optimum *FR*, T_a and a *WorkingPoint*). This protocol simulates the final behaviour of a face-PAD on an actual deployment using a bunch of videos. This end-to-end evaluation provides interesting information about the actual conditions on T_r (total time of system response), T_d (time of decision) and CPU_{usage} over a selected subset of videos. Although this evaluation is very useful for an initial decision concerning implementation parameters, we should keep in mind that it does not replace the end-to-end tests running in an actual production device.

Algorithmic Constrained Evaluation



(a) Texture-based face-PAD method (IQM)

(b) Motion-based face-PAD method (GRADIANT)

Fig. 2 The performance of a pre-trained face-PAD under different configurations (*FR* and *Ta*) on *OULU-NPU* dataset (Grandtest protocol and Algorithmic Constrained Evaluation).

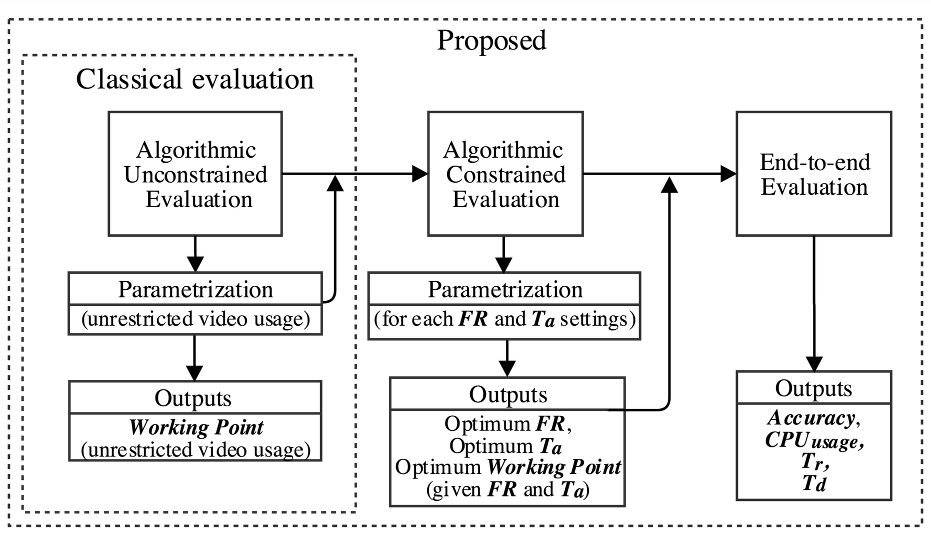


Fig. 1 Overview of our proposed evaluation framework.

Classical Evaluation

Method	Dev	Test	
	EER(%)	HTER(%)	ACER(%)
IQM	29.72	29.23	30.69
GRADIANT	1.11	0.76	0.97

Table 1 The performance of the proposed methods under OULU-NPU (Grandtest) measured through a classical evaluation.

End-to-end Evaluation

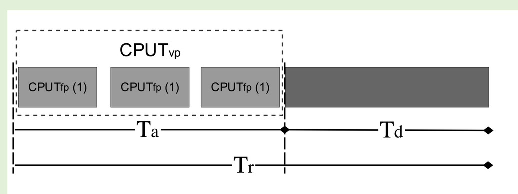


Fig. 3 Breakdown of biometric procedure in terms of computational demand.

$$CPUT_{vp} = \sum_{i=1}^{n} CPUT_{fp}(i) \quad (1)$$

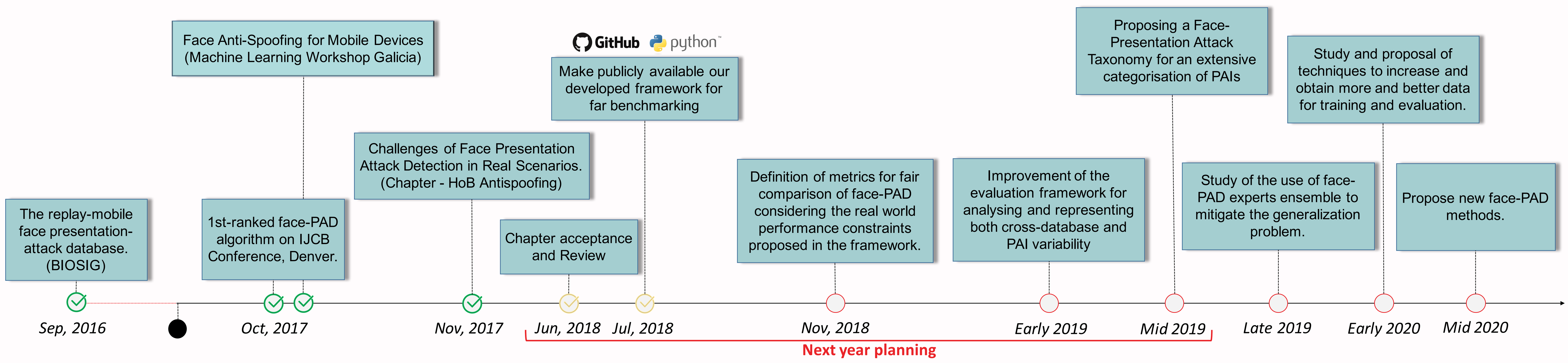
$$T_r = \max(T_a, CPUT_{vp}) + T_d \quad (2)$$

$$CPU_{usage} = \frac{CPUT_{vp}}{T_a} * 100(\%) \quad (3)$$

Method	CPU usage	T_{vp} (ms)	T_r (ms)	T_a (ms)	T_d (ms)	FR (frames per second)
IQM	2414%	48286.89	48301.89	**2000**	0.15	**25**
GRADIANT	155%	3104.64	3215.05	**2000**	110.41	**10**

Table 2 The end-to-end results for pre-trained *IQM* and *GRADIANT*

Research Plan



References

[1] Boulkenafet, Z et al.: A competition on generalized software-based face presentation attack detection in mobile scenarios. In: IJCB 2017: International Joint Conference on Biometrics, 2017.
[2] Costa-Pazo et al.: The replay-mobile face presentation-attack database. In: Proceedings of the international Conference on Biometrics Special Interests Group (BioSIG), 2016.
[3] Anjos, A et al.: Continuously reproducing toolchains in pattern recognition and machine learning experiments. In: International Conference on Machine Learning (ICML), 2017.
[4] Jackson, Aaron S et al.: Large Pose 3D Face Reconstruction from a Single Image via Direct Volumetric CNN Regression. International Conference on Computer Vision, 2017.
[5] Boulkenafet, Z et al.: Oulu-npu: A mobile face presentation attack database with real-world variations. IEEE International Conference on Automatic Face Gesture Recognition, 2017.
[6] Petel et al: Secure Face Unlock: Spoof Detection on Smartphones. IEEE Transactions on Information Forensics and Security, 2015.

gradiant Connectivity · Intelligence · Security for your business

(+34) 986 120 430 ext 3009 | acosta@gradiant.org

Universida de Vigo