PRESENTATION ATTACK DETECTION ON FACE RECOGNITION SYSTEMS IN MOBILE DEVICES

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

Universidad de Vigo

gradiant
Connectivity · Intelligence · Security
for your business

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. Despite the recent progress, current systems obtain good result analysing the intra-database performance. However, when the analysis of the performance is evaluated on other databases, the results decrease considerably.
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 a novel face-PAD which will be able to generalize between different conditions.

Thesis Objectives

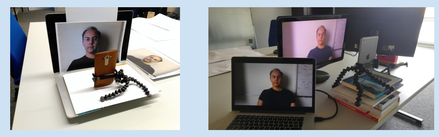
The overall objective of our research is to delve into the face-PAD problem in mobile devices. The following points summarize the main objectives of our work:

- Analyse the current challenges of face-PAD, reviewing the current anti-spoofing methods available in today's commercial face recognition systems for mobile authentication, including hardware-based methods, software-based methods, and their variants and derivatives (fusion, hybrid, multimodal)
- Create an evaluation framework for testing face-PAD systems using the main representative publicity available databases. The new metrics and recommendations presented on the standards ISO/IEC 30107-3 and ISO/IEC 30107-3 will be taken into account.
- Develop automatic face-PAD methods which will be able to achieve reasonable trade-off between usability and security. These methods will be tested and developed on practical mobile applications.

Preliminary Results

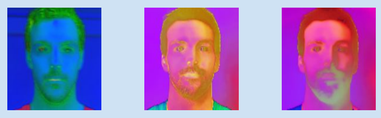
Proposal and commitment for writing a chapter on a book.
Handbook of Biometric Antispoofing

Participation on ***IJCB 2017*** *competition on generalized face presentation attack detection in mobile authentication scenarios* obtaining the **1st rank** across all the four protocols.



(a) Print-PAI (b) screen-PAI

Figure 1: Samples of the different presentations attack instruments, PAI. This database [4] was captured within the framework of collaboration between Idiap and Gradiant.



(a) Real access (b) Print-PAI (c) Screen-PAI

Figure 2: Preliminary method which extracts dynamic information over a given video sequence and maps the temporal variations into a single image.

Check results of the competition at: https://sites.google.com/site/faceantispoofing/results

Research Plan

Analysis of Presentation Attack Detection in Real Scenarios

- Review the available face presentation attack datasets and analyse their goodness and limitations.
- Analyse the existing gap between the research process and real scenario deployment for this case of mobile scenarios, including **generalisation** and **usability.**
- Point out the main threats and challenges that should drive the near-future research in order to meet mobile scenario security requirements.

Evaluation Framework

- Use standard evaluation to compare our systems over public databases.
- Creation of a public fair evaluation framework for PAD systems.
  - Design protocols which allows researchers to compare their system in the same conditions.
  - New measurement recommendations (*APCER, BPCER* and *ACER*)
  - Prepare suite for evaluation.

Develop robust face-PAD in mobile devices

Develop Automatic methods

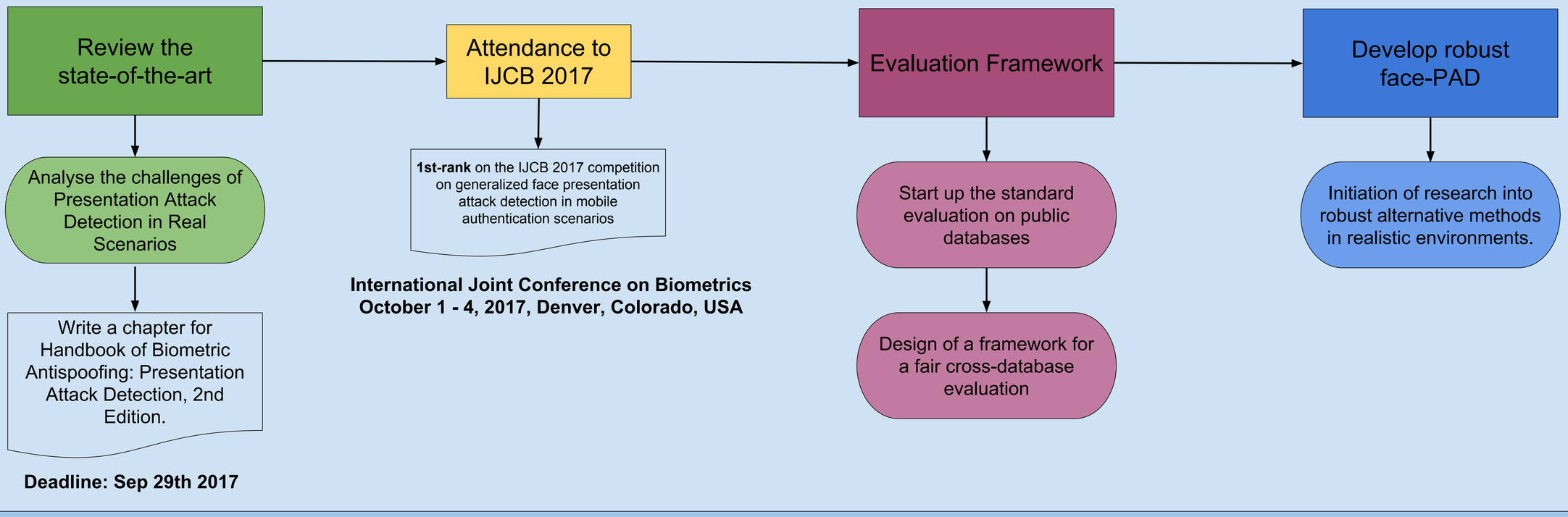
motion based | texture based | color based

Fusion, face landmarks, etc..

Analysis of collaborative methods

These methods imply challenge-response strategies (eye blinking, smiling, looking at different directions, etc…)

Next year planning



References

[1] The 2nd competition on counter measures to 2D face spoofing attacks, Ivana Chingovska, et al., in: International Conference of Biometrics 2013, Madrid, Spain, 2013
[2] Can face anti-spoofing countermeasures work in a real world scenario?, Tiago de Freitas Pereira, André Anjos, José Mario De Martino and Sébastien Marcel, in: International Conference on Biometrics, Madrid, Spain, 2013
[3] Secure Face Unlock: Spoof Detection on Smartphones, K. Patel, H. Han and A. K. Jain, in: IEEE Transactions on Information Forensics and Security
[4] The REPLAY-MOBILE Face Presentation-Attack Database, Artur Costa-Pazo, Sushil Bhattacharjee, Esteban Vazquez-Fernandez, Sebastien Marcel, in: IEEE biometrics international conference of the special interest group. BIOSIG, Darmstadt, Germany, 2017.

acosta@gradiant.org