

Secure Face Spoof Detection on Smartphone

Wakchaure Arti, Bamhane Swapnil, Bhor Ashwini, Varal Mohini

Student, Dept. of Computer Engineering,

SGOI COE, Belhe, Pune, Maharashtra, India

Abstract - Now a day, smart phone users are increasing rapidly. Information access from Smart-phones and tablets has become main stream both in business and personal environments over the last years. The use of these devices for accessing services like social networks, email or electronic commerce and banking has surpassed the access from traditional computers, turning mobile devices into essential tools in our everyday life. People use simple passwords, they reuse them on different accounts and services, passwords can be shared and cracked, etc. As a result, biometric technologies are now offered as alternatives to passwords, including face authentication on devices with front-facing cameras. However, face authentication is vulnerable to spoofing attacks, to address these issues with face authentication, we take the first step to design Secure Face Detection System On Smart-phone for device unlock. Meanwhile, most of existing databases only concentrate on the antispoofing of different kinds of attacks and ignore the environmental changes in real world applications. In proposed system, we focus on public-domain face spoof databases will show that the proposed approach is effective in face spoof detection for both cross-database and intra-database testing scenarios.

Key Words: Image aliasing, smart phone security, phone unlock, print attack, replay attack.

1. INTRODUCTION

Security in the access to information is one of the most important issues to consider in mobility scenarios. Passwords have been the usual mechanism for user authentication for many years. However, there are many usability and security concerns that compromise their effectiveness. People use simple passwords, they reuse them on different accounts and services, passwords can be shared and cracked, etc. The amount of different accounts and passwords we deal with these days contributes in making harder the proper usage and maintenance. As a result, we often see news and reports that alert of stolen accounts and passwords. This problem becomes critical in mobile devices, since they can be easily lost or stolen. Nevertheless, mobile devices can also become part of the solution, providing increased levels of security due to their new authentication options and capabilities.

As the increasing deployment of face recognition in a variety of applications, its security concern becomes increasingly important. Like the other biometric modalities, a major security issue is to detect the spoofing attack. Traditionally, photos and videos are the two medium to

carry out the face spoofing attack. In order to detect them, numbers of methods have been proposed and achieved promising results.

In this paper, we focus on video replay attacks (display video or photo on a screen) because these attacks are easier to launch than either printed photo attack. Replay video attacks can be easily launched simply using a Smartphone to obtain a photograph or video of the target subject. We study the problem of face spoof detection on Smartphone using a large unconstrained Smartphone spoof attack database, and provide a sample face spoof detection system running on Android. This paper expands upon our preliminary work in the following ways:

- We analyse the image distortion of print and replay attacks using different
 - ◆ Intensity channels (R, G, B and grayscale)
 - ◆ Image regions (whole face image, detected face)
 - ◆ Feature descriptors
- Analyses of face liveness.
- Determining the spoof faces by comparing RGB colour value with existing face and live face smile and eye detection to efficiently reject
- Verifying the drawn conclusion by using detected face and RGB colour value.
- Implementation of the proposed method on Android Smartphone

2. Literature Survey

X. Tan, Y. Li, J. Liu, and L. Jiang, present a real-time and non-intrusive method to address this based on individual images from a generic web camera. The task is formulated as a binary classification problem, in which, however, the distribution of positive and negative are largely overlapping in the input space, and a suitable representation space is hence of importance. Using the Lambertian model, we proposed two strategies to extract the essential information about different surface properties of a live human face or a photograph, in terms of latent samples. Based on these, we developed two new extensions to the sparse logistic regression model which allow quick and accurate spoof detection.

J. M'a'atta, A. Hadid, and M. Pietik'ainen, proposed to approach the problem of spoofing detection from texture analysis point of view. Indeed, face prints usually contain

printing quality defects that can be well detected using texture features. Hence, they presented a novel approach based on analyzing facial image textures for detecting whether there is a live person in front of the camera or a face print. This provides a unique feature space for coupling spoofing detection and face recognition.

Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, present a face anti-spoofing database which covers a diverse range of potential attack variations. Specifically, the database contains 50 genuine subjects, and fake faces are made from the high quality records of the genuine faces. Three imaging qualities are considered, namely the low quality, normal quality and high quality. Three fake face attacks are implemented, which include warped photo attack, cut photo attack and video attack.

J. Komulainen, A. Hadid, M. Pietikäinen, A. Anjos, and S. Marcel, present address issue by studying fusion of motion and texture based countermeasures under several types of scenic face attacks. They provide an intuitive way to explore the fusion potential of different visual cues and show that the performance of the individual methods can be vastly improved by performing fusion at score level. The Half-Total Error Rate (HTER) of the best individual countermeasure was decreased from 11.2% to 5.1% on the Replay Attack Database.

J. Galbally, S. Marcel, and J. Fierrez presented a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image.

D. Crouse, H. Han, D. Chandra, B. Barbelo, and A. K. Jain, worked on a face-based continuous authentication system that operates in an unobtrusive manner. This Paper presented a methodology for fusing mobile device (unconstrained) face capture with gyroscope, accelerometer, and magnetometer data to correct for camera orientation and, by extension, the orientation of the face image. But all the function are not perform on device and require separate server for matching.

S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho, proposed a classification pipeline consisting of DMD, Local Binary Patterns (LBP), and Support Vector Machines (SVM) with a histogram intersection kernel. They advanced the state of the art in facial anti-spoofing by applying a recently developed algorithm called Dynamic Mode Decomposition (DMD) as a general-purpose, entirely data driven approach to capture the above liveness cues. The pipeline of DMD+LBP+SVM proves to be efficient, convenient to use, and effective. In fact only the spatial configuration for LBP needs to be tuned. The effectiveness of the methodology

was demonstrated using three publicly available databases: print-attack, replay-attack, and CASIA-FASD.

D. Wen, H. Han, and A. K. Jain, they proposed an efficient and rather robust face spoof detection algorithm based on *Image Distortion Analysis (IDA)*. Four different features (specular reflection, blurriness, chromatic moment, and color diversity) are extracted to form the IDA feature vector. The proposed approach is extended to multi-frame face spoof detection in videos using a voting based scheme. We also collect a face spoof database, MSU Mobile Face Spoofing Database (MSU MFSD), using two mobile devices (Google Nexus 5 and MacBook Air) with three types of spoof attacks (printed photo, replayed video with iPhone 5S and iPad Air).

W. Kim, S. Suh, and J.-J. Han, proposed a real-time and nonintrusive method based on the diffusion speed of a single image to address this problem. In particular, inspired by the observation that the difference in surface properties between a live face and a fake one is efficiently revealed in the diffusion speed, they exploited antispoofing features by utilizing the total variation flow scheme. One important advantage of the proposed method is that, in contrast to previous approaches, it accurately identifies diverse malicious attacks regardless of the medium of the image.

Z. Boulkenafet, J. Komulainen, and A. Hadid, introduces a novel and appealing approach for detecting face spoofing using color texture analysis. They exploit the joint color texture information from the luminance and the chrominance channels by extracting complementary low level feature descriptions from different color spaces. More specifically, the feature histograms are computed over each image band separately.

3. Existing System

There are many approaches implemented in face spoofing detection. The existing methods for face spoofing detection can be classified into four groups: user behaviour modelling, user cooperation, methods that require additional software and hardware and methods based on data-driven characterization.

The first method user behaviour modelling captures the user behaviour with respect to acquisition sensor (e.g., eye blinking or small head and face movements) to determine whether a captured biometric sample is synthetic. In this method attack is detected based on eye blinking modelling under the assumption that a spoofed attack with photographs differs from valid access by the absence of movements.

The second method user cooperation is used to detect spoofing by asking challenging questions or by asking the user to perform specific movements which adds extra time and removes the naturalness inherent to biometric systems.

The third method that require additional hardware (e.g., infrared cameras or motion and depth sensors) use the extra information generated by these sensors to detect possible

clues of an attempted attack. The final method based on data-driven characterization looking for clues and artifacts that may detect attempted attack and exploit only the data captured by acquisition sensor. Methods that require additional hardware have the disadvantage of not being possible to implement in computational devices that do not support them, such as smartphones and tablets.

4. Proposed System

In our propose system, we implementing an android application for spoof face detection. For this purpose we will use two approaches as follows.

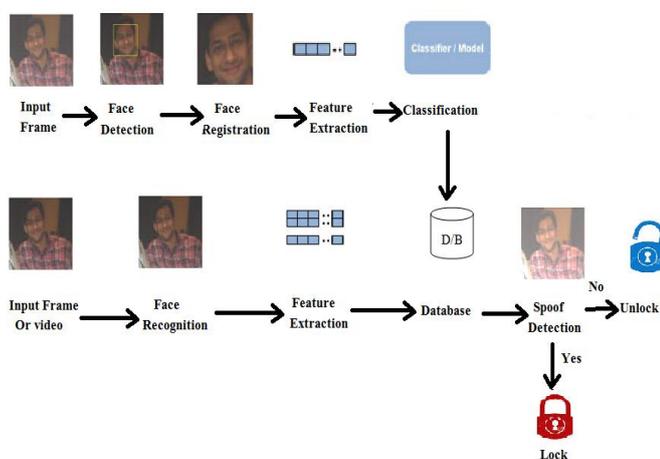


Fig-1: Proposed System

4.1 Face detection Framework

The face detection algorithm proposed by Viola and Jones will be used in our proposed system. The face detection algorithm looks for specific HAAR features of a human face. When one of these features is found, the algorithm allows the face candidate to pass to the next stage of detection. A face candidate is a rectangular section of the original image called a sub-window. Generally this sub-window has a fixed size. This sub-window is often scaled in order to obtain a variety of different size faces. The algorithm scans the entire image with this window and denotes each respective section a face candidate. The algorithm uses an integral image in order to process HAAR features of a face candidate in constant time. It uses a cascade of stages which is used to eliminate non-face candidates quickly. Each stage consists of many different HAAR features. Each feature is classified by a HAAR feature classifier. The HAAR feature classifiers generate an output which can then be provided to the stage comparator. The stage comparator sums the outputs of the HAAR feature classifiers and compares this value with a stage threshold to determine if the stage should be passed. If all stages are passed the face candidate is concluded to be a live face.

4.2 Face Recognition Framework

In this framework we use also same HAAR like feature based algorithm for face recognition. Different with face detection which needs only one training procedure for detection of all faces, each person's face should be trained in the face recognition step. In this framework we are going to recognize the face liveness, eye detection and smile detection.

4.3 Registration Phase

In registration phase we will use face detection framework. We provide sample faces as input to store image in database. Image has stored in encrypted format on database in smartphone. While storing face image in database, system will extracting image features using face detection framework and storing their RGB values and other values. User need to register once time while using this application. After saving their details in application user will ready to use this app by login their credentials.

4.4 Login Phase

While login user need to provide sample face as input to spoof detection application. After providing face input to the application face detection and recognition framework will work. Face recognition framework will retrieving their features from the system while giving input face to the app. Then feature extracted face images values will matching with existing face images which is store at the time of registraton. We are using eye and smile detection techniques for face liveness. If system found real face liveness then it will unlock the smartphone otherwise doesn't open lock.

By this way we will identify the real face liveness and spoof detection system on smartphone.

5 CONCLUSIONS

Spoofing using photographs or videos is one of the most common methods of attacking face recognition and verification systems. Spoof face detection and tracking is being a challenge for many researchers with real time applications. A simple and effective method is proposed in this paper. We are the first time proposed the spoof face detection using HAAR algorithm with the help of smart phone database. We also identify the face liveness using eye and smile detection in propose system. Both analysis and evaluation results confirm that our work can provide an effective solution to identify the spoof faces while unlocking the Smartphone. In future, more work should be on facial expression to identify the system easily.

ACKNOWLEDGEMENT

We express gratitude to our lead authorities such as College, University. The guide and the Prof. of our Department Ms. S.E. Ingale in valuable guidance for the success of this project.

REFERENCES

- [1] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, 2010, pp. 504–517.
- [2] J. Mˆatta, A. Hadid, and M. Pietikˆainen, "Face spoofing detection from single images using micro-texture analysis," in Proc. IJCB, 2011, pp. 1–7.
- [3] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face anti-spoofing database with diverse attacks," in Proc. ICB, 2012, pp. 26–31.
- [4] J. Komulainen, A. Hadid, M. Pietikˆainen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in Proc. ICB, 2013, pp. 1–7.
- [5] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, Feb. 2014.
- [6] D. Crouse, H. Han, D. Chandra, B. Barbelo, and A. K. Jain, "Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data," in Proc. ICB, 2015, pp. 135–142.
- [7] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho, "Detection of face spoofing using visual dynamics," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 762–777, Apr. 2015.
- [8] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 746–761, Apr. 2015.
- [9] W. Kim, S. Suh, and J.-J. Han, "Face liveness detection from a single image via diffusion speed model," IEEE Trans. Image Process., vol. 24, no. 8, pp. 2456–2465, Aug. 2015.
- [10] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in Proc. ICIP, 2015, pp. 2636–2640.
- [11] H. K. Jee, S. U. Jung, and J. H. Yoo, "Liveness detection for embedded face recognition system," Engineering and Technology, 2006.
- [12] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcam," in Proc. ICCV, 2007, pp.
- [13] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face anti-spoofing database with diverse attacks," in Proc. ICB, 2012, pp. 2631.
- [14] J. Yang, Z. Lei, S. Liao, and S. Li, "Face liveness detection with component dependent descriptor," in Proc. ICB, 2013, pp.
- [15] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in Proc. ICB, 2013, pp.
- [16] N. Evans, T. Kinnunen, and J. Yamagishi, "Spoofing and countermeasures for automatic speaker verification," in Proc. INTERSPEECH, 2013, pp. 925929.
- [17] J. Galbally, S. Marcel, and J. Fierrez, "Biometric anti-spoofing methods: A survey in face recognition," IEEE Access, vol. 2, no. 1530-1552, 2014.
- [18] D. Menotti, G. Chiachia, A. Pinto, W. Robson Schwartz, H. Pedrini, A. Xavier Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 4, pp.