Interactive versus Passive 2D Face Spoofing Detection

Alia Saad  
Computer Science and Engineering Department  
American University in Cairo  
Cairo, Egypt  
aliasaad@aucegypt.edu

Mohamed Moustafa  
Computer Science and Engineering Department  
American University in Cairo  
Cairo, Egypt  
m.moustafa@aucegypt.edu

Abstract—Due to its several advantages including practicality and simple requirements, facial identification has attracted a great amount of attention over the past years. Nonetheless, several studies have investigated the vulnerabilities a face biometrics system might face. Therefore, many researches are investigating the countermeasures to these spoof attempts. Unlike passive authentication methods that were profoundly studied, interaction was broadly examined as a potential robust spoofing prevention approach. In this paper, we present our collected dataset, propose an interactive authentication method, evaluate and compare its robustness to the best known static anti-spoofing detection approach under realistic conditions.

Keywords—face recognition, anti-spoofing, countermeasures, authentication, biometrics, challenge-response, interaction, texture analysis

I. INTRODUCTION

Biometric recognition applications, the ones depending on individual’s features to identify, have rapidly developed through the past years, particularly 2D facial authentication due to its simple setup that does not require complex and expensive software. However, it is ineffective to create a valid identification algorithm without considering possible vulnerabilities to occur. Despite its advantages, facial recognition systems became subject to spoof attempts. Face spoofing is defined as the action when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access [1]. Attackers could deceive the system by posing a still printed or digital image, replaying a video or wearing a 3D mask of a legitimate user. Consequently, investigating the most convenient method to prevent these attacks from happening is becoming a necessity in the face recognition field. Generally, face authentication methods are categories in two main classes: passive or motionless authentication method that does not require any involvement of user aside from posing before the capturing device and the interactive, also known as the challenge-response interaction method that requires, captures and computes person’s face or hand gestures to ensure that an actual person is using the system. This paper first investigates an existing still authentication anti-spoofing method, focuses on developing an interactive system that requires minimal user interaction and later evaluates and compares the performance of both approaches to decide which of the authentication modes is more robust to attacks.

This paper is organized as follows: Section II gives a brief overview of previous existing anti-spoofing solutions for both authentication methods. Section III introduces this paper’s contributions: dataset collection, analyzing and comparing the effectiveness of the two authentication approaches in spoofing detection. Section IV then describes in details our accomplished experiments, explains and compares final results and finally, Section V summarizes this paper and provides several conclusions about the proposed work to choose for creating a robust anti-spoofing system.
II. RELATED WORK

The most recognized classification of spoofing countermeasures for motionless authentication was proposed by Chakka et al. [2] in the following pattern: motion analysis, texture analysis and liveness detection. 

*Motion analysis* spoofing detection solutions evolved based on the fact that real faces express different motion patterns either between different regions of the face or in comparison with the surrounding background, unlike the spoof attacks where the faces and the background show the same motion sequence and direction. [3] proposed one of the most famous motion analyzing techniques that estimates the correspondence between different regions of the face using optical flow field. This solution has achieved great results in detecting spoofed still images. Another solution used the optical flow field to investigate the motion patterns of a real face as a 3D object compared with the motion order of a 2D planar object representing spoofed images [4]. Aside from the optical flow field, Anjos et al. [5] were interested in calculating the movement intensities of both face and neighboring scene, and they considered that the higher the correlation between both intensities, the more probable the tested video to be fake.

Real faces often show different texture appearance other than printed or displayed images. *Texture analysis* depends on discovering these changes that apply on images during spoofing scenarios. Considered to be the most favorable anti-spoofing method because of its basic structure and simple computation, analyzing the micro-texture of the image using Local Binary Pattern has expressed great results in recent studies. 

Finally, *liveness detection* is the spoofing countermeasure method executed during passive identification process. Several researches aimed at detecting various signs of life such as changes in facial expressions, eye blinking and mouth movements [6]. 

With the vast and rapid evolution of portable smart device display resolution, attackers are more capable of deceiving face recognition systems that use non-interactive posing mode. It was even concluded that without interaction, vitality and non-rigid motion detectors are powerless and vulnerable to video replay-attacks [6]. Therefore, our focus is now turned into investigating the effectiveness of employing interactive identification processes to raise the accuracy level of detecting an attacker. *BioID* is considered one of the first successful proposed solution of interactive authentication [7]. The proposed system specified a randomized set of changing face pose instructions to the user to act, then an estimation algorithm compares and matches the responses to requested actions.

III. PROPOSED WORK

We start our proposed work by explaining and defining the dataset we collected for experimentations, then we focus on the algorithm we used in texture analysis of the motionless authentication and finally we concentrate on the algorithm we followed for testing the efficiency of the interaction in spoofing detection.

A. Our Collected Dataset

Robust face recognition systems must successfully operate independently from any external conditions. Since existing datasets [8] were limited to controlled lighting conditions, we needed to collect more general video datasets that covers more illumination environments that user could encounter during the recognition process. For that reason we had recorded each user’s session, either interactive or passive, under four different lighting conditions, varying from direct sunlight outdoor environment, sun-lit indoors, typical artificial indoor lighting to somehow dimmer lighting state. Figure 1. shows a sample of video frames of an authentic user collected under the four different sources of light. Meanwhile, attack dataset were collected by replaying the real videos of each user once with a tablet and another time with a phone display. Second and third rows in Figure 1 highlight the similarity of appearance between the real and attack video frames, once more within
the four different illumination environment.\textsuperscript{1} Twenty-one users contributed in the collected data set, 8 videos were captured for each user covering all lighting conditions with the 2 types of authentication, still and interactive. With an equal number of videos for the phone and tablet replayed videos, the total number of videos in this dataset reaches up to 504 videos. Table I summarizes the collected video dataset.

TABLE I: Collected Dataset Summary

<table>
<thead>
<tr>
<th></th>
<th>Still</th>
<th>Interactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>84</td>
<td>84</td>
</tr>
<tr>
<td>Replay-Phone</td>
<td>84</td>
<td>84</td>
</tr>
<tr>
<td>Replay-Tablet</td>
<td>84</td>
<td>84</td>
</tr>
</tbody>
</table>

The recording protocol for the still dataset is also following the ICB’13 competition [9] with a 15 frames-per-second frame rate, 15 seconds video with a $320 \times 240$ screen resolution. The challenge-response process follows the same frame rate and screen resolution in addition to challenging the user to move face in the four main directions (up, down, left and right), figure 2, in a random sequence.

Fig. 1: Rows:(1) Sample of Genuine Video Frames under Different Lighting Conditions in Our Collected Dataset. (2) & (3) Replay Attacks from Phone and Tablet Display.

B. The Selected Passive Method

In this paper, two experiments were held for comparison, in the first experiment, we test the efficiency the Local Binary Pattern (LBP) in analyzing the texture of frames in captured videos. This method was chosen based on the promising results proved in the ICB competitions [9] [2] to be the best classification method between real and fake attempts.

This was achieved calculating a global histogram for each video in our collected dataset and using a Support Vector Machine (SVM) for classification. The SVM was trained by the global histograms of the videos from the replay-attack train dataset. Figure 3 illustrates the texture analysis process for spoofing detection. The reason behind choosing the Local Binary Pattern is based on its simple implementation and low dimensional features that lead to attain powerful results without the need of complicated computations or classifications [8].

Fig. 3: Texture Analysis Spoofing Classification [1]

C. Our Proposed Interactive Method

Next step focuses on the effectiveness of the interactive technique by applying it over the collected interactive videos. In this experiment, inspired by [7], a series of a random-ordered actions are displayed to the user and by tracking the head motion, user’s responses are compared and calculated. A threshold of minimum number of detected is selected for classification between real and attacks, all steps are illustrated in Figure 4. Our final conclusion about which most robust authentication method is based on the results achieved by both experiments. Following is a detailed description about our collected dataset.

---

\textsuperscript{1}Collected data will be publicly available for the research community once finalized
IV. EXPERIMENTS AND RESULTS

Two main experiments are presented in this paper, the first one is to evaluate the performance of solely utilizing the texture analysis on both still and interactive sessions. The assessment is achieved by calculating the output of an SVM that classifies between real and fake videos based on the local binary pattern (LBP) histogram. While second experimentation focuses on the efficiency of interactive face recognition authentication.

Evaluation Metric

We based our evaluation process on calculating the False Acceptance Rate (FAR), the ratio of intrusive attempts that were incorrectly classified as real over the total number of videos, the False Rejection Rate (FRR) representing the ratio of real video misclassified as attacks and the Half Total Error Rate which is the mean between FAR and FRR [9].

Experiment 1: Texture Analysis for the Passive Method

In this experiment, we observed the validity of exclusively employing the texture analysis as a sole spoofing detection criterion. We expanded our video database to include more videos covering more illumination conditions to cover more possible number of situations or locations where a face recognition systems might meet. The experiment started first by feeding global histograms of a basic (LBP\(_8,1\)) of each video in the Idiap’s train dataset to a liner Support Vector Machine. Later, each video in our collected Dataset, either passive or interactive videos, were then fed to the SVM for classification. The motivation behind choosing LBP for texture analysis was based on the outstanding resultls achieved in previous competitions [2] and [9]. Table II summarizes the results for both interactive and passive videos.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>FRR</th>
<th>FAR</th>
<th>HTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Still</td>
<td>4.7619</td>
<td>78.5714</td>
<td>41.666</td>
</tr>
<tr>
<td>Interactive</td>
<td>1.1904</td>
<td>80.9523</td>
<td>41.0714</td>
</tr>
</tbody>
</table>

By the end of this experiment, we observed that depending only on texture analysis with uncontrolled environments does not produce promising results, with an HTER arising up to 41%, we cannot depend only on the texture analysis for spoofing detection applications.

Experiment 2: Challenge-Response Interaction

The second experiment in this paper tests the performance of employing challenge-response interaction for achieving more accurate spoofing detection results. In this experiment, each user’s face is identified using the opencv’s haar cascade frontal face classifier. Then the center point is detected for tracking. Next, a random-ordered series of actions are required from the user to perform, after each challenge message, the face center point is tracked using the Lucas-Kanade method. The angle of motion is then processed to estimate the face motion. While Figure 5. displays face center point tracking, table III compares the error rates achieved with variation of the minimum threshold of accepted number of actions. Results presented in this table indicate the achieved error rates after setting a minimum threshold of minimum number of accepted actions. This threshold is set based on margin of human error. While in each session the user completes four required actions, the minimum number of successfully

![Fig. 4: Proposed Interactive Anti-Spoofing Method](image-url)
detected actions varies based on the security level the system want to maintain. From these results we can conclude that the more actions used, the more false acceptance ratio goes down unlike the false rejection that increases with a considerable rate. Therefore adapting the number of accepted actions is directly related to the critical nature of the face recognition system. Moreover, it is becoming clear to deduce that the suitable number of actions for an interactive authentication session should vary between 2-3 actions in order to minimize error opportunities.

V. CONCLUSION AND FUTURE WORK

Anti-spoofing is turning into a crucial matter following biometric identification. Despite its capability of identifying an individual, facial recognition system is useless unless its also capable of distinguishing between real an fake attempts. This paper tests and compares the efficiency of passive and interactive authentication methods in spoofing detection applications. We can finally conclude that interaction has achieved better results than the motionless authentication. With a significant 30% lower HTER, interactive method is considered to be more robust to attacks than analyzing the texture of video frames, especially under uncontrolled lighting conditions. We also reached a conclusion about the most advisable number of actions for the user to act to be 2-3 actions in order to insure proper results. Our future plan could be summarized in expanding our collected dataset, improving achieved results by adding more training data of wider set of videos for the support vector machine with more realistic illumination conditions and finally exploring more facial actions such as eye-blinking and smile detection in hopes of decreasing the system vulnerability.

REFERENCES


