Facial Liveness Testing: For The Web

Student Name: Ryan Collins

Supervisor Name: Prof A. Krokhin

Submitted as part of the degree of MEng Computer Science to the

Board of Examiners in the Department of Computer Sciences, Durham University

January 29, 2019

***Abstract* —**

Context/Background TODO

Aims TODO

Method TODO

Results TODO

Conclusions TODO

***Keywords* —** Facial liveness, convolutional neural networks, image quality metrics

I INTRODUCTION

Currently, username and password authentication is commonplace throughout the web. However, username and password based authentication systems have a number of problems. Some common passwords can be broken using dictionary attacks, especially if they consist partially or entirely of a word in a standard dictionary. Furthermore, the process of shoulder surfing is possible (watching out for someone's password, and how they type it).

An easy to use system is necessary to remove the choice from the user (in terms of password), relying on the user being automatically detected, and several confirmation methods to ensure the user is indeed who they say they are (and not just someone spoofing the system). Before such a system is developed, a facial liveness testing method must be found that operated in near real-time, and that is fairly accurate.

II RELATED WORK

- First basic metrics - image Quality assessment (different types of image quality metrics used ,and why they should be effective). Drawbacks of these - movement based assessment (requiring actions to be performed, and their problems). - Deep Learning methods (what methods exist, their performance) - 3D mask prevention methods (kinect based ones that require 3D input, or SFM, which isn't really valid here)

III SOLUTION

A Image Quality Assessment based liveness test

For 2D spoofing attacks, spoofed images are typically lower quality than the real images, and thus by measuring the image quality one can train a classifier to detect real and spoofed images respectively.

The method used, based on **CITE the paper we use here**, implements 24 different metrics (with varying differences), and produces a vector for each image. Initially, classification was done using a Support Vector Machine (SVM), but after experimentation this proved to be fairly unreliable (yielding 70% accuracy on the test set). The classifier was later changed to use Linear Discriminant Analysis

(LDA) which yielded a much improved accuracy (96% accuracy on the test set). **TODO: give more accuracy figures of accuracy here, I can't remember the exact numbers**.

B A system for preventing 3D spoofing attacks

While the systems before might go partially towards preventing 3D spoofing attacks, though primarily considering the 2D image, we now propose a method that is designed for classifying facial liveness based on a 3D point cloud.

B.1 Point Cloud Reconstruction

In order to classify an image/video, a 3D point cloud needs to be created, containing many 3D points (x, y, z) of a user's face. While 3d reconstruction is easier with videos (using structure from motion or other multiview based methods), there also exist image-based reconstruction methods such as vrn **CITE VRN network model here for 3d reconstruction**, which are more specific and designed for reconstructing faces based on images.

B.2 3D point cloud classification

Once the 3D reconstruction is obtained, one can then classify this using some model to produce the fake/real metric.

For points, PointNet is a model that can be used **EXPLAIN POINTNET**

However, as we are using voxels, there is a more specialised architecutre called Voxnet that is designed for classifying 3d volume-based objects. This is the model used here.

IV RESULTS

TODO results

V EVALUATION

TODO evaluation

VI CONCLUSIONS

References