DSAA Final Project Evaluation

Group 3

Background

The project focuses on authentication of a user using a hand gesture and a few properties of the hand which would be acting like his password. Abstractly, the authentication of a person plays a key role while working with confidential things may it be a project, deal or a codebase. For cases like online identity we have public and private keys validating a particular user and his system but for physical authentication, we tend to rely on classical biometric identification like voice and fingerprint which can be forged easily with the current technology.

Generally, physical authentication is done by pin codes or fingerprint as they are very feasible to be implemented. For a more secure purpose, we propose new method of authentication.

Problem Statement:

Our project mainly concentrates on authentication of a user having hand gesture and properties of hand as a unique properties. Properties of hand include but not are exclusive to size of hand, dimensions of fingers and more. The system would identify general and normal difference and also identify if someone attempts to break the system and it will raise an alarm.

Methodology - Explaination:

Using a pre trained model, we are currently identifying hand key points, connecting them to form a skeleton and then applying this on series of images to create a video and then smoothen the video to give more sensible and less cluttered output

We are working on storing it not as video but as primary distances which will finally be compared between two outputs and authenticate or deny a person.

Methodology - Ground Truth:

The Identification and location of the hand keypoints and comparison of skeleton of one hand to another and therefore comparing two videos consisting of hand motions

Results:

We were able to identify if the password is correct and also if the person who entered is actually the authorized person.

Confusion Matrix (For the right person):

	Authenticated	Not Authenticated
Password Correct	85.883%	14.117%
Password Incorrect	10.15%	89.85%

Confusion Matrix (In case of Forgery):

	Authenticated	Not Authenticated
Original Person	85.883%	14.117%
Forgerer	~40%	~60%

Analysis

The results are pretty good especially considering the ease of biometeric forgery and the accuracy of biometeric authentication devices.

Contribution Table:

Name	Work
Varun Chhangani	Processing single image and applying the model using Convolutional Deep Neural Network
Avinash Katariya	Extracting primary distances, save them and compare them accordingly
Nischal Talluri	Inputting video file, extracting frames as images and saving the output file
Lushaank Kanchrela	Smoothening and finding lost key points using other frames in a non causal manner by creating a window

References

- Hand Keypoint detection in Single Images using Multiple Bootstraping (arXiv:1704.070809v1)