Title Facial Authentication System for the Web

Project Type Computer Vision, Image Processing and Security

Description - Traditional username and password focused approaches to authentication have drawbacks (such as password leaks) - Existing biometric methods have their problems when applied to a web system, due to the transparency of web systems. - Overcoming the transparency hurdle would produce a secure method of authentication for the web, using faces of users. - Using multiple methods of facial recognition, facial liveness tests, coupled with implementation details, these can be used to create a robust authentication service.

Preliminary Preparation
- Existing biometric web-based authentication methods, how do they work, what are their benefits/drawbacks?
- What spoofing methods could be undertaken, and how can we prevent these?
- What are the privacy concerns regarding a facial recognition approach, and how can these be mitigated?
- How can this be integrated into a web service?
- Use as a single sign on service (SSO). What protocols are there, how do they work, how can we integrate our system into these standards?

Minimum Objectives
- Server that recognises a user given their face (therefore carrying out authentication), generating a token for a user given their face. This token can be used for authorization.
- Client side that accepts user video, and transmits it to the main application for further processing
- Main server that utilises microservices to do the large amounts of processing necessary at scale.

Intermediate Objectives
- CNN-based liveness for a photograph of a user's face
- Reference image facial matching, using a CNN.

Advanced Objectives
- Preventing replay attacks - preventing someone from intercepting someone's facial image using image metadata methods.
- Lipreading speech-based liveness check
- SAML2 protocol implemented, to provide an SSO to many other applications.

References
- Keras (https://keras.io) for Machine Learning
- OpenCV (https://opencv.org/) for image Processing

Facial Authentication for the Web

Creator	Ryan Collins
DATE	3/12/18

TASK TITLE	TIME (Weeks)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Framework Setup																													
Web Portal to capture and transmit video to a remote server	1																												
Main server applet to receive input from the web portal	1																												
Consolodation layer to manage microservices and process their output and trigger microservice processing	2																												
Facial Recognition																													
Preprocessing layer - obtaining just the facial area, with histogram equalisation to normalise the content	1																												
Autoencoder layer - producing a vector from an image of a face using an autoencoder	3																												
Database searching layer, utilising the vector from the autoencoder, coupled with query to find similarity	1																												
Siamese NN - a potential alternative that could also be tried if necessary	3																												
Liveness Tests																													
Key frame service to pick key frames from a much larger video	1																												
CNN model to detect liveness based on non-linear diffusion	3																												
Adding two way communication to our system, allowing instructions to be sent to the client side	1																												
Building a word recognition model based on lipreading	3																												
Building some lipreading confirmation model that's accurate enough for our captcha method	1																												
Pupil tracking - building a model based on this approach	3																												
Gathering statistics for each component, based on accuracy	4