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) - Applying a biometric based approach to web security could improve account security if done correctly.

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?
- OAuth Authentication - how could facial recognition play into an existing OAuth authentication method?

Minimum Objectives

- Server that accepts an image as input via a Web Request, and returns a unique token based on that image.
- Generating a token based on facial structure, resilient to background and lightness changes.

Intermediate Objectives

- Liveness tests - how can we ensure the user input image is of a person, and not a printout of someone's face?
- Scalable system - providing a service layer which is usable by many other users for a variety of uses, and that can scale up if required.

Advanced Objectives

- Preventing replay attacks - preventing someone from intercepting someone's facial image, and using it to gain access

References

- JSON Web Tokens, and their application
- Keras (https://keras.io)