Negative FaceBlurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass

TengQi Ye, Brian Moynagh, Rami Albatal and Cathal Gurrin
Insight Centre for Data Analytics, Dublin City University, Ireland
Brian.Moynagh@insight-centre.org

Abstract

Wearable devices such as Google Glass are receiving increasing attention and look set to become part of our technical landscape over the next few years. At the same time, lifelogging is a topic that is growing in popularity with a host of new devices on the market that visually capture life experience in an automated manner. We describe a visual lifelogging solution for Google Glass that is designed to capture life experience in rich visual detail, yet maintain the privacy of unknown bystanders.

1. Motivation

Using a wearable technology such as Google Glass to capture a visual lifelog often results in capturing images of unknown bystanders from whom the lifelogger may not have permission. Naturally this creates a tension between data gathering and society's concerns about an individuals right to privacy. Our goal is to facilitate the collection of visual lifelogging data whilst maintaining the privacy of any bystanders that are unknown to the lifelogger.

2. Problem Statement

In order to allow an individual to choose the lifelogs in which their image will appear and those in which it should not, the individual needs to be able to define a privacy policy. Successful implementation of such a policy is dependent upon the reliable detection of faces and accurate recognition of detected faces within images.

3. Related Work

Many of the early uses of lifelogging have focused on deploying wearable cameras to provide memory assistance or as a source of data for long-term user studies. However, none of the previously developed lifelogging prototypes take a privacy-by-design approach. Privacy by design principles are based on seven foundations [1]. From these seven principles, we choose to make privacy the proactive default configuration, inherent in the design of the software, that separates the lifelogger from the data and which respects the privacy of unwilling subjects and bystanders.

4. Research Question

What constitutes a violation of a bystanders privacy within a visual lifelog? What measures can be taken to preserve a bystanders' privacy? Can a satisfactory balance be reached between the goals of the lifelogger and the privacy rights of unknown bystanders?

5. Hypothesis

We believe that the visibility of an individuals face in an image is the main factor in preserving or violating that individuals privacy. For this reason, we are of the opinion that effective face detection and accurate face recognition are fundamental to any privacy by design based lifelogging system.

6. Proposed Solution

We propose employing user privacy policies for regulating *dynamic views* over lifelog data. In this way, a user (by nominating *friends*) is free to choose in which lifelogs their image can appear. These policies can be updated in real-time so that an individual can retrospectively add or remove access rights to their identifiable image. We call this approach *real-time policy-driven negative face blurring*. Haar-like Feature-based Cascade Classifiers [2] are used for face detection. Eigenfaces, Fisherfaces and Local Binary Patterns are used for facial recognition.

7. Evaluation

A total of 8,657 lifelog images were used to evaluate the system. Facial detection was evaluated by counting images containing faces, in which all faces were detected and images that contained no faces that were correctly identified as such, as a pass. A pass rate of 80.68% was observed.

For facial recognition, 1,300 pictures containing faces were randomly selected from dataset. From these images 1,310 faces were detected. The false positive rate (i.e bystanders classified as friends) was 0.76% and the false negative rate (i.e. friends classified as bystanders) was 29.01%. 67.18% of the faces were correctly identified as bystanders.

8. Acknowledgements

This publication has emanated from research supported in part by research grants from Irish Research Council (IRCSET) under Grant Number GOIPG/2013/330 and Science Foundation Ireland (SFI) under Grant Number SFI/12/RC/2289.

References

[1] A. Cavoukian. Privacy by design. *Report of the Information & Privacy Commissioner Ontario, Canada*, 2012.

[2] P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. In *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, volume 1, pages I–511. IEEE, 2001.