Demo: FaceBlock: Privacy-Aware Pictures for Google Glass

Roberto Yus[1], Primal Pappachan[2], Prajit Kumar Das[2],
Eduardo Mena[1], Anupam Joshi[2], Tim Finin[2]

University of Zaragoza, Spain[1], {ryus,emena}@unizar.es
University of Maryland, Baltimore County, USA[2], {primal1,prajit1,joshi,finin}@umbc.edu

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]: Privacy

Keywords

Google Glass, privacy-aware pictures, policy sharing

1. INTRODUCTION

Wearable technology is changing the human-computer interaction paradigm by improving the user experience. For example, *eyewear* technology, such as Google Glass, is opening a new world of possibilities. One of the best capabilities of such devices is that they allow spontaneous and effortless photo taking. Instead of pulling out your camera, turning it on, aiming, taking a picture and putting it away, Google Glass makes it as easy as saying "Okay Glass, take a picture".

However, their strength has also become controversial: people worry that their pictures could be taken without their knowledge or consent, violating their privacy. These privacy concerns are not new and have existed since camera technology became accessible to everyone. But, Google Glass makes it difficult to know when someone is taking a picture of you. Resorting to drastic measures, like banning their use in public places, is not a good solution. We demonstrate FaceBlock[1], which protects the privacy rights of individuals by allowing them to choose whether or not to be included in pictures taken with Glass (see [1] for more information).

Our approach allows a user's mobile device to share privacy policies with nearby Glass devices using a P2P communication channel (our prototype uses Bluetooth). Along with the policy, users share information that helps identify them in a picture. When the Google Glass takes a picture the system recognizes faces on it, checks policies it has received, and obscures faces as necessary. In our prototype, users share their *eigenface* [2] as a way to identify them on the pictures. An eigenface is an "encoded" picture of a face
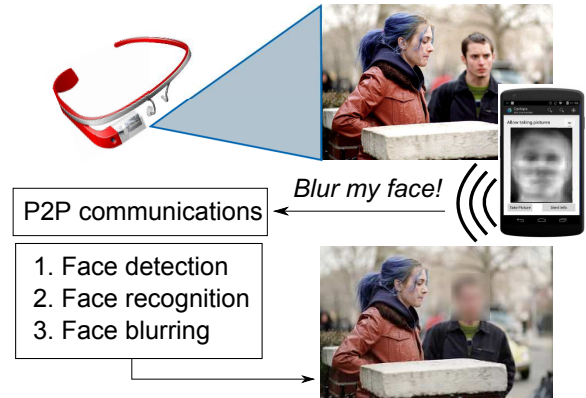
Figure 1: High-level architecture of our system

that showing its deviations with respect to a "mean face", which is composed of hundred of faces (Figure 1 shows an example). Other ways of recognizing people can also be used in such a system system, like unique clothes [3]. The use of a policy language grounded in semantic descriptions will enable context-aware constraints (e.g., "blur my picture except when I am at the office").

2. DEMO SETUP

The demo setup includes our prototype, a Google Glass, and two smart-phones. We will invite people to take privacy-aware pictures with FaceBlock. Figure 1 shows a possible scenario. Joel is using his Google Glass to take pictures of his girlfriend Clementine. Patrick is walking by and may be captured in Joel's picture. Patrick has FaceBlock on his smartphone and whenever it detects a Google Glass device, it will create a Bluetooth connection and shares Patrick's policy ("blur my face in pictures from strangers") and his face identifier (eigenface). Joel, who is also using FaceBlock, receives this information from Patrick and every time that Joel takes a picture, FaceBlock analyzes it and obscures Patrick's face if detected.

3. REFERENCES

[1] http://face-block.me.
[2] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of cognitive neuroscience*, 3(1):71–86, 1991.
[3] H. Wang, X. Bao, R. R. Choudhury, and S. Nelakuditi. Insight: Recognizing humans without face recognition. HotMobile'13.