Towards Secure Personal Device Unlock using Stereo Camera Pan Shots

Rainhard D. Findling and Rene Mayrhofer

Department for Mobile Computing, Upper Austria University of Applied Sciences,
Softwarepark 11, 4232 Hagenberg, Austria,
rainhard.findling@fh-hagenberg.at,
rene.mayrhofer@fh-hagenberg.at,
WWW home page: http://www.fh-ooe.at/en/

Abstract. Unlocking a personal device using unlock approaches like PIN, password or an unlock pattern is insecure, as it is prone to the shoulder surfing attack: an attacker watching the display during user authentication. Therefore, Face Unlock – using biometric face information for authentication – is an approach to a more secure personal device unlock. Unfortunately, when using frontal face information only, the authentication still can be circumvented by a photo attack: presenting a photo/video of the authorized person to the camera. We intend to create a Face Unlock which is harder to circumvent by using all face information that is available during a 180° pan shot around the user's head. Based on stereo vision, 2D and depth images are recorded of the user's head, along with sensor data of the device movement.

1 Introduction

Personal devices like smartphones hold important and private user data in the regular case, like access to emails/private messages, contacts, calendars and location information. Therefore, current smartphone platforms provide lock mechanisms, with which the devices has to be unlocked before usage. Unfortunately, the majority of current unlocking approaches like entering a PIN/password or drawing an unlock pattern are prone to the shoulder surfing attack [7] (an attacker watching the display while the user authenticates). An attacker could therefore perform a replay attack to unlock another person's personal device.

Face Unlock (face-based authentication) is an approach to unlock a personal device, which aims to a) increase usability, as the user does not have to remember an authentication secret and the authentication process can potentially be done faster, and b) be more robust against the shoulder surfing attack, as replay attacks are more complicated for face-based authentication. Unfortunately, with using frontal face information only for Face Unlock, the unlock mechanism can be circumvented by photo attacks [8] (presenting a photo/a short video of the user with sufficient quality to the personal device's camera). For many regular users, such data can be grabbed from social networks. Therefore, using frontal face information only for a Face Unlock approach cannot be considered secure enough for a personal device holding important and private data.

2 Face Unlock based on Stereo Vision Pan Shot

We intend to develop a Face Unlock which is more robust and more secure against photo attacks than with using frontal face information only. Our approach is based on our previous work [2] and uses all face information available from a 180° stereo camera pan shot around the user's head. Using stereo cameras, we take 2D and depth pictures of the user's head at multiple angles, along with gyroscope sensor data for each pair of pictures. Therefore, to circumvent a system based on this approach, more information would be needed than when using frontal face information only, like a 3D model of the user's head.

Using the recorded pictures, we first intend to perform a face detection based on the 2D pictures, or a face segmentation based on the depth pictures. For face recognition, we intend to use different classifiers for a) different angles and b) 2D pictures and depth pictures. In our previous work, we used Eigenfaces for Face Recognition [4], which delivered unsatisfying results. Therefore, we are currently analyzing other Face Recognition approaches to obtain better results both in the 2D and depth domain – among them are Feed Forward Neural Networks [6] and Support Vector Machines [5]. To finally combine the output of the different, used classifiers, we intent to use a boosting technology like AdaBoost [3]. The results of this analysis will be presented in the full paper.

3 Current Results

First face recognition experiments done on the Hagenberg Preliminary Face Database [2] indicate, that using Feed Forward Neural Networks on pan shot face pictures results in a more accurate recognition (compared to the results of our previous work), which coincides with literature [1]. Due to the time intense training of a Neural Network, training will likely be done on a PC instead of a personal device – while classification can be done on the personal device, as it is much faster.

References

1. A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino. 2d and 3d face recognition: A survey. *Pattern Recogn. Lett.*, 28:1885–1906, 2007.
2. R. Findling and R. Mayrhofer. Towards face unlock: On the difficulty of reliably detecting faces on mobile phones. In *Proc. MoMM 2012*, 2012.
3. Y. Freund and R. E. Schapire. A Decision Theoretic Generalization of On-Line Learning and an Application to Boosting. In *EuroCOLT-95*, 1995.
4. A. Pentland, B. Moghaddam, and T. Starner. View-based and modular eigenspaces for face recognition. In *Proc. CVPR '94*, 1994.
5. P. J. Phillips. Support vector machines applied to face recognition. In *NIPS*, pages 803–809, 1998.
6. H. A. Rowley, S. Member, S. Baluja, and T. Kanade. Neural network-based face detection. *IEEE Trans. Pattern Anal. Mach. Intell.*, 20:23–38, 1998.
7. F. Tari, A. A. Ozok, and S. H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proc. SOUPS '06*, 2006.
8. R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli. Fusion of multiple clues for photo-attack detection in face recognition systems. In *IJCB 11*, 2011.