Using Facial Behavior Biometric Modalities for Smartphone Authentication

***Abstract*—**

I. Introduction

Smartphone has been prevalently used in our daily life for storing and transmitting private data, conducting online payment. By 2016, the number of smartphone users is forecast to reach 2.1 billion and is expected to pass 5 billion by 2019 [2]. However, the security for mobile access control has became a non-negligible issue because of its ubiquitous nature. It is reported by loolout.com that smartphone is easily lost or stolen by an attacker as its small size, and there are nearly $2.5 billion worth of devices were lost or stolen in 2011 [1]. This may result in privacy leakage and finance lost.

Recently, human identification system based on biometrics has emerged as an usable and secure authentication approach for access control and identity recognition. Unlike traditional authentication methods like passwords or PINs, Biometric-based approach exploits individual's physiological and/or behavioral modalities to recognize user's identity. Moreover, passwords or PINs are hard to remember [4] and can be stolen by shoulder surfing [7, 8] or video-based attacks [10, 11] while individual's biometric traits are not easily to be stolen or forged.

In general, biometric-based technologies can be categorized as two types: physiological characteristics and behavioral traits. Physiological characteristics based on the personal trait to verify a user. Behavioral traits based on the way people do things.

1. Smartphone is easily lost or stolen by an attacker as its small size. This may result in privacy leakage and finance lost. It is reported by lookout.com that nearly $2.5 billion worth of devices were lost or stolen in 2011 [1].

2. Human face plays an important role in our social interaction. As compared with other biometric modalities such as fingerprint and iris, face recognition has distinct advantages because of its non-contact process. Face images could be captured from a distance without touching person being identified and identification does not require interaction with person. In addition, face recognition serves crime deterrent purpose because face images that have been recorded and archived could later help identify a person.

Permission to freely reproduce all or part of this paper for noncommercial purposes is granted provided that copies bear this notice and the full citation on the first page. Reproduction for commercial purposes is strictly prohibited without the prior written consent of the Internet Society, the first-named author (for reproduction of an entire paper only), and the author's employer if the paper was prepared within the scope of employment.
NDSS '17, 26 February -1 March 2017, San Diego, CA, USA
Copyright 2017 Internet Society, ISBN 1-891562-41-X
http://dx.doi.org/10.14722/ndss.2017.23xxx

3. Human identification system based on biometrics other than the face have already led to commercial products with very high identification rates: the iris [3] and fingerprints [9] can be cited as example. However, these systems are not always appreciated by users, as they require some close interaction with the machine often perceived as invasive. Moreover, they require the user to stop at the device and be cooperative, which is acceptable for access control to restricted areas, but not for other applications like surveillance. Face recognition may overcome some of these limitations.

4. Challenges in face recognition arise because the face is not a rigid object and images can be taken from many different viewpoints of the face.

5. Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, thses methods examine an individual's physiological and/or behavioral characteristics in order yo determine and/or ascertain his identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged.

Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioral traits (such as gait, signature and keystroke dynamics). Face recognition appears to offer several advantages over other biometric methods as follows:

1) Almost all these technologies require some voluntary action by the user, i.e., the user needs to place his hand on a hand-rest for fingerprinting or hand geometry detection and has to stand in a fixed position in front of a camera for iris or retina identification. However, face recognition can be done passively without any explicit action or participation on the part of the user since face images can be acquired from a distance by a camera. This is particulary beneficial for security and surveillance purposes.
2) Data acquisition in general is fraught with problems for other biometrics: techniques that rely on hands and fingers can be rendered useless if the epidermis tissue is damaged in some way (i.e., bruise or cracked). Iris and retina identification require expensive equipment and are much too sensitive to any body motion. Voice recognition is susceptible to background noises in public places and auditory fluctuations on a phone line or tape recording.

Signatures can be modified or forged. However, facial images can be easily obtained with a couple of inexpensive fixed cameras.

3) Good face recognition algorithms and appropriate preprocessing of the images can compensate for noise and slight variations in orientation, scale and illumination.
4) Technologies that require multiple individuals to use the same equipment to capture their biological characteristics potentially expose the user to the transmission of germs and impurities from other users. However, face recognition is totally non-intrusive and does not carry any such health risks.

6. In this section, we discuss the technical considerations that underpin the design of CarSafe while the detailed design is presented in section 3. CarSafe fundamentally relies on the real-time processing of dual camera video streams. In what follows, we discuss the challenges and design considerations that arise. This example motivates the need for the simultaneously processing of video streams from the front and rear cameras. SURF features are provided to a binary two-class SVM that is trained to classify eyes as either being open or closed (defined as an open or closed event).

7. Related Work–Face recognition techniques can be broadly divided into three categories based on the face data acquisition methodology: methods that operate on intensity images; those that deal with video sequences; and those that require other sensory data such 3D information or infra-red imagery [6].

8. Among our interesting finding is how large a role web passwords play in user lives. The average user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts that require passwords, and types an average of 8 passwords per day [5].

ACKNOWLEDGEMENTS

We would like to thank all participants who help for completing the experiments. Thank all volunteers for their time and insights as well as the anonymous reviewer for their critical and constructive comments. This work was supported by NSFC (Grant No. 61672427) and the UK Engineering and Physical Sciences Research Council (Grants No. EP/M01567X/1(SANDeRs) and EP/M015793/1(DIVIDEND)).

REFERENCES

[1] "Lookout inc." https://www.lookout.com/resources/reports/mobilelostand-found/billion-dollar-phone-bill, 2012.
[2] "Number of smartphone users worldwide from 2014 to 2020." https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/, 2016.
[3] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE transactions on pattern analysis and machine intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.
[4] A. De Angeli *et al.*, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," *Int. J. Hum.-Comput. Stud.*, 2005.
[5] H. C. Florencio D, "A large-scale stugy of web password habits," in *Proceedings of the 16th international conference on World Wide Web. ACM*, 2007, pp. 657–666.
[6] R. Jafri and H. R. Arabnia, "A survey of face recognition techniques," *Journal of Information Processing Systems*, vol. 5, no. 2, pp. 41–68, 2009.
[7] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," *Systems Man & Cybernetics Systems IEEE Transactions on*, vol. 44, no. 6, pp. 716–727, 2014.
[8] J. Rogers, "Please enter your four-digit pin," *Financial Services Technology*, 2007.
[9] R. R. Rogers, "Biometric identification systems: The science of transaction facilitation," in *SPIE's 1994 International Symposium on Optics, Imaging, and Instrumentation*. International Society for Optics and Photonics, 1994, pp. 194–199.
[10] D. Shukla *et al.*, "Beware, your hands reveal your secrets!" in *CCS '14*.
[11] Q. Yue *et al.*, "Blind recognition of touched keys: Attack and countermeasures," *arXiv preprint arXiv:1403.4829*, 2014.