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 user's 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 [10] and can be stolen by shoulder surfing [16, 20] or video-based attacks [24, 29] 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. *Physiological biometrics* such as fingerprints [9], voice [21] and iris [8] have already been widely commercial used with a high identification rate. However, these bio-features have facing the potential risk of being replayed by attackers. For example, fingerprint can be easily replicated by fingerprint membrane and voice can be forged by professional voice processing software. Even some researchers stated that iris can be counterfeited using victim's picture acquired from social media. Moreover, physiological biometrics is non-revocable, which means biometrics would permanent leakage once it was stolen. *Behavioral biometrics* have been explored by researchers in the past few years. Touch-based behavioral traits such as multitouch gestures [22] and keystroke pattern [30] have been proposed to provide access control on smartphone. However, these methods are not appreciated by user as they require close interaction with the touch-screen. This is not convenient in a frequent use. Other behavior-based methods such as in-air signature [5] and gait recognition [27] have the potential risks for adversaries to mimic. In addition, gait pattern is easily be altered by both the road condition and people's mental state.

Human facial expression plays an significant role in our social interaction. It is driven (motivated) by the complex interaction between the emotional state and the facial muscles [15]. Due to the fact that it carries both psychological and behavioral information, facial expression is unique so that it is highly immune to the replay attack by the attackers. Moreover, unlike fingerprint and iris, facial expression is revocable as an individual has many facial expressions such as six basic expressions (anger, disgust, fear, joy, sadness and surprise) and compound expressions constructed by combining basic expressions [12]. Thus, facial expression can be regarded as facial behavioral biometric modalities for authenticating identity on smartphone.

In this paper, we present a novel facial behavior authentication system for smartphone based on the serval seconds facial expression footage. It analyzes the dynamic changes of the facial expression and extracts an unique facial behavioral modalities for recognizing user's valid identity. Firstly, the dynamic changes of facial expression is related to facial bio-structure and each individual has a unique facial muscle condition. Specific facial structure or muscle-related bio-features such as the facial deformation or the distance of facial features are highly individual-dependent. Secondly, facial expression usually highly complies specific mental activity of human beings. Studies have found the close relationship between facial expression and human emotions [18]. Therefore, individuals hold unique facial behavioral modalities during expressing their emotions due to their different habits and experiences.

In our work, we develop an biometric-based authentication system and implement a prototype on android smartphone using video footage that captures the user's facial expression when authenticating the identity. Unlike *EyeVeri* [26], our approach does not require the visual stimuli to extract the physiological and behavioral biometrics. The user can appear any expression he wants to do when unlocking the device. This is more convenient and usability than the *EyeVeri* as the design of visual stimuli are obtrusive and require explicit action from the user. Furthermore, the video is filmed through built-in front camera of smatrphone. This differ from [25] that needs a additional eye tracking device, which limits it from being applied to a mobile environment.

This authentication system employs a computer vision algorithm to track the facial behavior from the video. Using

NDSS '17, 26 February -1 March 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2017.23xxx

the deformation information of facial features extracted from the facial behavior, it then establishes a disaggregated model to verify user's identity. Simultaneously, during authentication process we construct another classifier using the Gabor features of facial expression extracted by Gabor filter [14] to improve the recognition accuracy.

We thoroughly evaluate our approach using....

Contributions The key contribution of this paper is a novel authentication system for smart devices. Our system exploits techniques developed in the computer vision domain to address the key challenges highlighted above.

This paper makes the following specific contributions:

- *A New System:* We propose and implement a security and usable biometric-based authentication system based on facial expression on the smartphone without any extra hardware. Furthermore, this system does not require any visual stimuli so that it can accomplish authentication within 2 or 4 seconds.
- *New Findings:* We use the deformation information of facial features to authenticate user's identity and discovere that the facial deformation data can be regarded as a biometrics to uniquely identify one's identity.
- *Exploring New Technologies:* We develop a new authentication method by combining the facial deformation data with the Gabor features to dual coordination for improving the recognition accuracy. Our comprehensive evaluation shows that we can recognize one's identity with a accuracy of above 90%.

II. Background

A. Facial Expression

Facial expression is driven by a series of muscles movements beneath the skin of the face. These movements convey the individual's emotion status so that facial expressions are a form of nonverbal language to convey information in social interaction. Studies have discovered that there are at least 21 kinds of facial expressions including six basic expressions [13] and compound expressions consisted of the six basic expressions [12]. Psychologist stated that almost 55% volume of information are conveyed through facial expression in communication [17]. Thus, facial expressions carry a large amount of information in daily communication. Facial expression is pervasively used in human centered interfaces such as virtual reality [6], user profiling [4] and mental health [3] as it can present the individual's mental status. Unlike previous applications, in this paper, we discover that facial expressions also can be applied in recognize individual's identity because they are motivated by both individual's unique facial physiological structure and psychological activity. To the best of our knowledge, this is the first work to explore facial expressions as a biometrics on the smartphone.

B. Adversary Model

In adversary model, we assume an adversary wants to steal some sensitive information from or to install malware on victim's device. And we also assume that the adversary have the following abilities: (1) he can physically access to the target device for a short period of time; (2) he has the ability of impersonating the legitimate user for authenticating to the target device and (3) he is able to filmed the authentication process from a concealed angle since the authentication process can be observed in terms of the frequent use of smartphone.

Potential Attacks Given the above abilities that the adversary owns, we focus on two types of attack approaches that the adversary is able to perform:

- *Impersonation Attack* The adversary can mimic victim's expression to gain the access authority to the smartphone after temporary accessing to the target device. This is common attacks and is effective for some authentication methods such as keystroke [19] and touch gestures [11]. This attack can evaluate the robustness of biometric authentication system by calculating the Equal Error Rates (EER), which we further discussed in Section XX.
- *Replay Attack* Since the frequent use of smartphone, the adversary can record the entire authentication process from an unnoticeable position and replay the recorded authentication attempt to the authentication system. This poses a serious threat to current facial recognition system [23]. Our authentication system can effectively immune to this type of attack by detecting the facial deformation features, which is further detailed introduces in Section XX.

We believe the assumption that the attacker is able to access to legitimate user's authentication process is reasonable. This is because we are living in an age of interconnection and surrounded by many wireless or wired sensors so that it is possible to record our daily behaviors such as entire authentication process. However, most existing static biometric-based authentications such as iris and face recognition [7], are not secure under such assumptions. Our approach, in some extent, can prevent this this type of replay attack, which is one of the major strengths.

Limitations We do not consider the adversary is able to record the entire authentication process from the same view angle as the target device front camera. We believe this assumption is reasonable because it would arouse suspicion that recording the video from the right front view of users. Another potential threat to dynamic facial authentication system is that the attacker is able to compound facial expressions by construct 3D facial models [28]. However, this cannot pose threat to our authentication system as the compound facial expressions are not driven by user's real emotion statue so that the facial deformation features are not the same as real ones.

III. System Design Goals and Overview

We start this section by defining the design goals of our authentication system. We then gives an system overview which leverages the dynamic deformation features of facial expressions to authenticate identity.

A. Design Goals

Biometrics which refers to either the static physiological traits or dynamic behavioral modalities are all non-revocable. This is one of the major reasons why biometrics is possible to be stolen or replayed by an expert adversary. Unlike

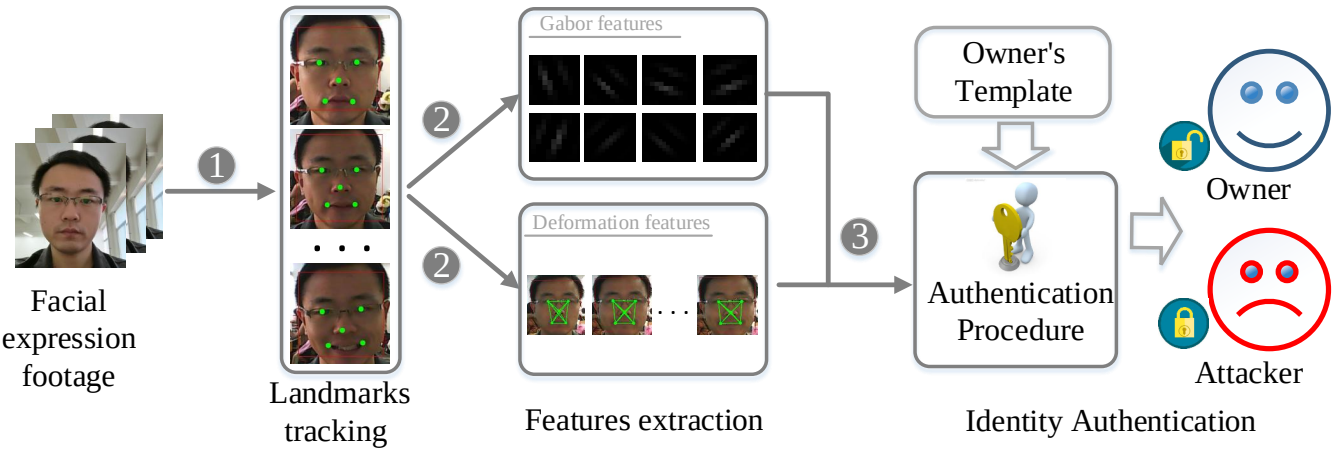

Figure 1. Overview of the attack.

traditional biometrics, facial behavioral traits is unique and can be changed with the changes of facial expressions. This is the biggest difference comparing with other biometric-based authentication systems. Therefore, facial behavior-based modalities are more secure than other biometrics in some extent. Furthermore, it is possible to decrease the authentication time as much as possible with the development of facial detection technologies as well as not requiring the visual stimuli. This making facial biometrics are more user-friendly. In conclusion, a secure biometric-based authentication system should be secure, fast and user-friendly. The following we summary the design goals of our system:

- *Simple:* This system should be simple as much as possible. Specifically, user should be minimal coordinate the system during authenticating process.
- *Fast:* A single authentication duration should be as short as possible.
- *Secure:* The system is able to immune to the replay and impersonation attacks.
- *Revocable:* The biometrics can be changed once it is stolen or leakage.

B. System Overview

The system authenticates the user's identity by analyzing the dynamic changes of facial expressions. It records the entire change of facial expressions using in-built front camera of smartphone. The deformation features of facial expressions are extracted by existing facial detection algorithm and they are used to recognize the user's identity. Figure 1 depicts the steps of this system:

① **Filming and Landmarks Tracking:** The authentication process begins from capturing the facial expressions. The video footage is filmed by in-built front camera of smartphone. During recording, the facial landmarks are simultaneously tracked automatically by facial detection algorithm.

② **Feature Extraction:** Once the facial landmarks are located, two types of feature extraction algorithms will be separately applied to extract two kinds of facial expression features. One is the Gabor features and the other is facial deformation features.

③ **Identity Authentication:** In this step, the system first verify the reality of the facial expressions by the part of facial deformation features. That is to say that whether or not the current facial expression is recorded by attacker in advance. Then it will check the user's identity combining the deformation features and the Gabor features. Finally, the system outputs the authentication results comparing to the owner's template trained when enrollment.

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] R. Acharya and M. Dolan, "Impact of antisocial and psychopathic traits on emotional facial expression recognition in alcohol abusers," *Personality and Mental Health*, vol. 6, no. 2, p. 126C137, 2012.

[4] I. Arapakis, Y. Moshfeghi, H. Joho, R. Ren, D. Hannah, and J. M. Jose, "Integrating facial expressions into user profiling for the improvement of a multimodal recommender system," in *IEEE International Conference on Multimedia and Expo*, 2009, pp. 1440–1443.

[5] G. Bailador, C. Sanchez-Avila, J. Guerra-Casanova, and D. S. S. Alberto, "Analysis of pattern recognition techniques for in-air signature biometrics," *Pattern Recognition*, vol. 44, no. 10-11, pp. 2468–2478, 2011.

[6] E. Bekele, Z. Zheng, A. Swanson, and J. Crittendon, "Understanding how adolescents with autism respond to

facial expressions in virtual reality environments," *IEEE Transactions on Visualization & Computer Graphics*, vol. 19, no. 4, pp. 711–720, 2013.

[7] A. Boehm, D. Chen, M. Frank, L. Huang, C. Kuo, T. Lolic, I. Martinovic, and D. Song, "Safe: Secure authentication with face and eyes," in *International Conference on Privacy and Security in Mobile Systems*, 2013, pp. 1 – 8.

[8] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *Pattern Analysis & Machine Intelligence IEEE Transactions on*, vol. 17, no. 10, pp. 955–966, 1995.

[9] X. Chen, J. Tian, Q. Su, X. Yang, and F. Y. Wang, *A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems*. Springer Berlin Heidelberg, 2005.

[10] 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.

[11] A. De Luca *et al.*, "Touch me once and I know it's you!: implicit authentication based on touch screen patterns," in *CHI '12*.

[12] S. Du, Y. Tao, and A. M. Martinez, "Compound facial expressions of emotion." *Proceedings of the National Academy of Sciences of the United States of America*, vol. 111, no. 15, pp. 1454–62, 2014.

[13] P. Ekman, W. V. Friesen, and P. Ellsworth, "- emotion in the human face," *Emotion in the Human Face*, p. 181C187, 1972.

[14] I. Fogel and D. Sagi, "Gabor filters as texture discriminator," *Biological Cybernetics*, vol. 61, no. 2, pp. 103–113, 1989.

[15] A. J. Fridlund, *Human facial expression: An evolutionary view.*, 1994.

[16] 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.

[17] I. Lebow, "Communication without wires," 2009, pp. 63–66.

[18] D. Matsumoto, H. S. Hwang, R. M. Lpez, and M. . Prez-Nieto, "Reading facial expressions of emotions: Basic research on emotions recognition improvement," *Ansiedad Y Estres*, vol. 19, no. 2, pp. 121–129, 2013.

[19] V. V. Phoha, S. Phoha, A. Ray, S. S. Joshi, and S. K. Vuyyuru, "Hidden markov model (hmm)-based user authentication using keystroke dynamics," 2012.

[20] J. Rogers, "Please enter your four-digit pin," *Financial Services Technology*, 2007.

[21] G. G. Rose, R. F. Quick, and A. Gantman, "Method and apparatus for simplified audio authentication," 2007.

[22] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch gesture-based authentication," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 4, pp. 568–582, 2014.

[23] K. P. Shashank Hegde, "Goldeneye: a face recognition based authentication system for smartphone applications," http://thegoldeneye.googlecode.com/files/GoldenEye.pdf.

[24] D. Shukla *et al.*, "Beware, your hands reveal your secrets!" in *CCS '14*.

[25] I. Sluganovic, M. Roeschlin, K. B. Rasmussen, and I. Martinovic, "Using reflexive eye movements for fast challenge-response authentication," in *ACM Sigsac Conference*, 2016.

[26] C. Song, A. Wang, K. Ren, and W. Xu, "Eyeveri: A secure and usable approach for smartphone user authentication," in *IEEE INFOCOM 2016 - IEEE Conference on Computer Communications*, 2016, pp. 1–9.

[27] W. Wang, A. X. Liu, and M. Shahzad, "Gait recognition using wifi signals," in *ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 363–373.

[28] Y. Xu, T. Price, J. M. Frahm, and F. Monrose, "Virtual u: Defeating face liveness detection by building virtual models from your public photos," in *25th USENIX Security Symposium (USENIX Security 16). USENIX Association*, 2016, pp. 497–512.

[29] Q. Yue *et al.*, "Blind recognition of touched keys: Attack and countermeasures," *arXiv preprint arXiv:1403.4829*, 2014.

[30] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in *Recent Advances in Intrusion Detection, International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009. Proceedings*, 2009, pp. 224–243.