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 [16] and can be stolen by shoulder surfing [28, 34] or video-based attacks [39, 45] 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 [13], voice [36] and iris [12] 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 [37] and keystroke pattern [46] 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 [7] and gait recognition [43] 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 [23]. 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 [18]. 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 [31]. 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* [41], 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 [40] 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
Copyright 2017 Internet Society, ISBN 1-891562-41-X
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 [22] 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 [19] and compound expressions consisted of the six basic expressions [18]. Psychologist stated that almost 55% volume of information are conveyed through facial expression in communication [29]. 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 [9], user profiling [6] and mental health [5] 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 [32] and touch gestures [17]. 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 [38]. 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 [10], 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 [44]. 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.

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.

3. Human identification system based on biometrics other than the face have already led to commercial products with very high identification rates: the iris [15] and fingerprints [35] 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:

- 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.
- 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.
- Good face recognition algorithms and appropriate preprocessing of the images can compensate for noise and slight variations in orientation, scale and illumination.
- 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 [24].

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 [21].

9. With the advances in miniaturization techniques, performance of the mobile and portable devices is rapidly increasing. This enables to use such devices not only as communication tools but also in an applications like m-banking [33] or m-government [26]. This means that they can store and process valuable information such as financial or private data. According to UK statistics in every three minutes a mobile phone is stolen [4]. The current protection mechanisms of these devices are usually based on PIN code or passwords. Nowadays a ”heavy” user has on average 21 passwords to remember [3]. Unfortunately, 81% of the users select common words as a passwords and 30% of users write their passwords down, which equally compromises security [3]. Recently, biometric modalities such as fingerprints [13, 42] have been proposed for mobile devices. However, both fingerprints and password entry are obtrusive and require explicit action from the user, which is not convenient in a frequent use. In order to improve security in mobile and portable devices, an unobtrusive mechanisms of authentication is desirable.

10. Geometric Deformation Features. The geometric displacement of certain selected Candide node,defined as the difference of the node coordinates between the first and the greatest facial expression intensity frame, is used as an input to a novel multiclass Support Vectot Machine (SVM) system of classifiers that are used to recognize either the six basic facial expressions or a set of chosen Facial Action Units (FAUs). **The leave-one cross-validation approach was used in order to make maximal use of the available data and produce averaged classification accuracy results.** [27].

11. The benefits of feature selection are not only to reduce recognition time by reducing the amount of data that needs to be analyzed, but also, in many cases, to produce better classification accuracy due to finite sample size effects [25].

III. Related Work

Our work lies at the intersection between human face recognition and biometric-based authentication methods. We bring together techniques developed in the domain of face recognition and identity authentication to develop a new authentication scheme.

Physiological biometrics

Behavioral biometrics

Face recognition The approaches reported regarding facial expression recognition can be distinguished in two main directions, the feature-based ones and the template-based ones, according to the method they use for facial information extraction. The feature-based methods use texture or geometrical information as features for expression information extraction. The template-based methods use 3-D or 2-D head and facial models as templates for expression information extraction.

- **Feature-Based Approaches:** Facial feature detection and tracking is based on active InfraRed illumination in [47], in order to provide visual information under variable lighting and head motion. The classification is performed using a Dynamic Bayesian Network (DBN). A method for static and dynamic segmentation and classification of facial expression is processed in [14]. For the static case, a DBN id used, organized in a tree structure. For the dynamic approach, multi level Hidden Markov Models (HMMs) classifiers are employed. The system proposed in [8] automatically detects frontal faces in the video stream and classifies them in seven classes in real time: neutral, anger, disgust, fear, joy, sadness, and surprise. An expression recognizer receives image regions produced by a face detector and then a Gabor representation of the facial image region is formed to be later processed by a bank of SVMs classifiers. Gabor filters are also used in [30] for facial expression recognition. Facial expression images are coded using a multiorientation, multiresolution set of Gabor filters which are topographically ordered and aligned approximately with the face. A Neural Network (NN) is employed to performe facial expression recognition in [48]. The features used can be either the geometric positions of a set of fiducial points on a face or a set of multiscale and multiorientation Gabor eavelet coefficients extracted from the facial image at the fiducial points. A convolutional NN was used in [20]. The system developed is robust to face location changes and scale variations. Feature extraction and facial expression classification were performed using neuron groups, having as input a feature map and properly adjusting the weights of the neurons for correct classification.
- **Model Template-Based Approaches:** A 3-D facial model used for facial expression recognition is also proposed in [11]. First, the head pose is estimated in a facial video sequences. Subsequently, face images are wraped onto a face model with canonical face geometry, then they are rotated to frontal ones, and are projected back onto the image plane. Pixels brightness is linearly rescaled and resulting images are convolved with a bank of Gabor kernels. The Gabor representations are then channelled to a bank of SVMs to perform facial expression recognition.

Expression recognition

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] "2002 nat monitor password survey." http://www.outlaw.com/page-3193, Last visit: 04.09.2006.

[4] "Huge surge in mobile phone thefts." http://news.bbc.co.uk/1/hi/uk/1748258.stm, Last visit: 04.09.2006.

[5] 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.

[6] 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.

[7] 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.

[8] M. S. Bartlett, G. Littlewort, I. Fasel, and J. R. Movellan, "Real time face detection and facial expression recognition: Development and applications to human computer interaction." vol. 5, pp. 53–53, 2003.

[9] 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.

[10] 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.

[11] B. Braathen, M. S. Bartlett, G. Littlewort, and E. Smith, "An approach to automatic recognition of spontaneous facial actions," in *IEEE International Conference on Automatic Face and Gesture Recognition, 2002. Proceedings*, 2002, pp. 360–365.

[12] 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.

[13] 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.

[14] I. Cohen, N. Sebe, A. Garg, L. S. Chen, and T. S. Huang, "Facial expression recognition from video sequences: temporal and static modeling," *Computer Vision & Image Understanding*, vol. 91, no. 1C2, pp. 160–187, 2003.

[15] 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.

[16] 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.

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

[18] 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.

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

[20] B. Fasel, "Multiscale facial expression recognition using convolutional neural networks." in *Icvgip 2002, Proceedings of the Third Indian Conference on Computer Vision, Graphics & Image Processing, Ahmadabad, India, December*, 2002, p. 8123.

[21] 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.

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

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

[24] 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.

[25] A. Jain and D. Zongker, "Feature selection: evaluation, application, and small sample performance," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 19, no. 2, pp. 153–158, 1997.

[26] Y. Kim, J. Yoon, S. Park, and J. Han, *Architecture for Implementing the Mobile Government Services in Korea*, 1970.

[27] I. Kotsia and I. Pitas, "Facial expression recognition in image sequences using geometric deformation features and support vector machines." *IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society*, vol. 16, no. 1, pp. 172–87, 2007.

[28] 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.

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

[30] M. Lyons, S. Akamatsu, M. Kamachi, and J. Gyoba, "Coding facial expressions with gabor wavelets," in *IEEE International Conference on Automatic Face and Gesture Recognition, 1998. Proceedings*, 1998, pp. 200–205.

[31] 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.

[32] 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.

[33] K. Pousttchi and M. Schurig, "Assessment of today's mobile banking applications from the view of customer requirements." in *Hawaii International Conference on System Sciences-Track*, 2004, pp. 70 184a–70 184a.

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

[35] 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.

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

[37] 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.

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

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

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

[41] 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.

[42] Q. Su, J. Tian, X. Chen, and X. Yang, *A Fingerprint Authentication System Based on Mobile Phone*. Springer Berlin Heidelberg, 2005.

[43] 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.

[44] 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.

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

[46] 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.

[47] Y. Zhang and Q. Ji, "Active and dynamic information fusion for facial expression understanding from image sequences," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 27, no. 5, pp. 699–714, 2005.

[48] Z. Zhang, M. Lyons, M. Schuster, and S. Akamatsu, "Comparison between geometry-based and gabor-wavelets-based facial expression recognition using multi-

layer perceptron," in *IEEE International Conference on Automatic Face and Gesture Recognition, 1998. Proceedings*, 1998, pp. 454–459.