Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics

Zhao Wang, Chao Shen(✉), and Yufei Chen

Xi'an Jiaotong University, No. 28 Xianning West Road, Xi'an 710049, China
{zhaowang,cshen,yfchen}@sei.xjtu.edu.cn

Abstract. The increasing usage of smartwatches to access sensitive and personal data while being applied in health monitoring and quick payment, has given rise to the need of convenient and secure authentication technique. However, traditional memory-based authentication methods like PIN are proved to be easily cracked or user-unfriendly. This paper presents a novel approach to unlock smartwatches or authenticate users' identities on smartwatches by analyzing a users' handwaving patterns. A filed study was conducted to design typical smartwatch unlocking scenarios and gather users' handwaving data. Behavioral features were extracted to accurately characterize users' handwaving patterns. Then a one-class classification algorithm based on scaled Manhattan distance was developed to perform the task of user authentication. Extensive experiments based on a newly established 150-person-time handwaving dataset with a smartwatch, are included to demonstrate the effectiveness of the proposed approach, which achieves an equal-error rate of 4.27% in free-shaking scenario and 14.46% in imitation-attack scenario. This level of accuracy shows that these is indeed identity information in handwaving behavior that can be used as a wearable authentication mechanism.

Keywords: Wearable devices · Smartwatch unlocking · User authentication · Motion sensor

1 Introduction

Recently, smart wearable devices gradually come into people's vision. They bring new means to human-computer interaction, and are also applied to instant messaging, quick payment and other fields, which usually store contact information, bank account password and other privacy information. Unfortunately, these devices are easy to be stolen for their portable and small size, even be attacked by malware [1]. Under such circumstances, it's emergency to solve the security problems of smart wearable devices.

The unlocking and identity authentication method is an indispensable part of smart wearable devices. Classical identity authentication methods are usually memory-based. The most widely used one is PIN unlock method. However, it's inconvenient to set a long password due to the small screen and frequent unlocking request especially in smart wearable devices, but short passwords are

J. Zhou et al. (Eds.): CCBR 2017, LNCS 10568, pp. 545–553, 2017.
https://doi.org/10.1007/978-3-319-69923-3_59

vulnerable to be cracked by guessing, peeping or brute-force attack. So, the traditional unlocking approaches seem to be not feasible for smart wearable devices.

Biometric methods are explored to meet the urgent demand for security and usability of the wearables, which can be divided into two main categories [2]: physiological characteristics and behavioral characteristics. The former contain voice, fingerprints, face, iris, etc., which are sensitive to external environment or personal status. While the latter, including gesture, typing habit, gait, mouse using habit, etc., which are not easy to be affected by external circumstance and performs well in most situations especially in terms of stability and reliability.

Compared with other behavioral characteristics, handwaving has its own advantages in biometric authentication for wearable devices. which is more unique, reliable and unduplicable, as it corresponds with physiological structure and behavioral habits. It has already been applied and proved feasible in some areas (e.g. smartphone unlock and authentication) preliminarily [3]. Meanwhile, handwaving based authentication is labour-saving, especially for smartwatch users.

However, how to extract a unique and stable pattern from handwaving gestures is still a challenging task. In this paper, we propose a handwaving based unlocking system, Alertor, for wearable devices, which is lightweight and user-friendly. The system first reads accelerometer data when user waves hand, and then preprocesses the raw data via shaking functions. And then it adopts Manhattan scaled one-class classifier to discriminate the true user and imposters. We recruited 10 volunteers and established a 150-person-time handwaving dataset with a Samsung Gear 2 smartwatch in multiple scenarios. Alertor achieves an EER of 4.27% in the free-shaking scenario and 14.46% in the imitation-attack scenario, demonstrating that our system is feasible and applicable.

2 Background and Related Work

In this section, we briefly review multiple applications of biometric methods.

2.1 Gait Authentication

Previous studies composed several different identity authentication methods based on user's gait habit [4–6]. But most results are claimed under an experimental environment. Actually, authentication accuracy may show an unstable behavior when facing various ground environments. For example, when people stand above the grass or snowfield or wet road, the precision rate may fluctuate observably. Besides, it can't be used while the user remains stationary. That is to say, this method's application is a bit limited.

2.2 Touch Authentication

The authentication based on touch gesture in literature started in 2013. Frank et al. published a paper about utilizing touchscreen swipe behavior to conduct continuous authentication [7]. After that, researchers concentrate on touchscreen click, swipe, drag and drop and other behavior features [8–10]. These previous studies proved the feasibility of identity authentication based on touch gesture: under the circumstance of a single environment and neglecting the observation time, the accuracy can reach more than 90% across current small data set. However, the stability of this method is not ideal since the numerical value of extracted feature vector is small. Feature will be indistinctive especially when the user has other drastic actions.

2.3 Accelerator Authentication

In biometrics areas, accelerator is an important data source for actions or behaviors sensing. There are several researches parallel to this study, utilizing accelerator to collect raw data of user's behavior pattern and extract features from these data to identify the user [11,12]. Just like what mentioned in [11], the user is asked to conduct a specific secret gesture in air to execute the authentication. Likewise, in [12], the user needs to hold a detection device and shake it up and down for 5 times. Both of the two means are similar to traditional PIN authentication method as they request for a specific behavior (or we can call it *gesture password*). So they have security vulnerabilities: once the gesture password has been recorded or glimpsed by someone else, the device may be hacked in without a hitch by action imitation.

3 Data Collection and Feature Extraction

In this section, we give a detailed introduction to data collection, establishment of dataset, and feature extraction.

3.1 Shaking Data Collection

We recruited 10 subjects into our experiment, including 7 males and 3 females, who are all students of campus. There are 9 right-handed and 1 left-handed. We developed a third-party application running in the background on a Samsung Gear S2 smartwatch to collect accelerometer data. All the data are recorded as a sequence of tuples in the form of (x_t, y_t, z_t), where x, y, z donate the acceleration in x-axis, y-axis and z-axis respectively, and t represents the timestamp.

In our experiment, we considered different attacker scenarios. In each session we select a user as the genius user and others as imposters, and all the subjects form a group. Then we divide the whole group into four classes (one genius-user type and three attacker types) with different tasks: firstly, the genius user shakes the smartwatch for three times and we record a video of him, where every single shaking procedure consists of one second waiting and nine seconds shaking. And then, we choose three imposters to watch the shaking video and shake the smartwatch for three times with recalling the gesture. Meanwhile, we select other three imposters to watch the video and imitate with the video while shaking the smartwatch for three times. At last, we choose all the remaining three imposters to shake the smartwatch for three times as they want. In this way, we collect 30 times shaking data for every single group, then we choose another genius user for data acquisition, we call it Group 2.

We can get data of Group 3 to Group 5 by repeating the steps. After 5 times collection, we have a total of 150 sets of shaking data (10 subjects × 3 times shaking × 5 different genius users). Finally, we has obtained approximately 150,000 raw tuples in total.

3.2 Data Preprocessing

Although in the data collection stage we set a built-in method to filter the outliers beyond the preset range, there are still some data not satisfied with our experiment. Therefore, we have to design a filter to remove these improper data, such as the data of the initial and end stage, whose value is too low to be recognized. The filter must have the properties of efficiency and robustness. We design a filter presented as follows:

$$\sum_{i=1}^{r}(A_i - m) \times \frac{(2b+1)}{(r-l+1)} < \alpha \qquad (1)$$

where A_i is the acceleration of time i, m is the mean value of raw data, r is the right boundary and l is the left boundary. b is the longest length of low-value data you can accept, a is the threshold which represents the lowest value you put into your experiment. The effect of this filtering algorithm is depicted in Fig. 1. It's obvious that the initial stage with low-value data have been removed.

3.3 Feature Extraction

The raw shaking data can't be used directly to anomaly detectors. So, we need to design a feature extraction procedure before system implementation. To investigate the raw data characteristics, we present several subjects' raw shaking data in Fig. 2, where the user 1 test1 and test2 represent two operations of same user, and the user 2 and 3 represent another two users' single operation respectively.

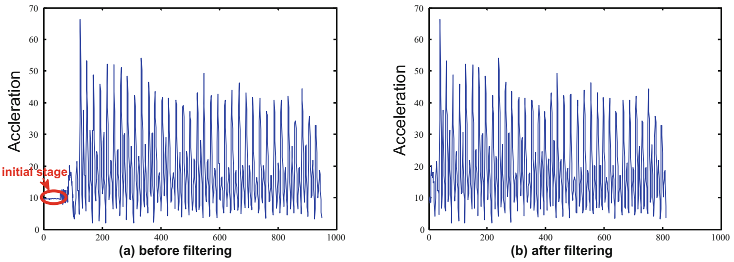


Fig. 1. Filter effect picture

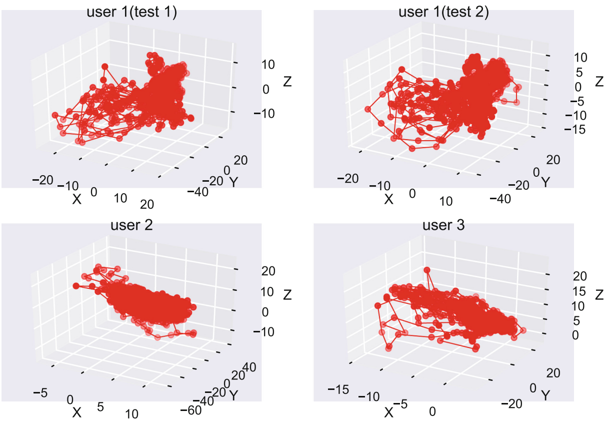
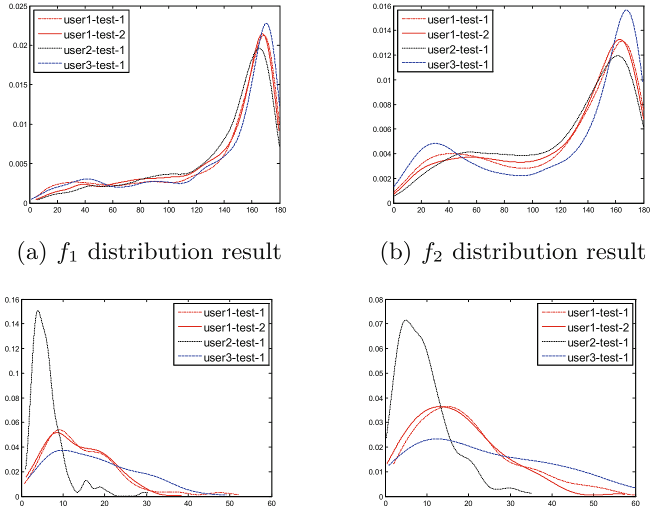


Fig. 2. User wave data contrast

Apparently, the raw data resemble across one test to another of the same subject, but differ from each other through different subjects. In order to depict the data characteristics, we define a shaking function, which is given by:

$$f = S(A) \tag{2}$$

where $A = \{(x_0, y_0, z_0), (x_1, y_1, z_1), \ldots, (x_n, y_n, z_n)\}$. A is the acceleration data sequence of subjects. We select A as the input and compute feature vector f as



(a) f_1 distribution result

(b) f_2 distribution result

(c) f_3 distribution result

(d) f_4 distribution result

Fig. 3. Shaking function distribution result

the output. We bring in 4 shaking functions which describe the data in angle and distance and apply them to the raw data and obtain results exhibited in Fig. 3. Obviously, the results of these four functions are satisfactory as the distinction of the features is clear. The distinguishing effect of f_4 is the most significant above all, so we finally choose f_4 as the shaking function we use to extract features.

4 Classification Framework and Experiments

Empirically, the features we extract in the previous section show a larger variance across different user than for a single user. This observation motivates us to classify the users among a classifier. In this section, we expound the classifier we use to identity authentication. Then we carried out various experiments to investigate the feasibility of the system we designed.

4.1 Choice of Classifiers

A classifier is designed to utilize the feature vector to distinguish the genius user and imposters. In the process of our experiment, we use Manhattan (scaled) classifier to classification. This classic detector was described by Araújo et al. [13]. In the training stage, the mean of feature vector matrix is computed, and the mean average deviation is also calculated. In the test stage, we calculate the Manhattan distance and make it to the similarity of two feature vectors, and choose it as the user score, the anomaly score is calculated by $\sum_{i=1}^{p} |x_i - y_i|/a_i$, where x_i and y_i are the value of i-th dimension of test and mean vector respectively, and a_i is the mean average deviation.

4.2 Influence of Application Scenarios

Safety guarantee varies with the application context and environment. If we set a high security level, the true user may be locked out of our system, while if it is too low, the imposters may easily hack in the system and theft of user's secret. Therefore, there must be a trade-off between usability and security. To measure the performance of our system, we use the FAR and FRR to generate a ROC curve, where FAR is *false acceptance rate*, representing the rate of imposters who has been accepted by our system; and FRR is the *false rejection rate*, representing the rate of genius user who has been rejected by our system. A ROC curve example of Manhattan (scaled) detector and SVM detector is shown in Fig. 4. We choose the point where the FAR equals to the FRR, and call it as EER (equal-error rate).

As described in Sect. 3, we consider three types of application scenarios, which are: imitating, imitating with video and the shake as what you like. Instinctively the first two scenarios may have a high ability to break into the system, but the last is weaker. For this reason, we experimentally analyze three different authentication scenarios.

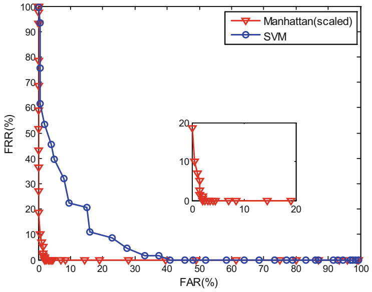


Fig. 4. ROC curve example

We train our system and test it as follows:

1. In every single test, we choose one genius user, and let the rest of the group subjects as imposters.
2. Then, we train our system with the first set of shaking data of the true user.
3. Finally, we test the system with the remaining data of the true user and all the three sets of data of imposters.

This progress is repeated among 5 groups, designating single person in every group as the genius user in turn, and train the system the corresponding three-time shaking data. After training 150 times (10 subjects × 5 groups × 3 times) and testing for all datasets we collected for 4350 times(29 Non-training data × 30 individual data in every group × 5group), we have got 150 sets EERs (10 subjects × 5 groups × 3 times) in total. Then we calculate the mean value of them, and present the experiment result in Table 1 and Fig. 4. In general, the performance of our system works well in the case of uninformed imposters, and the video imitators can enter the system more easily than the imitators of memory.

Table 1. Different scenarios authentication accuracy

User type	Video imitation	Recall imitation	Free shaking
Mean EERs	0.2314	0.0578	0.0427

5 Conclusion

The trend to access and store privacy information using wearable devices has stressed an urgent demand of applicable and handy authentication mechanism for wearable devices. To the best of our knowledge, our work is the first to systematically design and evaluate the biometric authentication scheme on smart wearable devices. From data acquisition and preprocessing, feature extraction to classification, we provide a detailed implementation of handwaving-gesture authentication system on wearable devices. Furthermore, we collected handwaving data from 10 subjects and have established a 150-person-time dataset to evaluate authentication performance and facilitate future research. Our experimental results indicate that our system is capable of discriminating genuine user and resisting imitation attacks.

Aknowledgement. This work was supported in part by the National Natural Science Foundation of China under Grant 61403301 and Grant 61773310, in part by the China Postdoctoral Science Foundation under Grant 2014M560783 and Grant 2015T81032, in part by the Natural Science Foundation of Shaanxi Province under Grant 2015JQ6216, and in part by the Fundamental Research Funds for the Central Universities under Grant xjj2015115.

References

1. Shrestha, B., Saxena, N., Harrison, J.: Wave-to-access: protecting sensitive mobile device services via a hand waving gesture. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 199–217. Springer, Cham (2013). doi:10.1007/978-3-319-02937-5_11
2. Alzubaidi, A., Kalita, J.: Authentication of smartphone users using behavioral biometrics. IEEE Commun. Surv. Tutor. **18**(3), 1998–2026 (2016)
3. Blasco, J., Chen, T.M., Tapiador, J., Peris-Lopez, P.: A survey of wearable biometric recognition systems. ACM Comput. Surv. (CSUR) **49**(3), 43 (2016)
4. Gafurov, D., Helkala, K., Søndrol, T.: Biometric gait authentication using accelerometer sensor. JCP **1**(7), 51–59 (2006)
5. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1–7. IEEE (2010)
6. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.M., Ailisto, H.A.: Identifying users of portable devices from gait pattern with accelerometers. In: IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP 2005), Vol. 2, pp. ii-973. IEEE (2005)
7. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. **8**(1), 136–148 (2013)
8. Saravanan, P., Clarke, S., Chau, D.H.P., Zha, H.: Latentgesture: active user authentication through background touch analysis. In: Proceedings of the Second International Symposium of Chinese CHI, pp. 110–113. ACM (2014)
9. Zhang, H., Patel, V.M., Fathy, M., Chellappa, R.: Touch gesture-based active user authentication using dictionaries. In: 2015 IEEE Winter Conference on Applications of Computer Vision (WACV), pp. 207–214. IEEE (2015)
10. El Masri, A., Wechsler, H., Likarish, P., Grayson, C., Pu, C., Al-Arayed, D., Kang, B.B.: Active authentication using scrolling behaviors. In: 2015 6th International Conference on Information and Communication Systems (ICICS), pp. 257–262. IEEE (2015)
11. Liu, J., Zhong, L., Wickramasuriya, J., Vasudevan, V.: User evaluation of lightweight user authentication with a single tri-axis accelerometer. In: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services, p. 15. ACM (2009)

12. Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A.: A study on biometric authentication based on arm sweep action with acceleration sensor. In: 2006 International Symposium on Intelligent Signal Processing and Communications, ISPACS 2006, pp. 219–222. IEEE (2006)
13. Araújo, L.C., Sucupira, L.H., Lizarraga, M.G., Ling, L.L., Yabu-Uti, J.B.T.: User authentication through typing biometrics features. IEEE Trans. Signal Process. **53**(2), 851–855 (2005)