Enhancing smartphone security through behavioral biometrics-based gestures

Daniela Chudá [1], Lukáš Janík [2]

[1]*Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Slovakia*
[2]*UXtweak, Bratislava, Slovakia*

Abstract

Smartphones have become a personal device allowing access to various services with the need for additional protection against theft or leakage of personal data. One possibility is an alternative method of user recognition on the Android platform based on behavioral biometrics. We suggest using simple movement gestures performed by the user while holding the smartphone in their hand as an additional form of recognition of the authorized user. We experimentally verify the usability of individual gestures, and the security achieved in terms of the ability to distinguish the authorized user.

Keywords

behavioral biometrics, user identification, gestures, biometric features

1. Introduction

With the advancement of technology, smartphones are becoming a means of enabling access to various services, increasing the importance of securing the device and accessing its data. Achieving a sufficient level of security is more complicated in smartphones, as the average time of interaction with the device is much shorter than in the case of a laptop computer, and asking the user to authenticate again can have a disruptive effect. A promising approach is behavioral biometrics, which deals with monitoring the user's behavior concerning selected activities. We can monitor the way the user touches the display, or the user performs the gesture with the device. Based on such biometric (behavioral) data, it is subsequently possible to create a unique biometric signature of the user for identification or authentication.

In this work, we propose an alternative user recognition method on the Android platform based on behavioral biometrics. Simple movement gestures when the user holds the smartphone in hand serve to model the user behavior. This approach has the premise of easily becoming part of the user's normal interaction with the device, without the need for the user to think about the gesture being performed.

The biometric characteristics should be sufficiently invariant with respect to time with no significant changes [6]. Otherwise, the system working with biometrics might not work properly. The user would need to frequently repeat the registration phase given the significant changes in the monitored biometric characteristics.

For biometric systems, there are three basic metrics, or criteria based on which we can evaluate its performance (correctness): the probability of false acceptance of the user (False Acceptance Rate - FAR), the probability of false rejection of the user (False Rejection Rate - FRR) and the equal error rate (Equal Error Rate - ERR) [3, 6].

The most frequently used and commonly found sensors in smartphones include the accelerometer [1,2,7,8], gyroscope [1,2,5,8], and magnetometer [1,2].

S. Lee and the collective [4] in their work dealt with the use of gestures performed with a smartphone held in the hand for authentication. They were based on the idea that users can

ITAT'24: Workshop on Applied Security 2024, September 20–24, 2024, Drienica, Slovakia
EMAIL: daniela.chuda@stuba.sk (D.Chudá)
ORCID: 0000-0002-3873-9308

generate a password in the form of gestures instead of a traditional numeric password.

In their work, L. Yang and colleagues [8] dealt with the use of shaking and waving with a smartphone (handwaving) for authentication.

Z. Sun and his team [6] dealt with the authentication system in their work using gestures and created an application for obtaining data about gestures and their subsequent evaluation to distinguish the authorized user. They also tested their solution using different devices. They attribute the different results they achieved to differences in the devices' sensors.

2. Use of gestures based on behavioral biometrics

In this work, we investigated the use of behavioral biometrics in context of smartphones with a focus on using data from the device's sensors for behavior modeling of the user, which can take various forms - touch, writing, or movement with the device perceived as simple gestures. We focused on these simple gestures in this work.

We created a set of 5 gestures:

1. device shaking,
2. holding the device to the ear,
3. turning left and right,
4. movement of the device within one axis,
5. movement in a circle.

We designed, implemented, and verified a prototype mechanism using gestures to recognize a targeted user.

We devoted ourselves to researching the usability of simple gestures from a defined set performed with a smartphone held in the hand, as well as different approaches in data processing for user recognition. We can consider the most common use of gestures to invoke some activity. However, considering the results achieved, we can consider individual gestures to be equivalent and usable for user recognition. We can also consider it interesting to enrich the execution of the gesture with the element of touch. The proposed solution assumes a mechanism for recognizing the targeted user based on the behavior when performing the mentioned gestures from the selected set. When experimenting, we use two modules: the module that collects and logs the data of individual gestures and the data evaluation module. The data evaluation module implements the entire process from processing the collected data to model training and subsequent data evaluation. The generic approach is an approach applicable primarily in the case of a binary classification model, in which data from other users is also made available during training. In this case, we can consider creating a generic model setting, or models, since we are considering having a separate model on the one hand for each gesture, but also for each sensor. For the model created in this way, we assume that it will generally perform well and be applicable. An important part of the model is the very features with which the model works. In this direction, we are also considering the creation of a general set of features, based on which the model will be able to sufficiently distinguish individual users. It is important to note, however, that under a generic model, we do not imagine the creation of a model that will be trained once and then be generally applicable to any user. Model training will be performed for each user separately, but we will have the settings and features selected in advance.

We conducted experiments with 30 participants. Due to the sensors used, we use and log data - data in two-dimensional space (touch data from the touch screen of the device) and in three-dimensional space (accelerometer, gyroscope, linear acceleration, rotation vector). The calculated characteristics can be divided into two basic groups - characteristics from the time domain and the frequency domain. The collected, logged data from participants must be pre-processed. We used filtering, segmentation, calculation of characteristics, and then division into three data sets - training, validation, and testing. We decided to experiment with models for binary classification: *k*-nearest neighbors (*k*NN), support vector machine (SVM), and random forest (RF). We also decided to experiment with the size of the time window for gesture segmentation (0.25s and 0.50s interval) with 50% overlap. Since we collected data from several sensors during logging, we needed to create a separate model for each sensor and then aggregate partial predictions into one final prediction. For this purpose, we created a mechanism that adds up either the percentage certainty of the prediction belonging to the class or binary values and determines the final prediction by comparing the resulting values. We selected three models that achieved promising results. The performance of individual models for binary classification, generic model, interval 0.25s, without touch and with touch can be seen in Figures 1 and 2.

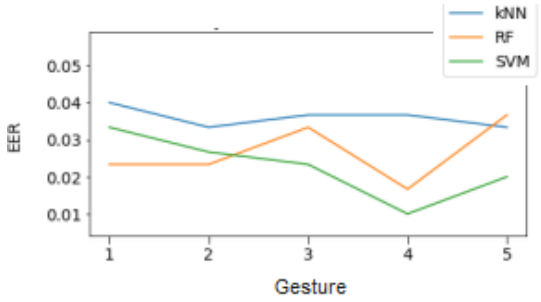

Figure 1: Graph of balanced error rate EER for all gestures 1-5. Generic model, interval 0.25s, with touch.

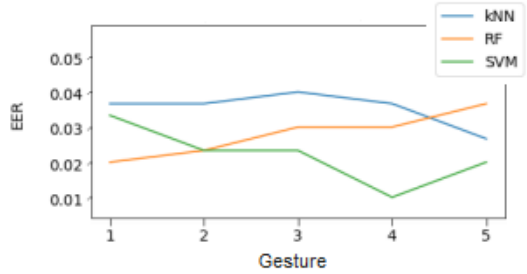

Figure 2: Graph of balanced error rate EER for all gestures 1-5. Generic model, interval 0.25s, without touch.

3. Conclusion

For a user recognition system, it is very important to have a low FAR value, since wrong identification as an expected user can cause considerable damage, especially if the recognition mechanism is used for authentication purposes. However, it is also important to achieve low FRR, as this can also significantly reduce the usability of the system in the case of the expected user being too often marked as some other user. Therefore, we consider it important to achieve a balance between both values, which are expressed by the EER metric and which we used in the optimization of the models.

From the point of view of the chosen size of the time window, binary classification models generally performed better on a shorter time window (interval 0.25s). Taking all results into account, on average the models achieve an EER of ~0.028 at this interval compared to ~0.030 for the longer time window (0.50s interval). The reason for the greater success of a shorter window can be attributed to a larger number of samples and thus a slightly more accurate representation of the execution of the gesture, which also means more information for the model. To evaluate overall success, we work with average values that are calculated from all gestures and all considered models. From the results achieved on the test and validation data, as well as in comparison with other works, we can conclude that such a user recognition mechanism can recognize the targeted user with sufficient accuracy. We also note that this is a usable set of gestures for user recognition.

References

[1] Noureldin, A., Yanyan, Y. (2017). Game Authentication Based on Behavior Pattern. In Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia (MoMM2017). Association for Computing Machinery, New York, NY, USA, 151–156. https://doi.org/10.1145/3151848.3151878

[2] Ehatisham-ul-Haq, M., et all (2017). Identifying Smartphone Users based on their Activity Patterns via Mobile Sensing, In Procedia Computer Science, Volume 113, 2017, Pages 202-209, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.08.349.

[3] Guse, D., Müller, B. (2012). Gesture-based User Authentication for Mobile Devices using Accelerometer and Gyroscope. Informatiktage.

[4] Lee, S. et al. (2012). Access to an automated security system using gesture-based passwords. In Proceedings of the 2012 15th International Conference on Network-Based Information Systems, NBIS 2012. 2012. s. 760–765.

[5] Lee, W.H. - LEE, R.B. (2017). Sensor-Based Implicit Authentication of Smartphone Users. In Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017. Institute of Electrical and Electronics Engineers Inc., 2017. s. 309–320.

[6] Sun, Z. et al. (2016). A 3-D hand gesture signature based biometric authentication system for smartphones. In Security and Communication Networks. 2016. Vol. 9, no. 11, s. 1359–1373.

[7] Varga, J. et al. (2017). Authentication based on gestures with smartphone in hand. In Journal of Electrical Engineering. 2017. Vol. 68, s. 256–266.

[8] Yang, L. et al. (2015). Unlocking Smart Phone through Handwaving Biometrics. In IEEE Transactions on Mobile Computing. 2015. Vol. 14, no. 5, s. 1044–1055.