Pre-print of article that will appear at ICB 2019.

Gesture-based User Identity Verification as an Open Set Problem for Smartphones

Kálmán Tornai
Fac. of Information Technology and Bionics
Pazmany Peter Catholic University
Budapest, Hungary
tornai.kalman@itk.ppke.hu

Walter J. Scheirer
Dept. of Computer Science and Engineering
University of Notre Dame
Notre Dame, IN 46556
walter.scheirer@nd.edu

Abstract

The most straightforward, yet insecure, methods of authenticating a person on smartphones derive from the solutions applied to personal computers or smart cards, namely the authorization by passwords or numeric codes. Alarmingly, the widespread use of smartphone platforms implies that people are carrying around sensitive information in their pocket, making the information more available physically. As smartphone owners are often using their devices in public areas, these short numeric codes or other forms of passwords can be obtained quickly through shoulder surfing, resulting in making that restricted data far more accessible for those who are not authorized to access the device. In this paper, we address the problem of biometric verification on smartphones. We propose a new approach for gesture-based verification that makes use of open set recognition algorithms. Further, we introduce a new database of inertial measurements to investigate the user identification capabilities of this approach. The results we have obtained indicate that this approach is a feasible solution, although the precision of the method depends highly on the chosen samples of the training set.

1. Introduction

The evolution of the tools of proving identity to access data or capabilities of a device has a long, and often checkered, history. The most simple, but inherently insecure, ways of authentication are the password- or passcode-based solutions. In these schemes, the user identity is recognized based on a knowledge of information that is supposed to be known only by that specific user. In the case of these methods, it is also presumed that authorized users are using unique, long, randomized and secret passphrases to prevent successful attacks. However, usability studies have shown that the security awareness of computer and smartphone users is far from ideal, which ultimately leads to unauthorized access to sensitive data.

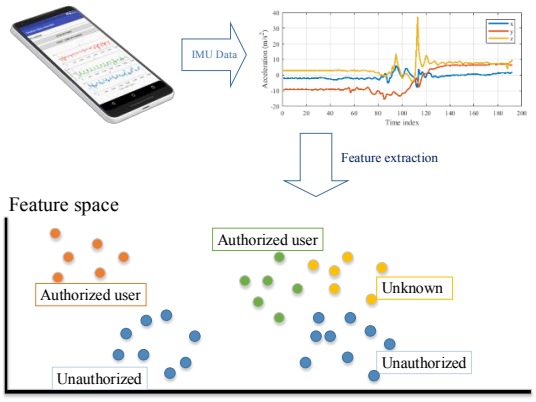

Figure 1. The identity of the smartphone user is verified based on the accelerometer measurements recorded while the user is responding to a notification or call from the device. Open set recognition algorithms are deployed to detect authorized users and to reject unknown and unauthorized users as well.

Developers have recognized this fact, and manufacturers as well, resulting in new techniques and algorithms for user authentication involving the recognition of different physiological biometric properties. The most current solutions are the application of fingerprint sensors and face recognition algorithms.

Although these technologies are advertised as a significant advancement in security, they are prone to attack by spoofing. Therefore, it is necessary to step forward to behavioral biometrics, which are often described as the next level of user authentication. Hence, the focus of research

978-1-7281-3640-0/19/$31.00

into individual biometric modalities is shifting to develop better behavioral biometric-based solutions.

With mobile phones taking over the role of wallets, as well as becoming the primary platform for banking, the importance of developments in behavioral biometrics is increasing, especially the development of authentication methods that are capable of mitigating the typical types of attacks like spoofing that affect other modalities.

The primary objective of our research is to investigate whether smartphone user identity verification can be solved by applying open set recognition algorithms on brief measurements from the inertial measurement unit (IMU). Every user (authorized, unauthorized, and unknown) can be characterized by a set of features, which is calculated from the IMU measurement time series data. The novel approach introduced in this work is that the feature set space is considered as an open space where the authorized users are supposed to be recognized, and any other, unknown users (or attempts of spoofing) have to be declined. We carried out the accurate recognition of the authorized users by the application of recently introduced open set machine learning tools [14, 23]. Figure 1 illustrates the concept of our method. To investigate the capabilities and the performance of this approach we collected a new database containing IMU recordings of volunteers performing brief gestures such as picking the phone up from different places and in different positions.

The rest of this paper is organized as follows. In Section 2, the current existing smartphone user authentication methods are briefly introduced, as well as an overview of IMU sensor technology. The main contributions of this paper are the new open set recognition-based user identity verification method and the database of the IMU measurements. In Section 3.1 we review recent innovations in algorithms that address the open set recognition problem, and discuss our problem formulation for this work. A comprehensive description of the database is given in Section 4. The details of the experiments and the obtained performance results are described in Section 5. Finally, Section 6 concludes the paper with the interpretation of the results and a few suggestions for future work.

2. Related Work in Biometrics

In this section, the related technologies and results of the field of mobile biometric user identification and IMU data processing will be briefly summarized.

2.1. Biometric Authentication on Smartphones

Lately, manufacturers and developers have put more emphasis on biometric authentication for both mobile and traditional desktop platforms. Modern devices are equipped with fingerprint readers, and a high-resolution front-facing camera is available for face recognition purposes. Beyond these traditional biometric modalities, results have been published on behavioral biometric-based solutions such as i) the analysis of keystroke dynamics; ii) touch gesture-based authentication; iii) behavioral profiling; and iv) gait recognition [19].

Fingerprint readers are commonly deployed on many devices and are now considered a standard security feature in mobile product lines. The sensor technologies underlying commercial fingerprint readers are still developing. Recently, An *et al*. [2] published details about a transparent and flexible fingerprint sensor array.

Despite the widespread adoption of this technology, it cannot be considered entirely reliable. Several research groups have demonstrated the vulnerability of fingerprint reader including the use of fake fingerprint data, and other spoofing methods [22]. Along with the counterfeiting methods, the algorithms for detecting attacks are also improving. In an open set context, where not all attacks are known at enrollment time, Rattani *et al*. [21] described a method for spoof detection across novel fabrication materials.

Latterly, smartphone manufacturers have started to implement **face recognition-based user authentication** methods in their devices using different sensors and software solutions. In the case of this approach, still images or brief video streams are taken by the front-facing camera of the device and are subsequently analyzed for correspondence to an enrolled template. To further enhance the setup, dedicated infrared sensors or cameras may be used to obtain a better model of the user's face, even in poor lighting conditions.

Similarly to the fingerprint recognition based methods, the main drawback of this solution is that current applications on the market are vulnerable to even simple methods of attacks [10]. With respect to physical attacks, recent research results indicate that face recognition systems can be hacked even with cheap materials. For example, the iPhone X face ID has been hacked with a 3D printed mask [28], and the facial recognition methods implemented by Samsung can be spoofed with a photo displayed on another phone [16].

Recently Repera et al. [20] demonstrated that open-set recognition based face authentication can be applied on mobile devices. They introduce the Extremal Openset Rejection method and a semi-parametric model based on the Extreme Value Theory. Performance demonstrations on three publicly available datasets are showing that the method can achieve good results on small datasets.

The analysis of **keystroke dynamics** is one of the oldest behavioral biometric authentication methods. It was introduced a long time ago to verify the user identity on desktop computers in a continuous manner (an early instance of active authentication). In the case of smartphones, the method can be adapted for use in a mobile setting. However, instead

of keystroke dynamics, the touch strokes of the virtual keyboard have to be analyzed.

State of the art keystroke-based methods show a wide range of performance. Feng *et al*. [9] deployed J48 Decision Trees, Random Forests, and Bayesian Network classification methods to achieve performance as low as a 1.0% false accept rate (FAR) and 1.0% false reject rate (FRR). Attaullah *et al*. [3] introduced a method that combines the keystroke analysis with the IMU measurements, improving the final recognition capabilities.

Touch gesture-based methods are based on measuring and analyzing the touch positions, intensity, timings, and movements associated with unlocking a phone. The touch gesture is a fingertip drawn shape on the smartphone's touchscreen containing one or several strokes. The touch gesture can be used either as an extra measure for security or the primary authentication method for the device.

The available gesture-based authentication solutions are mostly based on the assumption that the smartphone users are performing the gestures in a way that reflects their distinct behaviors. Thus the features extracted from measurements should be different from one user to another. Feng *et al*. [8] demonstrated that touch gesture analysis could be used for user authentication with a FAR is below 5% and the FRR is 0.13%. By the application of several different classification methods, the equal error rate (EER) for these methods varies between 0.5% and 42% [1].

The analysis of **behavioral patterns** can also be used as a transparent and continuous identity verification method. The typical user interactions with the services and application of the mobile device as well as the locations that are being discovered can be profiled, and any deviations from the learned profile can be detected. This method has been deployed mainly as a network-based approach since its inception. However, good results also could be achieved by using model-based approaches, such as Hidden Markovian Models. [18] Recent methods are utilizing machine learning algorithms to create user profiles.

The capability of providing transparent and continuous identity verification is the main advantage of these methods. However, if the legitimate user demonstrates unusual behavioral patterns, then the accuracy of these methods decreases.

The wide range of features of the user's behavior covers the usage statistics of different applications; call and texting behavior patterns; ambient sensor measurements; and Wi-Fi/GPS locations. By deploying these methods, the FAR and FRR can be as low as 11.4% and 4.2% respectively [17].

Gait-based recognition methods identify the user based on the properties of the way the they walk. Gait analysis using the smartphone's inertial measurements unit for authentication. These sensors are hidden in the devices and do not make direct contact with the user. Therefore this method can be designed to be resistant to spoofing attacks.

By applying a fuzzy commitment scheme for specific movements, Hoang *et al*. [12] introduced a solution which provides a 0% FAR and 16.81% FRR. In general, an EER of between $5 - 20\%$ can be achieved in the case of gait based authentication [19, 24]. Although the performance of gait-based recognition solutions is good, two significant drawbacks introduce restrictions on the possible use cases. The first is that some of the best results are obtained by using several external sensors in addition to hidden internal sensors. Secondly, recognizing the gait of a user requires them to perform specific movements (lasting several seconds) to unlock the phone.

2.2. IMU Sensors of Smartphones

The IMU of the modern smartphone (in reference here to both Android and iPhone platforms) measures the translational acceleration values (in three dimensions) and the angular velocity values (gyroscopic motion) of actions. Based on the signals of the IMU chip, further virtual sensors can be invoked by the system. However, the precision and capabilities are bound by the actual hardware. In the case of a high-end device, the sensor precision is $12 - 14$ bits, and the theoretical sampling frequency is in the kilohertz interval. (e.g., the Bosh Sensortec BMA456 [5]). Depending on the implementation, the sensitivity of the sensor can be $0.009m/s^2$ when the range is $\pm 2g$ as well as $0.08m/s^2$ for the range of $\pm 16g$. The typical offset error is $\pm 0.9m/s^2$ for calibrated sensors. The built-in gyroscope also has similar properties: $\pm 31.25rad/sec$ to $\pm 2000rad/sec$ along with 1% precision up to a 33 kHz sampling interval (InvenSense ICM-20690 [13]). Smartphones can capture gestures and movements with a high level of precision, and in most cases with low energy consumption as well.

3. Identity Verification as Open Set Recognition

In the case of a closed set problem (typically multi-class classification in biometrics) all of the classes are known before training. That leads to the problem that instances of an initially unknown class are "forced" into any of the known classes. However, the task of general recognition implies that the solution should be capable of labeling a sample as unknown or unrecognized, which would significantly decrease the rate of false positives in a real application. Existing approaches are focusing on the (multimodal) authentication of a single user, and considering others as intruders. By applying open set recognition tools, our objective is to create an authentication solution that is capable of recognizing multiple known users (who are distinguished. Therefore their access to sensitive data or applications can be controlled) as well as rejecting any other people or impostors.

3.1. The Open Set Recognition Problem

Recent studies of open set problems resulted in the formalization of openness, open space risk [26] and a probability model for open set recognition [25]. Scheirer *et al*. introduced [26] a new variant of the support vector machine (SVM), the 1-vs-Set machine, which minimizes the positive labeled region of the open space (the labeled space far from the support of any known training data). Experimental results for open set problems showed better performance for the 1-vs-Set machine compared to the standard SVM. Cevikalp and Triggs described a similar algorithm to the 1-vs-set machine [6]. They combine a binary classifier and an SVDD classifier for positive classes to provide improved performance.

A number of algorithms that are underpinned by the statistical extreme value theory also exist. They are the current state-of-the-art in open set recognition. Jain *et al*. introduced the P_I-SVM and P_I-OSVM [14], which estimates the unnormalized posterior probability of class inclusion. The P_I-SVM significantly outperformed the 1-vs-Set machine with between a $12\% - 22\%$ improvement in F-measure. Later, Scheirer *et al*. introduced the W-SVM [25] for multi-class open set recognition problems. The W-SVM uses nonlinear kernels providing a more accurate solution. However, the model construction requires more computations and memory. Bendale and Boult created the OpenMax architecture [4], which limits the open space risk for deep networks, allowing the rejection of "fooling" and unrelated open set objects presented to a deep network. The Extreme Value Machine (EVM) [23] takes distributional information into account while learning the recognition function for a classifier. The EVM is capable of performing nonlinear classification without using kernels. According to the experimental results reported by Rudd *et al*. [23], the EVM performs similarly to the W-SVM and also outperforms the other methods. Furthermore G unther el al. [11] demonstrated the performance of the EVM on face recognition problems, achieving 1% FAR. However, the overall accuracy of the method was around 60%. In this work, we will focus our attention on the P_I-SVM and EVM algorithms.

3.2. Novel Approach for Identity Verification

Our research objective is to establish a transparent biometric authentication method, which processes short segments of data measurements, but does not require the smartphone user to perform a specific action after a prompt (e.g., walk, type, or perform a gesture on screen) to unlock the device. (Behavioral pattern analysis-based methods require longer observations.) Therefore we implemented a method for the identity verification of smartphone users problem that uses short sequences of inertial sensor measurements. The inertial sensor data can represent different everyday user actions such as retrieving the phone from a pocket or a desk.

Other user authentication methods based on keystroke, gesture, gait or behavioral profile analysis use standard classification methods to make a decision about the identity associated with a newly recorded sample. As previously discussed, in the case of recognition tasks the classification-based approach is always forced to assign a class label to every object, which can lead to false acceptance. For that reason, we have investigated what level of detection accuracy can be achieved if the user identity verification problem is considered as an open set recognition problem, where not all users encountered in operation are known at training time. In a biometrics context, open set-specific classifiers are able to reject impostors, who do not have legitimate access to a device. Figure 2 illustrates the concept of this approach.

4. Data Collection

To conduct the experiments, a new database has been constructed as existing databases are mainly focusing on capturing data while different users are performing the same or similar actions. We required this dataset as we needed IMU readings about the same activities performed multiple times by different people to train and test our system.

IMU time-series data have been recorded by using a Google Pixel XL (G-2PW2200) smartphone and a Huawei Watch (0213). On these devices, the latest publicly available Android OS versions were running (Android 8.1.0 OPM4 and Android 7.1.1 NWD1 respectively). A new Android application was developed to record the sensor measurements, which implements the following measurement protocol. The sample ratio was set to the maximum, which was 200 Hz in the case of the phone, and 50 Hz for the smartwatch.

The measurement protocol was designed to imitate a real-life scenario as follows: the phone is initially unused and is being held in a pocket or laying on a table. During this inactive period, the phone receives a text message or a call which triggers a visible and audible notification. The user, wishing to respond to the notification, then locates and grabs the device (i.e., pulls out the phone from a pocket or lifts it up from the table).

The inertial and acceleration sensor readings that are collected while the user grabs or picks up the device are stored in the database. To collect such data, each participant was asked to perform the following tasks repeatedly: i) Press the physical power button on the phone to initiate the measurement and lock the phone; ii) Place the device in the pocket or on the desk depending on the scenario; iii) Wait for the notification. This step starts the data recording; iv) Respond to the notification by removing the device from the pocket or table; v) Dismiss the notification with a swipe or touch gesture. This step finishes the data recording.

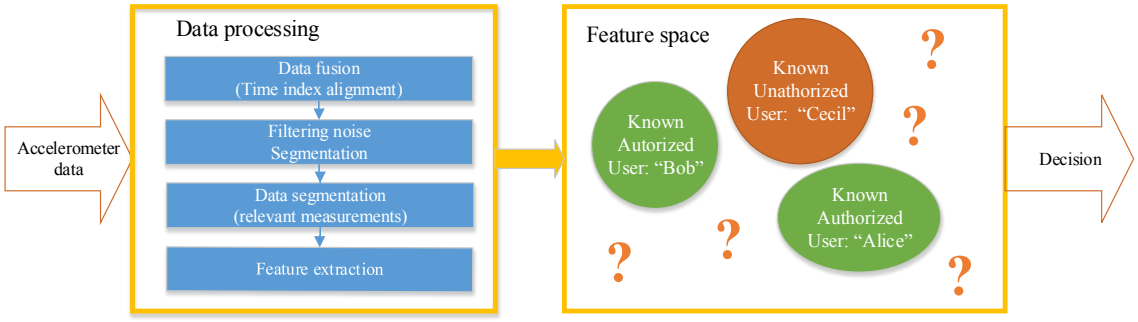

Figure 2. At acqusition time, accelerometer data is recorded while the smartphone user is responding to notifications of the phone. The recorded accelerometer values are processed, noise is filtered, and a segment is cut that corresponds to the gesture. The input of the open set recognition algorithm is a set of statistical features of the recorded signal. Over the feature space, the P_I-SVM and EVM algorithms are being used to verify the identity of known, authorized users.

Participants were also asked to perform the task with the same hand each time, but no further instruction was given (e.g., where or how to place the phone on the table; use different or the same positions during the session). Further, the proctor of the experiments engaged in small talk with the participants to avoid a situation where they were extensively focusing on "performing well" on the tasks; and to ensure natural behavior was captured as much as possible.

During each measuring session, four or five different scenarios have been simulated. (Each session had a fixed 30 minute timeframe, which limited the number of scenarios.) These were the following: i) The phone is in the pocket while sitting; ii) The phone is on the table while sitting; iii) The phone is in the pocket while standing; iv) The phone is on the table while standing; v) The phone is in the pocket while walking. (To ensure that each measurement is recorded while walking, participants were instructed not to stop while the experiment was in progress.)

The notification was randomly delayed, with a sampled interval in seconds defined by normal distribution $\mathcal{N}(\mu, 0.5)$. The value of μ was adjusted by the proctor to be between 2 and 7 seconds. (The actual values have been set to match the needs and comfort of the participant, leaving enough time to place the device on the table or in the pocket.)

Each inertial measurement consists of time series data from the physical acceleration and gyroscope sensors. (When available, measurements from the virtual sensors called "linear acceleration" and "gravitational acceleration" have also been included. The availability of these measurements depends on what interfaces are exposed in each device's API.) A time series in these collections is a sequence of quadruples (x, y, z, t) where x, y, z represent the momentary values measured by the sensor on the three axes and t denotes the relative timestamp. The measure of acceleration values is in m/s^2 and the measure of gyroscope values is in rad/s.

The resulting database contains time series data captured from 14 different smartphone users. Six of them participated in two data recording sessions. (Between the two sessions approximately one month elapsed.) We were able to record data for all five scenarios for most of the participants. In some cases, auxiliary measurements were recorded on a wrist-worn smartwatch. However, we have not evaluated that information in the experiments described below. It is however, included in the dataset which will be released following the publication of this paper.

Some of the recorded data had to be deleted as the participant either i) missed the notification; ii) started to perform the task before the notification was displayed and recording was started; iii) experienced software problems caused by the massive battery optimization of the platform.

5. Experimental Results

We have executed experiments to investigate whether the collected measurements can be used for user identity verification or not. In this section, the detailed results will be introduced, after a short description of the data preprocessing steps.

5.1. Data Preprocessing and Feature Extraction

The database contained 1595 entries after the removal of misaligned time series (caused either by a premature or missing reaction to the notification). For the experimental results presented, we used only the acceleration sensor data of the smartphone. Thus all of the time series data from the smartwatch and the gyroscope data has not been considered.

The following data preprocessing steps were applied to each time series. A basic low-pass IIR filter ($\alpha_0 = 0.8$)

has been applied on acceleration sensor measurements to remove the effect of the gravitational force, yielding a time series containing the linear acceleration measurements from the device. A band-stop Butterworth filter has been used to eliminate the noise generated by the built-in vibration motor. (The phone vibrates at 180 Hz.) High-frequency noises have been removed by a sliding window weighted moving average. (The window size was 50 samples.) In addition, we have used a Coiflet 5 wavelet with a fixed threshold [7]. Each measurement has been segmented to focus on the gesture itself. The segments have been determined by using change-point detection, which detects changes in the mean and slope of the signal [15].

The training and test sets have been assembled using the features extracted from the preprocessed data. (In accordance with the methodology described by Shen *et al*. [27].) We used calculated the following properties for each dimension for every time series: i) Statistical properties of time series data: mean, variance, standard deviation, kurtosis, skewness, root mean square; ii) Statistical properties of pairwise cross-correlation data: standard deviation, mean, variance; iii) Length of time series in milliseconds; iv) First five most significant peaks of power spectral density; v) The descriptions of the initial and final position of the device (screen facing up or down on the table; the device is upside down in the pocket, etc.). The length of every sample vector was 44 dimensions.

5.1.1 Training and Testing Datasets

We conducted experiments on the five scenarios that have been described in Section 4. We use the following abbreviations for the scenarios: SID: Sitting and the phone is laying on the desk; SIP: Sitting and having the phone in a pocket; STD: Standing and the phone is laying on the desk; STP: Standing and having the phone in pocket; WAP: Walking and storing the phone in a pocket. The different users have been assigned randomized IDs.

For the baseline closed set classification experiments, the dataset was randomly split into a training and testing set, where the fraction of test samples is 30% of the total number of instances, per user. In the case of the open set recognition experiments, the dataset is further partitioned into "known" and "unknown" classes. 50% of the samples of the target class have been assigned to the training set along with another 33% representing "known" negative samples for other class training. The remainder of the samples were used as the test set (including the classes that were not seen at training time). The openness of the problem has been calculated according to the number of the samples in these sets, using the formula of Scheirer *et al*. [26].

5.2. Closed Set SVM Classification Results

To investigate the feasibility of our hypothesis that based on the acceleration data different smartphone users can be distinguished from each other, we used a traditional SVM to classify the data. The top of Table 1 summarizes the results from experiments carried out on the entire dataset. The bottom of Table 1 summarizes the results obtained on a reduced version of the dataset. To obtain these results, we removed users from the database who had fewer than ten data entries in the database. This increased the precision by decreasing the number of false predictions caused by insufficient information during the training. As can be seen, the features contain enough information to facilitate the standard classification task.

Scenario	Accuracy	Average FAR	Average FRR
SID	85.5%	13.15%	16.25%
SIP	93.1%	8.38%	6.69%
STD	79.8%	19.00%	19.14%
STP	80.0%	24.78%	25.21%
WAP	90.1%	10.35%	12.71%
SID*	89.1%	11.09%	10.09%
SIP*	94.3%	5.72%	5.81%
STD*	84.3%	15.09%	15.18%
STP*	85.4%	14.72%	14.81%
WAP*	91.2%	10.18%	10.45%

Table 1. Averaged results of SVM classification for different scenarios. The resulting numbers suggest that it is possible to distinguish different users from each other based on the measurements of their gestures.

5.3. Open Set Recognition Results

The experiments for open set identity verification have been carried out by using the P_I-SVM [14] and the EVM [23]. These results are introduced separately.

5.3.1 P_I-SVM Results

We selected one user from the dataset and considered them as the positive class (i.e., the user that is authorized to access the device). The remaining users represent the known negative or unknown classes, in accordance with data breakdown in Section 5.1.1. This test setup has been repeated for all users, and the results have been averaged across all scenarios. Table 2 summarizes the outcomes for the entire dataset, and for the smaller subset as well. It can be observed that the data quality (the number of training samples) poses a great impact on the performance as the accuracy increases when the users with only a few measurements are excluded from the experiment. The other important observation is: although the number of false rejection is high, the method

Scenario	Accuracy	FAR	FRR
SID	49.0%	0%	51.0%
SIP	83.0%	0%	17.0%
STD	80.0%	0%	20.1%
STP	82.8%	0%	17.2%
WAP	80.3%	0%	20.7%
SID*	76.85%	0%	23.15%
SIP*	71.40%	0%	28.60%
STD*	73.14%	0%	26.86%
STP*	96.77%	0%	3.23%
WAP*	81.68%	0%	18.32%

Table 2. Results of the P_I-SVM for open set recognition. One may observe that – possibly due to the lack of enough training samples and random selection – the accuracy of specific scenarios is different than what is possible in a closed set scenario based on the SVM results.

is capable of entirely avoiding the false acceptance of other users.

The performance of the method when two authorized users are present was also investigated to better characterize the capabilities of the open set recognition approach. The training and the evaluation of the method in this case was carried out for all possible pairs of users (as positive samples) on the smaller subset of the dataset. The results in Table 3 indicate that in this case, the accuracy of the algorithm is better, compared to the single user use case. One may observe that the choice of pairs of users influences the final results, as the accuracy range is between 43.6% to 100%.

	Scen.	Avg.	Worst	Best	Std.
Accuracy	SID	89.8%	64.2%	100%	10.0%
	SIP	91.2%	75.0%	100%	8.5%
	STD	84.2%	43.7%	100%	12.1%
	STP	86.5%	68.4%	100%	9.0%
	WAP	94.2%	81.3%	100%	5.4%
FAR	Each	0%	0%	0%	0%
FFR	SID	10.2%	35.8%	100%	10.0%
	SIP	8.8%	25.0%	100%	8.5%
	STD	15.8%	56.3%	100%	12.1%
	STP	13.5%	41.6%	100%	9.0%
	WAP	5.8%	18.6%	100%	5.4%
F measure	SID	0.943	0.782	1	0.061
	SIP	0.952	0.857	1	0.048
	STD	0.909	0.608	1	0.081
	STP	0.925	0.812	1	0.053
	WAP	0.969	0.897	1	0.029

Table 3. The results of experiments with the P_I-SVM where two classes have been elected as target (to be recognized).

5.3.2 EVM results

We also conducted experiments with the EVM for the single user use case, using the smaller dataset partition. The test setup is similar to the previous one, however, the obtained results show that the EVM provides better accuracy. It is also important to note, however, that in some cases the FAR is greater than zero. A detailed breakdown of the results can be found in Table 4.

Scenario	Accuracy	FAR	FRR
SID	94.05%	0.5%	5.45%
SIP	95.72%	0%	4.28%
STD	91.27%	0%	8.73%
STP	90.52%	0.4%	9.08%
WAP	88.77%	0.2%	11.21%

Table 4. Results on the smaller subset of the dataset for the EVM. Better overall accuracy can be achieved by deploying the EVM instead of P_I-SVM. However, the false accept rate also increases, which can lead to security breaches.

6. Conclusion

In this paper, the first results from a novel open set approach for user identity verification on smartphones have been introduced. We have proposed that common, brief user gestures (such as picking up the device) contain person-specific attributes which can be a basis for the recognition of one or more users at a high level of precision. Further, the identity recognition problem is considered as an open set recognition problem. Hence we have investigated what kind of accuracy can be achieved in this setting by applying different state-of-the-art open set recognition algorithms.

In addition, we introduced a new database that has been created with measurements of five different gestures of 13 volunteered participants. We used this database to verify the feasibility of the proposed solution. Experimental results show that i) the patterns of these gestures are separable (an SVM is capable of achieving closed set classification accuracy of between $84\% - 91\%$); ii) the P_I-SVM and EVM methods can also be deployed in an open set scenario, achieving accuracy between $71\% - 91\%$.

The following questions are still open: i) what is the effect on performance as the openness of the problem grows? (i.e., how might the results change if the dataset is drastically increased?); ii) do other pattern recognition methods have comparable or better accuracy results than open set recognition methods?; iii) what are the probabilities for overlapping samples for different users? (can we estimate the theoretical limitations of this method?); iv) what are the effects of temporal or permanent behavioral changes on the recognition accuracy? In our future work, we are going to focus on these questions, hoping that the performance of

the methods can be increased so that we can move forward with implementing these techniques in the hardware of mobile devices.

Acknowledgements

This work have been supported by the Rosztoczy Foundation, the University of Notre Dame and Pázmány Péter Catholic University (KAP17 3.6 ITK and KAP18 1.1 ITK Grants). These sources of support are gratefully acknowledged.

References

[1] S. J. Alghamdi and L. A. Elrefaei. Dynamic authentication of smartphone users based on touchscreen gestures. *Arabian Journal for Science and Engineering*, 43(2):789–810, Feb 2018. 3

[2] B. W. An, S. Heo, S. Ji, F. Bien, and J.-U. Park. Transparent and flexible fingerprint sensor array with multiplexed detection of tactile pressure and skin temperature. *Nature Communications*, 9(1):2458, 2018. 2

[3] B. Attaullah, B. Crispo, S. Gupta, and F. Del Frari. Dialerauth: A motion-assisted touch-based smartphone user authentication scheme. In *Eighth ACM Conference on Data and Application Security and Privacy*, March 2018. 3

[4] A. Bendale and T. E. Boult. Towards open set deep networks. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2016. 4

[5] Bosch Sensortec GmbH. BST-BMA456-DS000-01 Datasheet, 2017. 3

[6] H. Cevikalp and B. Triggs. Efficient object detection using cascades of nearest convex model classifiers. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2012. 4

[7] D. L. Donoho. De-noising by soft-thresholding. *IEEE Transactions on Information Theory*, 41(3):613–627, May 1995. 6

[8] T. Feng, Z. Liu, K. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen. Continuous mobile authentication using touchscreen gestures. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 451–456, Nov 2012. 3

[9] T. Feng, X. Zhao, B. Carbunar, and W. Shi. Continuous mobile authentication using virtual key typing biometrics. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, July 2013. 3

[10] S. Gupta, A. Buriro, and B. Crispo. Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems*, 2018:16, 2018. 2

[11] M. Gnther, S. Cruz, E. M. Rudd, and T. E. Boult. Toward open-set face recognition. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 573–582, July 2017. 4

[12] T. Hoang, D. Choi, and T. Nguyen. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security*, 14(6):549–560, Nov 2015. 3

[13] InvenSense Inc. ICM-20690 Datasheet, 2016. 3

[14] L. P. Jain, W. J. Scheirer, and T. E. Boult. Multi-class open set recognition using probability of inclusion. In *European Conference on Computer Vision (ECCV)*, 2014. 2, 4, 6

[15] R. Killick, P. Fearnhead, and I. A. Eckley. Optimal detection of changepoints with a linear computational cost. *Journal of the American Statistical Association*, 107(500):1590–1598, 2012. 6

[16] S. Kovach. Business Insider: Samsungs Galaxy S8 facial recognition feature can be fooled with a photo, 2017. 2

[17] F. Li, N. Clarke, M. Papadaki, and P. Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3):229–244, Jun 2014. 3

[18] U. Mahbub and R. Chellappa. Path: Person authentication using trace histories. In *2016 IEEE 7th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pages 1–8, Oct 2016. 3

[19] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, 37:28 – 37, 2017. 2, 3

[20] P. Perera and V. M. Patel. Face-based multiple user active authentication on mobile devices. *IEEE Transactions on Information Forensics and Security*, 14(5):1240–1250, May 2019. 2

[21] A. Rattani, W. J. Scheirer, and A. Ross. Open set fingerprint spoof detection across novel fabrication materials. *IEEE Transactions on Information Forensics and Security*, 10(11):2447–2460, 2015. 2

[22] A. Roy, N. Memon, and A. Ross. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 12(9):2013–2025, 2017. 2

[23] E. M. Rudd, L. P. Jain, W. J. Scheirer, and T. E. Boult. The extreme value machine. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(3):762–768, March 2018. 2, 4, 6

[24] R. San-Segundo, J. D. Echeverry-Correa, C. Salamea-Palacios, S. L. Lutfi, and J. M. Pardo. I-vector analysis for gait-based person identification using smartphone inertial signals. *Pervasive and Mobile Computing*, 38:140 – 153, 2017. 3

[25] W. J. Scheirer, L. P. Jain, and T. E. Boult. Probability models for open set recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 36(11):2317–2324, Nov 2014. 4

[26] W. J. Scheirer, A. Rocha, A. Sapkota, and T. E. Boult. Towards open set recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence (T-PAMI)*, 35, July 2013. 4, 6

[27] C. Shen, Y. Li, Y. Chen, X. Guan, and R. A. Maxion. Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security*, 13(1):48–62, Jan 2018. 6

[28] J. Titcomb. The Telegraph: Hackers claim to beat iPhone X's face id in one week with 115 mask, 2017. 2