

BodyLock: Human Identity Recogniser App from Walking Activity Data

Karolis Kašys[1], Aurimas Dundulis[1], Mindaugas Vasiljevas[1], Rytis Maskeliūnas[2], and Robertas Damaševičius[1(✉)]

[1] Department of Software Engineering, Kaunas University of Technology, Kaunas, Lithuania
robertas.damasevicius@ktu.lt
[2] Department of Multimedia Engineering, Kaunas University of Technology, Kaunas, Lithuania

Abstract. A person's identity can be recognized based on his/her biometric data such as fingerprints, voice or gait. A person can also be recognized from his/her gait, which requires having sensors capable of detecting changes in speed and direction of movement. Such sensors are readily available on almost every smartphone model. We perform user identity verification using his/her walking activity data captured by smartphone sensors. To support identity verification, we have developed a mobile application for Android-based devices, which has achieved 97% accuracy of identity verification using data from acceleration, gravity and gyroscope sensors of a smartphone and a linear Support Vector Machine (SVM) classifier. The developed unobtrusive human walking analyser provides an additional active layer of protection, which may invoke a stronger authentication measure (mandatory locking) if a threat threshold is exceeded.

Keywords: Biometrics · Gait recognition · Person identification · Mobile app · Smart environment

1 Introduction

In the age of digital information, ubiquitous computing, smart devices and smart environments, the security of a person's data, devices and/or identity is a priority. To protect valuable data and to ensure that only authorized person(s) get access to user device(s) such as smartphones or tablets, a variety of techniques can be used. Password-based identification is, perhaps, the most popular now, but it suffers from eavesdropping and users avoiding the use of complex but secure passwords. As a result, the passwords have a high probability of being cracked or exposed. Moreover, passwords can be forgotten or lost. Furthermore, mobile phones secured with only a password are still vulnerable to data theft when left in an unlocked mode [1]. This is especially important for smartphone users, since smartphones are used to store personal data, emails, photos but also more and more often the commercial data, when smartphones are used in the context of BYOD (bring your own device), when users bring their own devices to workplace and utilize them for any work-related tasks such as to

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12250, pp. 307–319, 2020.
https://doi.org/10.1007/978-3-030-58802-1_23

access privileged company information and applications [2]. Therefore, it is important to prevent smartphone intrusion and theft using human biometrics [3]. Using biometrics is becoming a common and popular method of identifying individuals. Examples are fingerprints, iris, voice, face form. Each of these biometrical characteristics has its own advantages, but also disadvantages. Voice recognition requires a microphone, and cameras - to identify the shape and landmarks of the face. A high-resolution sensor is required to read the iris or fingerprints.

Biometrics is a more powerful authentication factor as compared to usual password authentication, but it still has its own disadvantages, such as non-repeatability (the same biometrical features of a user are not identical all the time) and non-revocability (it is a permanent characteristic of the user and can not be changed) [4]. A person can also be recognized from his walking behaviour characteristics (or so-called gait). Such recognition requires sensors capable of detecting changes in speed and direction of movement, i.e. accelerometer and gyroscope. Such sensors can be found on almost every smartphone model currently produced, as well as on several other devices such as smart watches. A person's identity recognition program would allow a person's authentication to allow the use of various security-enhancing systems without additional user intervention (such as passcode entry). Among the various biometric characteristics, gait has been shown to be robust to direct spoofing attacks [5].

Currently, the study of human parameters for a variety of applications, including security but also health diagnostics, is a very relevant topic for research. The examples include iris [6], voice [7], ear biometrics [8], electroencephalography (EEG) biometrics [9]. Gait (walking) is one of the most natural human biometrics. However, gait-based identification has not yet been solved yet. All biometric technologies depend on the quality of the input signal: if the received signal is weak or distorted, the task of identification becomes more difficult. The main challenge for the development of modern biometric algorithms is to overcome these complex conditions and to obtain as much reliable evidence as possible for the high level of personal identification. In addition, human gait differs from other human biometric properties, for example, fingerprints or voice, since its properties change over time due to aging. The human gait also depends on his emotional state, feeling well-being, fatigue, injuries, illnesses, environmental conditions, the type of shoes, etc. Therefore, the creation of a system based on the parameters of a human gait requires that the system continuously trace the characteristics of the human walking characteristics and continually persist in adapting to the present state of the subject.

Biometric security technology depends on the input signal quality: if the received signal is weak or distorted noise, identification task becomes more difficult. The main challenge for modern biometric algorithms to create is to overcome these difficult conditions and to extract the maximum amount of reliable evidence to pinpoint accuracy to make personal status and identity recognition possible. Moreover, human gait is different from other human biometric such as fingerprint or voice, because its properties over time can change significantly. Human gait depends on the emotional state of well-being, fatigue, injuries, diseases, environmental conditions, shoe type, etc. Therefore, developing a reliable security system based on human gait parameters requires following the human gait characteristics in real-time and constantly adapting to the changes in human condition.

Recently, the application of human gait parameters for security applications has been a subject of extensive research. For example, Cola et al. [10] used the acceleration collected at the user's wrist to learn the user's typical gait pattern, and then used anomalies detected in a set of acceleration-based features to identify a possible impostor. The method has been evaluated with 15 subjects, reaching an Equal Error Rate (EER) of 2.9%. De Marsico [11] investigated biometric identification by gait recognition via smartphone accelerometer, and achieved the EER of 7.69%. Derawi and Bours [12] collected data from five users, and constructed three different gait templates, where each template related to varying walking speeds. The phone learned the individual features at the various walk speeds, allowing the phone to recognize the correct user using the proposed Cross Dynamic Time Warping (DTW) Metric. The Correct Recognition Rate (CRR) was 89.3% and the false positive probability was as low as 1.4%. Hoang and Choi [13] proposed a gait based biometric cryptosystem to enhance smartphone user security and privacy. Gait signals were acquired by using an accelerometer sensor in the mobile device and error-correcting codes (ECC) were adopted to deal with intra-class variability of gait measurements. The results using gait samples of 34 volunteers are false acceptance rate (FAR) and false rejection rate (FRR) of 3.92% and 11.76%, respectively, in terms of key length of 50 bits. Watanabe and Sara [14] created a similar gait capture app for Android devices. They collected gait data for 15 subjects in 5 walking states. From the 3-axes accelerometer data, we they extracted 52 features with high accuracy. Nguyen et al. [15] used the signal captured in different positions of mobile phone: in front pocket and on the waist. Using Principal Component Analysis (PCA) and Support Vector Machine (SVM) allowed to achieve an EER of 2.45% and accuracy rate of 99.14% regarding the verification and identification process, respectively. Chetty et al. [16] used smartphone inertial sensor data based on information theory with feature ranking and random forest, ensemble learning and lazy learning classifiers. The best results were achieved by random forests classifier with 96.3% accuracy. Ferrero et al. [17] used the data acquired from the 3-axis accelerometer embedded in a smartphone, and provided the description of walking features in the time (statistical characteristics, moments, root means square of the walking waveform, autocorrelation, cycle rotation metric) and frequency (coefficients of Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT)) domains. Fernandez-Lopez et al. [18] implemented accelerometer-based gait recognition (ABGR) using custom gate cycle detection algorithm and achieved and an Equal Error Rate (EER) of 16.38% to 29.07%. Lai et al. [19] extracted frequency features (coefficients of FFT) from gait data obtained using the acceleration sensor and used Weighted SVM to recognize users, reaching 3.5% EER. Yuan and Zhang [20] used periodogram based gait categorization to identify patterns in the walking periodicity, and convolutional neural network (CNN) for based gait-based identification and achieving an accuracy of over 87%. Anusha and Jaidhar [21] used histogram of oriented gradients (HOG), followed by sum variance Haralick texture descriptor calculated from gradient magnitude image to derive low level features which are used for gait recognition. He et al. [22] suggested multi-task generative adversarial networks for learning view-specific gait features. Zhang et al. [23] used Convolutional Neural Network (CNN) for soft biometrics such as age and gender recognition. A review on gait-based identity recognition methods has been presented by Liu et al. [24].

Our aim is to analyse complex human gait characteristics for monitoring the state and identity of a human (smartphone user), to propose methods for selecting reliable gait features, and to develop and approve the passive user state monitoring system, running on a portable mobile device (smartphone) and allows the device to distinguish the changes in the state (condition) of the smartphone user (e.g., change of owner in case of attempted theft) according to his/her gait parameters.

Such system would be most relevant to smart device holders who want to prevent unauthorized access to smartphone data without using too cumbersome methods of security. Our approach follows the multi-layered model of security [25], which calls for different layers of security to address different security challenges. While each layer of security alone does not provide the required defence against attacks, their entirety ensures a higher level of security. Therefore, an unobtrusive human walking analyser could provide an additional active layer of protection, which could invoke a stronger authentication measure (mandatory locking) if a threat threshold is exceeded.

We propose and validate a passive user authentication system that operates on a portable mobile device (smartphone) and allows the device owner to be distinguished from an outsider by its track parameters. Upon detecting a changed owner, the system will take appropriate security measures to ensure the security of the data stored on the device (e.g., blocking access to data, informing the owner about the location of the device, etc.) without waiting for active intruder attempts to connect to the device.

2 Method and Tools

2.1 Overview

In this paper, the following methodology is applied: data acquisition from smartphone sensors; data preprocessing and denoising; feature generation, feature ranking and dimensionality reduction, activity detection and gait model construction. The identification of a subject is performed by comparing the current gait characteristics of a subject with his gait model learned from previous observations during the training stage. The methodology is visualized in Fig. 1.

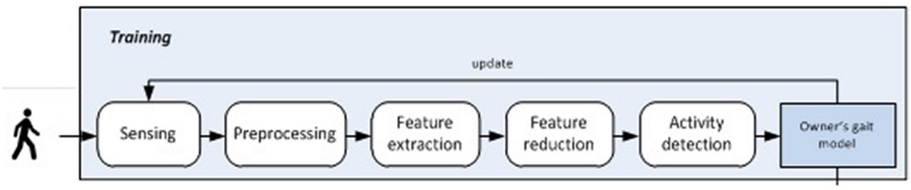


Fig. 1. Overview of the method stages

2.2 Data Acquisition

During data acquisition, the smartphone is kept in a static position - the phone can be located either in the trouser pocket or in the jacket pocket (chest level), which however affects the collected data, even if the same type of activity is performed. In order to avoid this problem, the smartphone needs to be kept in the same constant position with regards to the human body. The raw data provided by the smart phone is accelerometer and gyro data, since these sensors are equipped with most smart devices, but other sensors, for example, will also be taken, if possible, e.g., the magnetic field sensor data, if it helps to more accurately identify identity, but more data does not always mean more accurate results because their information is not relevant.

We have selected gait data in 3 states of walking: State 1 (walking forwards): walking on an even surface and holding the smartphone. State 2 (walking stairs up): going stairs up and holding the smartphone in the pocket. State 3 (walking stairs down): going downstairs and holding the smartphone in the pocket.

The following data set is logged by the developed Android application: Logged time (ms); Raw 3 axes of acceleration data (m/s^2); Raw 3 axes of gravity data (m/s^2); Raw 3 axes of the gyroscope data (rad/s).

2.3 Primary Data Processing

When the data is collected, the primary data processing is carried out - the data is normalized. Removing noise can help increase the accuracy of the results by eliminating unnecessary noisy data, bat also the important information characterising differences between individuals may be smoothed, therefore, the denoising has not been used. A common problem was that the sensor data returned by the device is not acquired at regular time intervals. In that case, a linear time interpolation was used to ensure the equal time interval between two data records.

Another problem was the removal of spikes from the data. The cause for these spikes remained unclear and may be related to phone's hardware behaviour. We have identified the spikes as outliers, which are more than 4 standard deviations (sigmas) away from the signal's mean value, thus guaranteeing that less than 0.1% of data is removed and replaced by the mean of the adjacent values.

2.4 Feature Calculation

In many cases (such as calculation of a mean or a moving average), calculation requires using sliding windows over sensor data. For sliding window, following the suggestion of Primo et al. [26], we use the sliding window of 100 data points with overlap of 50%. As features, we use a set of statistical and other signal features described in [27, 28]. The full list involves 102 different features. Some of the sample features are presented in Table 1.

Table 1. Representative features of smartphone sensor signals

Feature number	Description	Equation (notation)
4–6	Acceleration (x-, y-, and z-axes)	a_x, a_y, a_z
7–9	Gyroscope (x-, y-, and z-axes)	g_x, g_y, g_z
10–15	Moving variance of 100 samples of acceleration and gyroscope data	$\mathrm{var} = \frac{1}{N(N-1)}\left(N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2\right)$, here $x = a_x, a_y, a_z, g_x, g_y, g_z$
16-17	Movement intensity of acceleration and gyroscope data	$\mathrm{MI}_a = \sqrt{a_x^2 + a_y^2 + a_z^2}$ $\mathrm{MI}_g = \sqrt{g_x^2 + g_y^2 + g_z^2}$
18	Movement intensity of difference between acceleration and gyroscope data	$\mathrm{MI}_{ga} = \sqrt{(g_x - a_x)^2 + (g_y - a_y)^2 + (g_y - a_y)^2}$
19–21	Moving variance of 100 samples of movement intensity data	$\mathrm{var} = \frac{1}{N(N-1)}\left(N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2\right)$, here $x = \mathrm{MI}_a, \mathrm{MI}_g, \mathrm{MI}_{ga}$
22–24	Polar coordinates of acceleration data	$\varphi_a = \arctan(a_y, a_x)$, $r_a = \sqrt{a_x^2 + a_y^2}$, $z_a = a_z$
25–27	Polar coordinates of gyroscope data	$\varphi_g = \arctan(g_y, g_x)$, $r_g = \sqrt{g_x^2 + g_y^2}$, $z_g = g_z$
28–30	Polar coordinates of difference between acceleration and gyroscope data	$\varphi_{ag} = \arctan(a_y - g_y, a_x - g_x)$, $r_{ag} = \sqrt{(a_y - g_y)^2 + (a_x - g_x)^2}$, $z_{ag} = a_z - g_z$

2.5 Classification

For classification we use Support Vector Machine (SVM) [29] with a linear kernel. 80% of data is retained from training and 20% of data is used for testing. The procedure is repeated 20 times using Hold-Out cross-validation, and the results are evaluated using the accuracy, Kappa and F-score metrics. Accuracy is the number of correct guesses made divided by the total number of guesses made. Kappa value compares an observed accuracy with an expected accuracy (random guessing). F-score combines

precision and recall, and it characterises the precision (how many samples it classifies correctly) and robustness (it does not miss many positive samples) of the classifier.

3 Implementation and Results

3.1 BodyLock App

The human identity recognizer has been implemented as Android app, called BodyLock. The app has two parts (see Fig. 2): the device part is responsible for collection of sensor data, generation of features, sending of data to server, and user interface. The server part is responsible for storage of data and classification of walking features. The application itself works silently in the background mode.

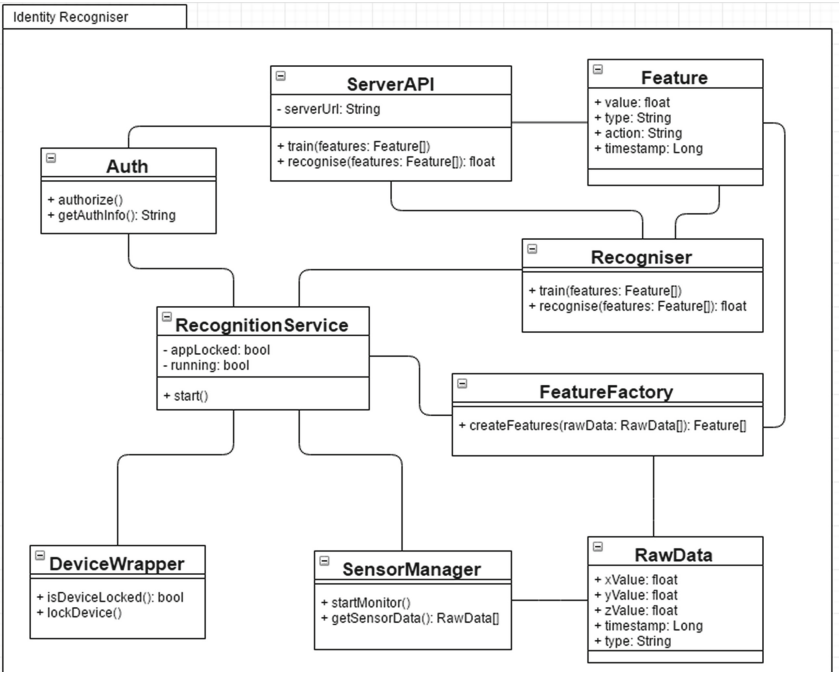


Fig. 2. Class diagram of the BodyLock application

3.2 Data Collection Environment

For our experiments we used walking trajectories of 13 different subjects collected in the office environment (in the SANTAKA valley building of Kaunas University of Technology), which included three different types of trajectories: walking forward, walking upstairs and walking downstairs. All individuals were health without any foot

problems. All subjects took the same walking trajectory using a flat-surface corridor about 50 m long, as well as up-stair and down-stairs (see Fig. 3).

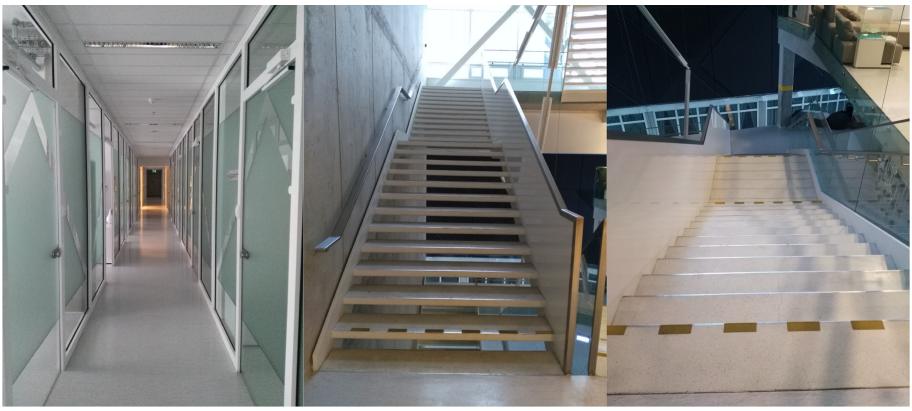


Fig. 3. Environment of data collection: walking forward (left), walking upstairs (middle), and walking downstairs (right)

The even floor of the corridor allowed to capture the usual gait characteristics of the subjects without any obstacles or unevenness of the floor. The data capture sessions were organized during the first half of the day to avoid the effect of tiredness, exhaustion at the end of a business day, or office fatigue due to sitting all day.

3.3 Results

The results of feature ranking are presented in Fig. 4. The most important features refer to the 95th and 99th percentiles of acceleration in the X and Z axes of the device, which means that extreme events such as the speed of sudden movements help to recognize people and differentiate one subject from another.

An example of the distribution of sample data is presented in Fig. 5. Here the 2D feature space is formed by only two features (axz_p95, the 95th percentile of acceleration sensor value and in the X-Z axis, and ry_75, the 75th percentile of gyroscope sensor value in the Z axis). Even in this low-dimensional feature space, the gait characteristics of subjects can be clearly separated.

Figure 6 shows the confusion matrix of the classification results.

Finally, Fig. 7 shows the classification results. We have achieved 97% accuracy of correct identification, while the Copen's kappa was 0.944, and F-score was 94%.

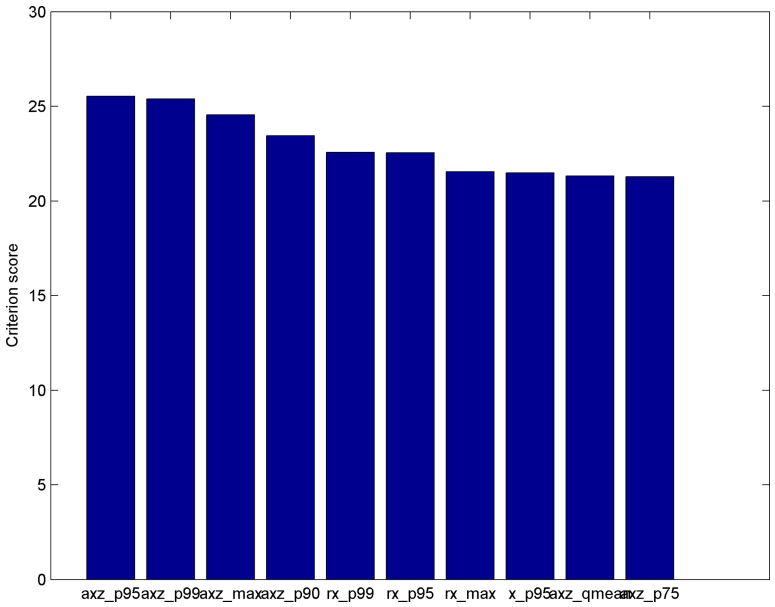


Fig. 4. Results of feature ranking (left) and distribution of data according in feature space of two top ranked features

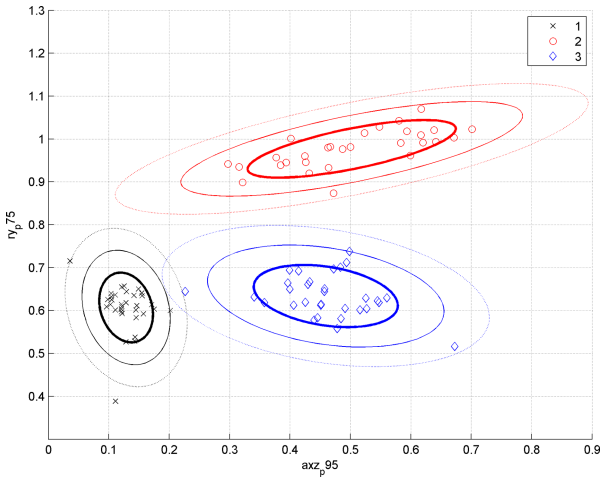


Fig. 5. Results of feature ranking (left) and distribution of data according in feature space of two top ranked features

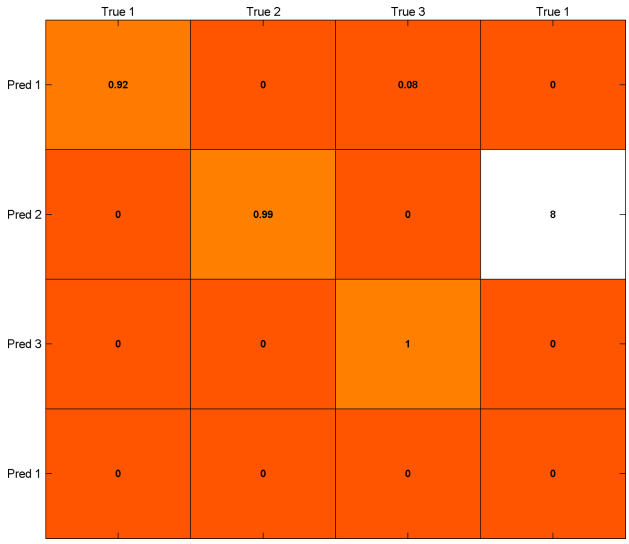


Fig. 6. Classification results: confusion matrix (left) and performance measures (right)

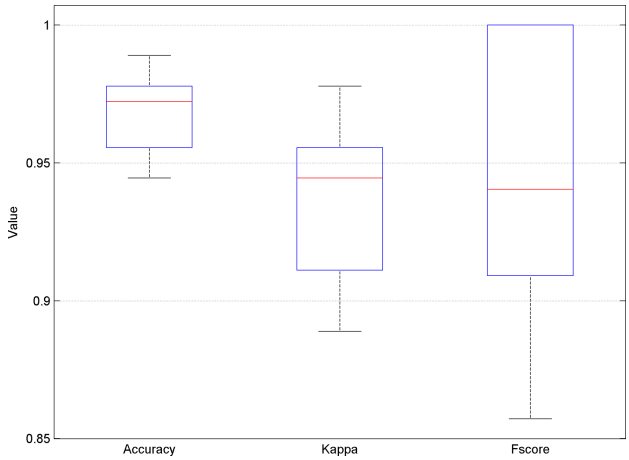


Fig. 7. Classification results: confusion matrix (left) and performance measures (right)

3.4 Evaluation

The limitations of the presented approach towards user identification are as follows:

1) Contamination of data with noise, which may lead to incorrect identification of user. Some lower-end smartphone models have low-quality sensors, which return unreliable data, which can be observed practically by high variability of a sensor signal even if the phone is laying in the static position without any movement.

2) Significant intra-class variability due to changing condition of the subject (e.g., illness, fatigue or stress [30, 31] may influence his/her gait), different shoes and clothes, different environment and flooring conditions (e.g., field environment can vary from solid pavement to grass, sand or snow).
3) Discriminability – the interclass similarities may be large if the sufficiently large number of subjects is explored, thus restricting the discriminability provided by the gait analyser.

One of the key challenges is determining how to achieve required functionality and performance without jeopardizing the user experience and power consumption with the overhead of additional computational burden to the mobile phone. The two-tiered (client-server) approach used in the design of the BodyLock app allowed to move computationally costly operations to the server, thus reducing the performance overhead. However, the data still must be secured during transfer and storage at the cloud server to avoid stealing and impersonation attempts. Gait verification might not reach the same level of reliability as fingerprint or iris recognition. However, it still could be used as a method of continuous (active) authentication for accessing less sensitive content on a smartphone (such as games) or be used in concert with other biometrics (e.g. iris recognition) to provide a more reliable user authentication method.

When combined with other signals such as GPS or WiFi from low energy Bluetooth beacons, it could be used for providing smart localisation [32, 33] services as well.

4 Conclusion

Biometric authentication is a good solution for smartphone users since it relies on the uniqueness of certain physical traits in humans. By continuously and unobtrusively recognizing the phone's owner, the human walking analyser has potential to improve user authentication on the go. Here we described the development of a mobile app for Android-based smartphones, which performs user identity verification using his/her walking activity data. We have achieved 97% accuracy of identity verification using features generated from data acquired from the acceleration, gravity and gyroscope sensors of a smartphone and a linear Support Vector Machine (SVM) classifier. The results achieved are in line with the results achieved by other authors working in the same area of research. As gait-based authentication technologies move towards being deployed as an extra security layer in portable mobile devices, our work represents a step in this direction.

References

1. Crouse, D., Han, H., Chandra, D., Barbello, B., Jain, A.K.: Continuous authentication of mobile user: fusion of face image and inertial measurement unit data. In: International Conference on Biometrics, ICB 2015, pp. 135–142 (2015). https://doi.org/10.1109/ICB.2015.7139043

2. Keith, W.M., Jeffrey, M.V., George, F.H.: BYOD: security and privacy considerations. IT Prof. **14**(5), 53–55 (2012)
3. Ohana, D.J., Phillips, L., Chen, L.: Preventing cell phone intrusion and theft using biometrics. In: IEEE CS Security and Privacy Workshops, SPW 2013, pp. 173–180 (2013). https://doi.org/10.1109/SPW.2013.19
4. Gunasinghe, H., Bertino, E.: PrivBioMTAuth: privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. IEEE Trans. Inf. Forensics Secur. **13**(4), 1042–1057 (2018). https://doi.org/10.1109/TIFS.2017.2777787
5. Hadid, A., Evans, N., Marcel, S., Fierrez, J.: Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process. Mag. **32**, 20–30 (2015). https://doi.org/10.1109/MSP.2015.2437652
6. Sholokhov, A., Kinnunen, T., Vestman, V., Lee, K. A.: Voice biometrics security: extrapolating false alarm rate via hierarchical bayesian modeling of speaker verification scores. Comput. Speech Lang. **60** (2020). https://doi.org/10.1016/j.csl.2019.101024
7. Wang, K., Kumar, A.: Cross-spectral iris recognition using CNN and supervised discrete hashing. Pattern Recogn. **86**, 85–98 (2019). https://doi.org/10.1016/j.patcog.2018.08.010
8. Olanrewaju, L., Oyebiyi, O., Misra, S., Maskeliunas, R., Damasevicius, R.: Secure ear biometrics using circular kernel principal component analysis, Chebyshev transform hashing and Bose–Chaudhuri–Hocquenghem error-correcting codes. Signal Image Video Process. (2020). https://doi.org/10.1007/s11760-019-01609-y
9. Damaševičius, R., Maskeliunas, R., Kazanavičius, E., Woźniak, M.: Combining cryptography with EEG biometrics. Comput. Intell. Neurosci. **2018** (2018). https://doi.org/10.1155/2018/1867548
10. Cola, G., Avvenuti, M., Musso, F., Vecchio, A.: Gait-based authentication using a wrist-worn device. In: ACM International Conference Proceeding Series, pp. 208–217 (2016). https://doi.org/10.1145/2994374.2994393
11. Marsico, M.D., Mecca, A.: Biometric walk recognizer. Multimed. Tools Appl. **76**(4), 4713–4745 (2016). https://doi.org/10.1007/s11042-016-3654-1
12. Derawi, M., Bours, P.: Gait and activity recognition using commercial phones. Comput. Secur. **39**(PART B), 137–144 (2013). https://doi.org/10.1016/j.cose.2013.07.004
13. Hoang, T., Choi, D.: Secure and privacy enhanced gait authentication on smart phone. Sci. World J. **2014** (2014). https://doi.org/10.1155/2014/438254. Article ID 438254, 8 p.
14. Watanabe, Y., Sara, S.: Toward an immunity-based gait recognition on smart phone: a study of feature selection and walking state classification. Procedia Comput. Sci. **96**, 1790–1800 (2016). https://doi.org/10.1016/j.procs.2016.08.228
15. Nguyen, H., Nguyen, H.H., Hoang, T., Choi, D., Nguyen, T.D.: A generalized authentication scheme for mobile phones using gait signals. In: Obaidat, M.S., Lorenz, P. (eds.) ICETE 2015. CCIS, vol. 585, pp. 386–407. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-30222-5_18
16. Chetty, G., White, M., Akther, F.: Smart phone based data mining for human activity recognition. Procedia Comput. Sci. **46**, 1181–1187 (2015). https://doi.org/10.1016/j.procs.2015.01.031
17. Ferrero, R., Gandino, F., Montrucchio, B., Rebaudengo, M., Velasco, A., Benkhelifa, I.: On gait recognition with smartphone accelerometer. In: 4th Mediterranean Conference on Embedded Computing, MECO 2015, pp. 368–373 (2015). https://doi.org/10.1109/MECO.2015.7181946
18. Fernandez-Lopez, P., Liu-Jimenez, J., Sanchez-Redondo, C., Sanchez-Reillo, R.: Gait recognition using smartphone. In: International Carnahan Conference on Security Technology, pp. 1–7 (2016). https://doi.org/10.1109/CCST.2016.7815698

19. Lai, Q., Chen, B., Xu, C.: Using weighted SVM for identifying user from gait with smart phone. In: 7th International Conference on Cloud Computing and Big Data, CCBD 2016, pp. 41–45 (2017). https://doi.org/10.1109/CCBD.2016.019
20. Yuan, W., Zhang, L.: Gait classification and identity authentication using CNN. In: Li, L., Hasegawa, K., Tanaka, S. (eds.) AsiaSim 2018. CCIS, vol. 946, pp. 119–128. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-2853-4_10
21. Anusha, R., Jaidhar, C.D.: Human gait recognition based on histogram of oriented gradients and Haralick texture descriptor. Multimed. Tools Appl. (2020). https://doi.org/10.1007/s11042-019-08469-1
22. He, Y., Zhang, J., Shan, H., Wang, L.: Multi-task GANs for view-specific feature learning in gait recognition. IEEE Trans. Inf. Forensics Secur. **14**(1), 102–113 (2019). https://doi.org/10.1109/TIFS.2018.2844819
23. Zhang, Y., Huang, Y., Wang, L., Yu, S.: A comprehensive study on gait biometrics using a joint CNN-based method. Pattern Recogn. **93**, 228–236 (2019). https://doi.org/10.1016/j.patcog.2019.04.023
24. Liu, C., Zhao, J., Wei, Z.: A review of gait behavior recognition methods based on wearable devices. In: Xie, Y., Zhang, A., Liu, H., Feng, L. (eds.) GSES 2018. CCIS, vol. 980, pp. 134–145. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-7025-0_14
25. Denman, S.: Why multi-layered security is still the best defence. Network Security, 5–7 (2012)
26. Primo, A., Phoha, V.V., Kumar, R., Serwadda, A.: Context-Aware active authentication using smartphone accelerometer measurements. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, pp. 98–105 (2014). https://doi.org/10.1109/CVPRW.2014.20
27. Damasevicius, R., Vasiljevas, M., Salkevicius, J., Wozniak, M.: Human activity recognition in AAL environments using random projections. Comput. Math. Methods Med. **2016**, 1–17 (2016). https://doi.org/10.1155/2016/4073584
28. Damasevicius, R., Maskeliunas, R., Venckauskas, A., Wozniak, M.: Smartphone user identity verification using gait characteristics. Symmetry **8**(10), 100 (2016). https://doi.org/10.3390/sym8100100
29. Cortes, C., Vapnik, V.: Support vector networks. Mach. Learn. **20**, 273–297 (1995)
30. Raudonis, V., Maskeliūnas, R., Stankevičius, K., Damaševičius, R.: Gender, age, colour, position and stress: how they influence attention at workplace? In: Gervasi, O., et al. (eds.) ICCSA 2017. LNCS, vol. 10408, pp. 248–264. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-62404-4_19
31. Ulinskas, M., Damaševičius, R., Maskeliunas, R., Woźniak, M.: Recognition of human daytime fatigue using keystroke data. Procedia Comput. Sci. **130**, 947–952 (2018). https://doi.org/10.1016/j.procs.2018.04.094
32. Al-Madani, B., Orujov, F., Maskeliūnas, R., Damaševičius, R., Venčkauskas, A.: Fuzzy logic type-2 based wireless indoor localization system for navigation of visually impaired people in buildings. Sensors **19**(9) (2019). https://doi.org/10.3390/s19092114
33. Orujov, F., Maskeliūnas, R., Damaševičius, R., Wei, W., Li, Y.: Smartphone based intelligent indoor positioning using fuzzy logic. Future Gener. Comput. Syst. **89**, 335–348 (2018). https://doi.org/10.1016/j.future.2018.06.030