Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 177 (2020) 8–15

Procedia Computer Science

www.elsevier.com/locate/procedia

The 11th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2020)
November 2-5, 2020, Madeira, Portugal

Identifying Users with Wearable Sensors based on Activity Patterns

Muhammad Ehatisham-ul-Haq[a], Maryam Naseer Malik[a], Muhammad Awais Azam[b], Usman Naeem[c,*], Asra Khalid[d], and Mustansar Ali Ghazanfar[e]

[a]*Department of Computer Engineering, University of Engineering and Technology, Taxila, Punjab, 47050, Pakistan*
[b]*Whitecliffe Technologies, Wellington, New Zealand*
[c]*School of Electronic Engineering and Computer Science, Queen Mary University of London, United Kingdom*
[d]*School of Engineering & Computer Science, Victoria University of Wellington, New Zealand*
[e]*School of Architecture, Computing and Engineering, University of East London, United Kingdom*

Abstract

We live in a world where ubiquitous systems surround us in the form of automated homes, smart appliances and wearable devices. These ubiquitous systems not only enhance productivity but can also provide assistance given a variety of different scenarios. However, these systems are vulnerable to the risk of unauthorized access, hence the ability to authenticate the end-user seamlessly and securely is important. This paper presents an approach for user identification given the physical activity patterns captured using on-body wearable sensors, such as accelerometer, gyroscope, and magnetometer. Three machine learning classifiers have been used to discover the activity patterns of users given the data captured from wearable sensors. The recognition results prove that the proposed scheme can effectively recognize a user's identity based on his/her daily living physical activity patterns.

Keywords: Activity recognition; machine learning; user identification; wearable sensors;

* Usman Naeem. Tel.: +44-7882-6171.
E-mail address: u.naeem@qmul.ac.uk

10.1016/j.procs.2020.10.005

1. Introduction

With the advancement in networking and sensing capabilities, the Internet of Things (IoT) has gained much attention from academic and industrial research. IoT allows people to connect anywhere at any time, thus showing great potential in technologies such as smart appliances, automated home, e-health and wearable devices. However, these applications are vulnerable to the possible risk of unauthorized access. Authentication is the most common mechanism used for the prevention of unauthorized access to resources. It is the process of recognizing the identity of a user and granting/refusing access to a particular resource/service [1]. Generally, the authentication consists of factors that can be categorized as "something you know" (e.g. passwords, PIN), "something you have" (e.g. card, token), and "something you are (e.g. biometrics; psychological or behavioral)" [2]. The traditional authentication techniques include personal identification numbers (PINs) and passwords that can be used to access electronic locks, online accounts, smart devices, and computer systems [3]. Although these are widely used authentication mechanisms, they are weak and thus vulnerable to guessing attacks [4, 5]. To avoid the limitations associated with passwords, USB tokens and hardware keys were adopted broadly as a *second-factor* authentication to enhance security [6]. However, the major drawback with these is that they pose a risk of being lost or misplaced. Biometric verification schemes have also been employed for authentication. Typical applications of this include user identification to provide access to a computer system, room (e.g., biometric attendance), transportation, and healthcare by introducing *fingerprints*, *iris*, and *face recognition* techniques. However, these methods can be insecure as they are susceptible to *spoofing* attacks. Moreover, most of these common authentication mechanisms are based on the one-time manner, i.e., once a user is granted access, he/she could be considered as an authenticated user for a long period without any re-verification.

Increased capability within sensors and machine learning algorithms paves the way for robust solutions being explored for addressing authentication challenges. In the last decade, wearable devices have escalated and have been adopted widely. It is expected that wearable devices sale will reach 100 million by 2020 [7]. Wearable sensors are attached to the body unobtrusively and can continuously authenticate users based on their behavioral biometrics [15]. Behavioral biometrics aims to identify the behavioral characteristics that a user possesses, such as touchscreen interactions, hand movements, gait patterns, and wave patterns. By nature, wearable sensors are always attached to the user's body, thus providing ubiquitous authentication of the person with a wearable device [8]. Therefore, in this research, we utilize wearable on-body sensors for passive and continuous authentication of the users by analyzing their physical activity patterns. The objective of our work is to learn the activity patterns of a user for distinguishing him/her from other users. For this purpose, we choose eight (08) different activities of daily life for user identification. These activities included *walking*, *nordic walking*, *running*, *walking upstairs*, *walking downstairs*, *sitting*, *standing*, and *lying*. We have used a public domain dataset PAMAP2 [9] for experiments and evaluation, which contains data of three Inertial Measurement Units (IMU) (consisting of *accelerometer*, *gyroscope*, and *magnetometer*) for three different body positions including *ankle*, *chest*, and *hand*. After preprocessing the raw data and extracting features, we have applied three machine learning classifiers, i.e., Support Vector Machine, Decision Tree, and Random Forest for user identification based on the activity data. We provide a detailed performance analysis of these classifiers and compared their performance for user recognition. Besides, we have also examined the impact of sensor positioning on the user's body and provide empirical evidence of how variation in sensor position affects the user recognition accuracy.

The remaining paper is organized as follows: Section 2 describes the related work, whereas Section 3 presents the proposed methodology in detail. Section 4 presents and discusses the experimental results. Finally, Section 5 concludes the findings of this research work.

2. Related Works

In recent years, continuous user authentication has gained popularity amongst the research community, which is due to the exponential growth in mobile devices being used to store sensitive data. Several authors have proposed different schemes to identify a user in real-time systems for *human-computer interaction* [10] and surveillance [11].

Biometrics features such as facial [12] and gait recognition [13] have also been explored. Nguyen and Sigg [14] proposed an authentication mechanism by retrieving conceited video recorded using wearable cameras. Video cameras provide ease for retrieving visual information through the environment. However, vision-based technologies have a drawback as they can infringe on user privacy, which limits their use at every place.

Motion sensors have been widely used for Human Activity Recognition (HAR), however, research based on authentication using motion sensors is comparatively new. Smartphones have a range of embedded motion sensors, which have also been used for authentication purposes. For example, the authors in [15] used built-in sensors of a smartphone for user authentication based on their physical activity patterns. Shen et al. [16] used smartphone sensors, i.e., accelerometer and orientation sensor, to authenticate a user based on the actions performed while entering the passcode as an input. Conti et al. [17] proposed an authentication scheme, which considered the movement of users when they answered a phone call. However, there are some limitations associated with these smartphone-based authentication schemes as smartphones are orientation and position-sensitive, which can lead to false positives. Moreover, in practice, there are limited body positions where the smartphone can be placed.

Xu et al. [18] used face recognition and smart glasses composed of the camera as well as inertial sensors to recognize a user. The recognition accuracy improved up to 15% by utilizing angle information through inertial sensors. Zhang et al. [19] used gait recognition for identification using a multiscale signature points extraction scheme that achieved the recognition accuracy of 95.8% using five accelerometers placed at different body positions. Zeng et al. [20] used dynamic behavior as a unique entity of users to propose an authentication framework using wearable devices. Since every user has a specific activity pattern, they constructed an activity specification model to differentiate between the different activities based on the different placement positions of the sensors. These experimental results showed a false positive rate of 0.3% in the case of correct detection of walking. Blasco et al. [21] designed a biometric system using wearable sensors composed of acceleration, photoplethysmogram, electrocardiogram, and galvanic skin response sensors. Their results showed an equal error rate of 0.02 with one minute of training data. Wu et al. [22] presented a two-step authentication scheme based on a wearable sensor, which captured the user's motion data and physiological signals at the same time. Their results achieved the average accuracy of 98.5%. To summarise, wearable sensors have great potential in authenticating the identity of a user. Considering the benefits of wearable sensors over built-in smartphone sensors, it can be seen as an encouraging alternative for user identification. Thus, this study presents an approach for user identification based on wearable sensors.

3. Proposed Method

The proposed methodology for user identification is based on the activity patterns recognised from the data captured by wearable sensors. Fig. 1 shows the basic steps involved in the proposed methodology.

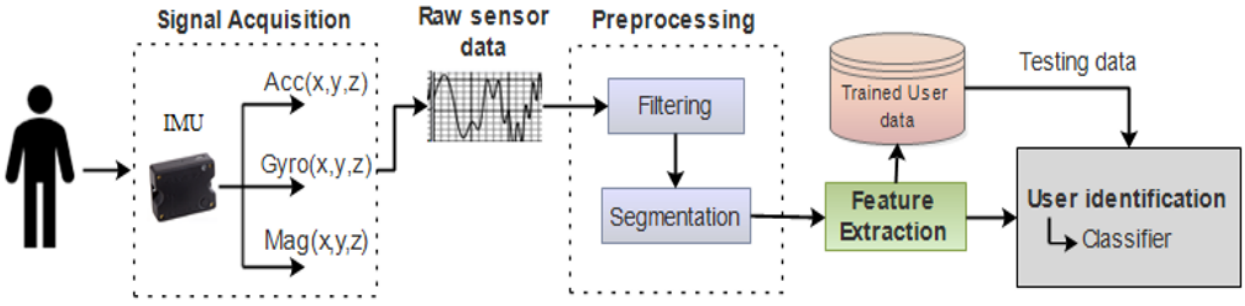

Fig. 1. Proposed methodology for user identification based on wearable sensors

3.1. Data Acquisition

To evaluate our experimental study, an existing dataset for physical activity monitoring was utilized. The PAMAP2 dataset [9] is based on on-body wearable sensors and collected using four sensors: three inertial sensors (accelerometer, gyroscope, and magnetometer) and one heart rate monitoring sensor. The data was collected at a sampling rate of 100 Hz. Nine subjects, one female and eight males, took part in the data collection experiments for eighteen different physical activities. From all these activities, we selected eight commonly occurring activities of daily living in our study for user identification. These activities included *walking*, *running*, *nordic walking*, *walking upstairs*, *walking downstairs*, *sitting*, *standing*, and *lying*. We used inertial sensor data to recognize the participants based on these eight activities.

3.2. Preprocessing: Filtering and Segmentation

The raw data from IMU sensors contained system measurement noise, or noise due to the vivacious motion of the participant, which corrupted the signal. To reduce the effect of the noise, we employed a *median* filter on the acquired data. The filtered data was continuous and inappropriate for feature extraction, so the segmentation of data was required. Each signal was divided into equal-sized segments of 10 seconds in time.

3.3. Feature Extraction

The objective of this stage was to choose suitable features that give efficient recognition performance. So, fourteen different time and frequency domain features were extracted for each segment of data. The detail of the selected features is listed in Table 1, where each feature gave a single output value except autoregression that is of size [1×4]. So, the overall size of the final feature vector obtained was [1×153] as the features are computed on all three dimensions of the sensor data.

Table 1. Time and frequency domain features for user identification

Category	Features	Formula
Time-domain	Arithmetic mean	$\bar{s} = \frac{1}{N}\sum_{i=1}^{N} s_i$
	Minimum amplitude	$s_{max} = \max(s_i)$
	Maximum amplitude	$s_{min} = \min(s_i)$
	Kurtosis	$E[(s-\bar{s})^4]/E[(s-\bar{s})^2]^2$
	Skewness	$E\left[\left(\frac{s-\bar{s}}{\sigma}\right)^3\right]$
	Signal magnitude area	$\frac{1}{3}\sum_{i=1}^{3}\sum_{j=1}^{N}\lvert s_{i,j}\rvert$
	Standard deviation	$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(s-\bar{s})^2}$
	Median absolute deviation	$median_i\left(\lvert s_i - median_{j(s_j)}\rvert\right)$
	Autoregression	$a = arburg(s,4), a\epsilon \mathrm{R}^4$
	Interquartile range	$Q3(s) - Q1(s)$
Frequency-domain	Maximum frequency index	$arg\ max_i(s_i)$
	Mean frequency	$\sum_{i=1}^{N}(is_i)/\sum_{j=1}^{N} s_j$
	Energy	$\frac{1}{N}\sum_{i=1}^{N} s_i^2$
	Entropy	$\sum_{i=1}^{N} c_i(\log(c_i)), c_i = s_i/\sum_{j=1}^{N} s_j$

3.4. User Identification

The final step in the proposed methodology was identifying a user based on his/her physical activity patterns. For this purpose, we used three supervised machine learning classifiers: Support Vector Machine (SVM), Decision Tree (DT), and Random Forest (RF). The classifiers were selected due to their efficient performance in state-of-the-art studies. A comparison has been made among the performance of these classifiers in user recognition.

4. Experimental Results

To achieve continuous authentication, user identification was performed by learning the activity patterns of each user using SVM, DT, and RF classifier. The activity patterns for each user were trained and tested separately for three different sensor positions using a 10-fold cross-validation scheme. The evaluation metrics used to evaluate the performance of the proposed scheme are shown in Table 2.

Table 2. Evaluation metrics to assess the classification performance for user identification

Metric	Formula
Accuracy	$A = \frac{T_p + T_n}{T_p + T_n + F_p + F_n}$
Precision	$P = \frac{T_p}{T_p + F_p}$
Recall	$R = \frac{T_p}{T_p + F_n}$
F-Measure	$F1 = 2\left(\frac{P.R}{P + R}\right)$

Tables 3 shows the performance of the classifiers in recognizing the users for three sensor positions based on eight different physical activities. It can be seen from the table that the classification accuracy of SVM and RF classifiers was almost similar for user identification, which is higher than DT. Based on the walking activity, the users are best identified when the sensors are placed at ankle. In this case, the recognition accuracies obtained by SVM and RF were 98.2 and 97.4 respectively. The worst accuracy achieved by RF and SVM is 85.4% and 79.5% respectively for the case of *standing* activity with sensors placed at hand. The classification results also depict the effect of sensors placement at different body positions for user identification. The results demonstrate that the ankle was the best position to show discrimination among users, and it provided maximum accuracy in recognizing users based on all selected activities. Sensor placement at the *chest* and *hand* positions provided satisfactory results for user recognition based on *nordic walking*, *running*, walking, and *lying* activities. For the other four activities, placing sensors at *hand* position did not accurately recognize all the users due to the intricate patterns of hands' movement. SVM achieved an overall accuracy of 82.3%, 87.1%, 80.6%, and 79.5% in recognizing when the sensors were placed at hand position in the case of *walking upstairs*, *walking downstairs*, *sitting*, and *standing* activities respectively. *Sitting* and *standing* activities shows low results because of the static nature of these activities.

Fig. 2 shows the average accuracy achieved for RF, SVM, and DT classifier in identifying users based on different activities performed by the user. The average accuracy of a classifier was calculated by taking the mean of accuracy values obtained for all three positions for a single activity. For all the activities, the best average accuracy for user identification was achieved by RF classifier. The performance of RF classifier was identical to SVM based on *walking*, *running*, *nordic walking*, *lying*, and *walking downstairs* activities. For *sitting* and *standing* activities, where the performance accuracy of SVM was reduced, RF performed better than SVM. However, DT classifier showed lower performance than SVM and RF in recognizing users for all activities. The overall average accuracy rate achieved by RF classifier was 92.68%, which is 0.33% and 7.89% higher than the overall average accuracy rate obtained by SVM and DT classifiers. So, RF classifier shows better user recognition accuracy than SVM and DT classifiers due to its feature selection ability and stability.

Table 3. Performance evaluation of user identification based on different activities

User Identification based on 'Walking' Activity						User Identification based on 'Walking Upstairs' Activity					
Body Position	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**	**Body Position**	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**
Hand	94.89	0.951	0.949	0.949	94.89	Hand	SVM	82.30	0.827	0.823	0.822
	88.08	0.882	0.881	0.881	88.08		DT	60.17	0.633	0.602	0.605
	93.61	0.943	0.936	0.938	93.61		RF	82.30	0.828	0.823	0.822
Chest	97.02	0.972	0.970	0.970	97.02	Chest	SVM	93.80	0.942	0.938	0.939
	92.76	0.928	0.928	0.927	92.76		DT	81.41	0.815	0.814	0.813
	97.02	0.972	0.970	0.970	97.02		RF	92.92	0.937	0.929	0.929
Ankle	98.29	0.984	0.983	0.983	98.29	Ankle	SVM	93.80	0.942	0.938	0.939
	94.89	0.952	0.949	0.949	94.89		DT	77.87	0.778	0.779	0.773
	97.44	0.976	0.974	0.975	97.44		RF	92.92	0.931	0.929	0.928
User Identification based on 'Walking Downstairs' Activity						**User Identification based on 'Running' Activity**					
Body Position	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**	**Body Position**	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**
Hand	SVM	87.12	0.873	0.871	0.870	Hand	SVM	95.78	0.958	0.958	0.958
	DT	66.33	0.673	0.663	0.667		DT	93.68	0.940	0.937	0.937
	RF	84.15	0.852	0.842	0.843		RF	95.78	0.958	0.958	0.958
Chest	SVM	90.09	0.903	0.901	0.901	Chest	SVM	95.78	0.958	0.958	0.958
	DT	72.27	0.729	0.723	0.725		DT	93.68	0.940	0.937	0.937
	RF	86.13	0.865	0.861	0.858		RF	95.78	0.958	0.958	0.958
Ankle	SVM	97.02	0.972	0.970	0.970	Ankle	SVM	97.89	0.980	0.979	0.978
	DT	78.21	0.785	0.776	0.749		DT	90.52	0.907	0.905	0.903
	RF	91.08	0.917	0.911	0.910		RF	96.84	0.965	0.968	0.966
User Identification based on 'Nordic Walking' Activity						**User Identification based on 'Sitting' Activity**					
Body Position	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**	**Body Position**	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**
Hand	SVM	98.36	0.985	0.984	0.984	Hand	SVM	80.66	0.806	0.807	0.805
	DT	90.21	0.904	0.902	0.902		DT	79.55	0.798	0.796	0.792
	RF	96.73	0.970	0.967	0.967		RF	87.84	0.881	0.878	0.879
Chest	SVM	97.28	0.973	0.973	0.973	Chest	SVM	83.97	0.848	0.840	0.842
	DT	91.30	0.914	0.913	0.913		DT	81.76	0.820	0.818	0.816
	RF	97.82	0.981	0.978	0.979		RF	92.81	0.931	0.928	0.929
Ankle	SVM	97.28	0.975	0.973	0.973	Ankle	SVM	94.47	0.948	0.945	0.945
	DT	96.73	0.968	0.967	0.968		DT	88.95	0.892	0.890	0.890
	RF	97.28	0.974	0.973	0.973		RF	96.13	0.962	0.961	0.961
User Identification based on 'Standing' Activity						**User Identification based on 'Lying' Activity**					
Body Position	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**	**Body Position**	**Classifier**	**Accuracy %**	**Precision**	**Recall**	**F1**
Hand	SVM	79.56	0.799	0.796	0.974	Hand	SVM	90.52	0.905	0.905	0.905
	DT	75.80	0.755	0.758	0.754		DT	87.36	0.874	0.874	0.873
	RF	85.48	0.862	0.855	0.857		RF	91.57	0.920	0.916	0.916
Chest	SVM	91.39	0.916	0.914	0.915	Chest	SVM	93.68	0.938	0.937	0.937
	DT	83.33	0.843	0.833	0.836		DT	92.63	0.928	0.926	0.926
	RF	91.93	0.921	0.929	0.920		RF	94.21	0.943	0.942	0.942
Ankle	SVM	93.01	0.930	0.930	0.930	Ankle	SVM	93.15	0.936	0.932	0.932
	DT	85.55	0.866	0.866	0.864		DT	91.05	0.913	0.911	0.910
	RF	93.54	0.939	0.935	0.936		RF	93.15	0.934	0.932	0.932

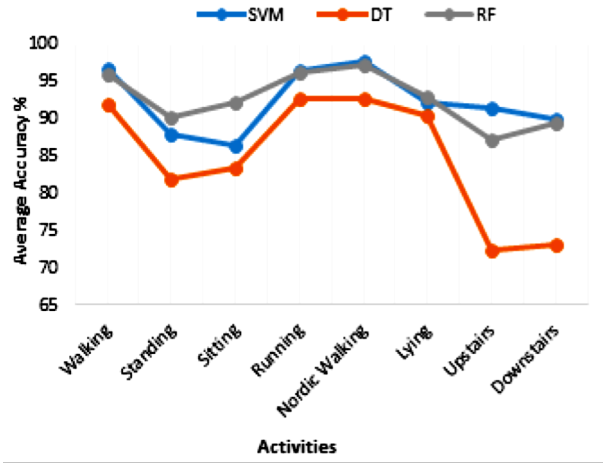

Fig. 2. Average accuracy rate for user recognition achieved by selected classifiers based on all activities

To provide the individual recognition accuracies for all eight users, Table 4 and Table 5 show the sample confusion matrices obtained for the best-case recognition results using RF classifier (for the *ankle* position). It can be observed from these tables that all eight users were individually recognized with a very high accuracy rate, which shows the effectiveness of the proposed approach for user identification.

Table 4. Confusion matrix for user identification obtained using RF classifier based on *walking* (accuracy = 97.44%)

	U1	U2	U3	U4	U5	U6	U7	U8
U1	22	0	0	0	0	0	0	0
U2	0	31	0	0	0	1	0	0
U3	0	0	28	0	0	1	0	0
U4	0	0	0	31	0	0	0	0
U5	0	0	0	1	30	1	0	0
U6	0	0	0	1	0	24	0	0
U7	0	0	0	0	1	0	32	0
U8	0	0	0	0	0	0	0	31

Table 5. Confusion matrix for user identification obtained using RF classifier based on *sitting* (accuracy = 96.13%)

	U1	U2	U3	U4	U5	U6	U7	U8
U1	23	0	0	0	0	0	0	0
U2	0	21	0	1	0	0	0	0
U3	0	0	27	1	0	0	0	0
U4	0	0	0	24	1	0	0	0
U5	1	1	0	0	24	0	0	0
U6	0	0	0	0	1	22	0	0
U7	0	0	0	0	0	1	11	0
U8	0	0	0	0	0	0	0	22

5. Conclusions

This paper focused on the identification of individual users based on their activity patterns using data captured from wearable sensors. These sensors were placed at three different body locations, i.e., *hand*, *chest*, and *ankle*. Selected activities were used to validate the proposed scheme which included *walking*, *nordic walking*, *running*, *walking upstairs*, *walking downstairs*, *sitting*, *standing*, and *lying*. Fourteen different time and frequency domain features were extracted from wearable sensors data to recognize the user by learning different activities efficiently. It was observed that the performance of RF classifier was better than SVM and DT classifier for identifying users.

The results demonstrated that user identification was the most accurate during the *walking* activity where the sensors were placed on the *ankle* position. In contrast, user identification achieved the least accurate performance when the sensors were placed at the *hand* position during activities such as *sitting* and *standing*.

References

1. Alzubaidi, A. and J. Kalita, Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 2016. 18(3): p. 1998-2026.
2. Delac, K. and M. Grgic. A survey of biometric recognition methods. in 46th International Symposium Electronics in Marine. 2004.
3. Chiasson, S.v.O.P.C.B., R. A Usability Study and Critique of Two Password Managers. in In Proceedings of the 15th conference on USENIX Security Symposium, Vancouver, BC, Canada,. 2006.
4. Ma, J., et al. A study of probabilistic password models. in Security and Privacy (SP), 2014 IEEE Symposium on. 2014. IEEE.
5. Kelley, P.G., et al. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. in Security and Privacy (SP), 2012 IEEE Symposium on. 2012. IEEE.
6. Srinivas, S., D. Balfanz, and E. Tiffany. FIDO Universal 2nd Factor (U2F) Overview. [cited 2018 5 December]; Available from:https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf.
7. Lee, P., D. Stewart, and J. Barker, Deloitte TMT Predictions 2014, in Technical Report Deloitte: New York, NY, USA,. 2014.
8. Šprager, S., R. Trobec, and M.B. Jurič. Feasibility of biometric authentication using wearable ECG body sensor based on higher-order statistics. in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on. 2017. IEEE.
9. Reiss, A. and D. Stricker. Introducing a new benchmarked dataset for activity monitoring. in Wearable Computers (ISWC), 2012 16th International Symposium on. 2012. IEEE.
10. Song, K.-T. and W.-J. Chen. Face recognition and tracking for human-robot interaction. in Systems, Man and Cybernetics, 2004 IEEE International Conference on. 2004. IEEE.
11. Chien, Y.-T., et al. Real-time Surveillance System by Use of the Face Understanding Technologies. in DICTA. 2003. Citeseer.
12. Pentland, A., B. Moghaddam, and T. Starner, View-based and modular eigenspaces for face recognition. 1994.
13. Rajpoot, N. and K. Masood. Human gait recognition with 3dwavelets and kernel based subspace projections. in International Workshop on HAREM. 2005.
14. Nguyen, L.N. and S. Sigg, Personalized Image-based User Authentication using Wearable Cameras. arXiv preprint arXiv:1612.06209, 2016.
15. Ehatisham-ul-Haq, M.; Azam, M.A.; Loo, J.; Shuang, K.; Islam, S.; Naeem, U.; Amin, Y. Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing. *Sensors* 2017, *17*, 2043.
16. Shen, C., et al., Performance analysis of motion-sensor behavior for user authentication on smartphones. Sensors, 2016. 16(3): p. 345.
17. Conti, M., I. Zachia-Zlatea, and B. Crispo. Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call. in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. 2011. ACM.
18. Xu, W., et al. Sensor-assisted face recognition system on smart glass via multi-view sparse representation classification. in Information Processing in Sensor Networks (IPSN), 2016 15th ACM/IEEE International Conference on. 2016. IEEE.
19. Zhang, Y., et al., Accelerometer-based gait recognition by sparse representation of signature points with clusters. IEEE transactions on cybernetics, 2015. 45(9): p. 1864-1875.
20. Zeng, Y. Activity-based implicit authentication for wearable devices: Ph. D. forum abstract. in Proceedings of the 15th International Conference on Information Processing in Sensor Networks. 2016. IEEE Press.
21. Blasco, J. and P. Peris-Lopez, On the Feasibility of Low-Cost Wearable Sensors for Multi-Modal Biometric Verification. Sensors, 2018. 18(9): p. 2782.
22. Wu, G., et al., A Continuous Identity Authentication Scheme Based on Physiological and Behavioral Characteristics. Sensors, 2018. 18(1): p. 179.